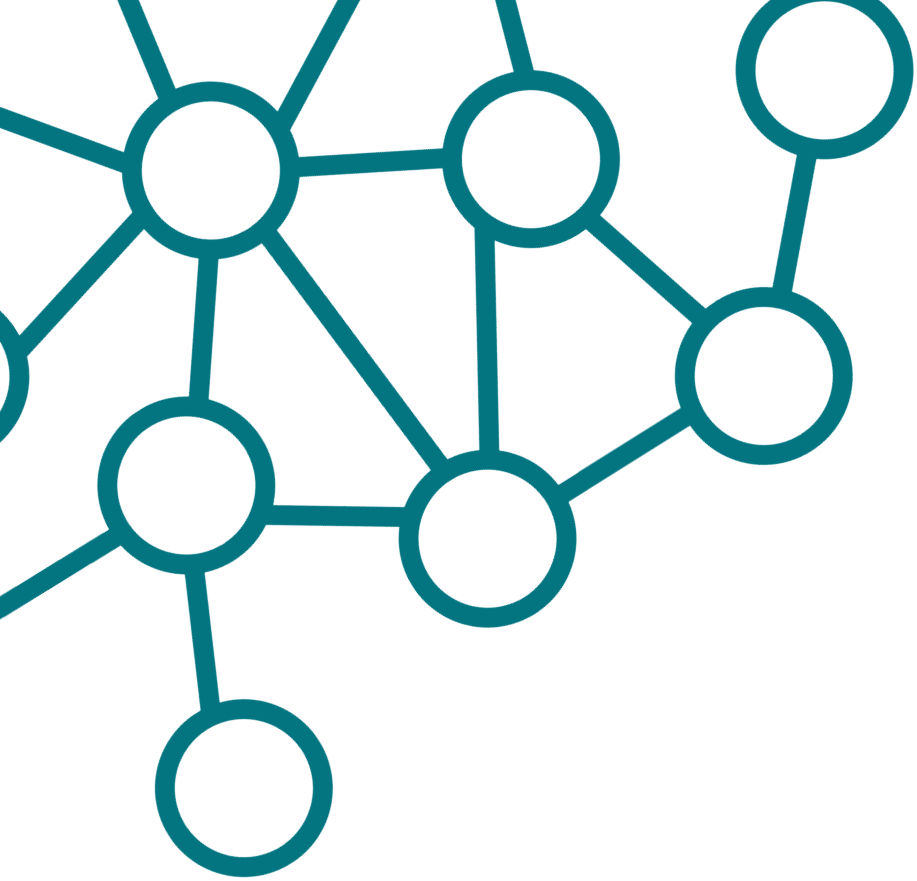
PolicyWise
for Children & Families

LAW & GOVERNANCE OF SECONDARY DATA USE

OBLIGATIONS OF NOT-FOR-PROFIT ORGANIZATIONS IN ALBERTA

KIRAN POHAR MANHAS, JD, PHD
POLICYWISE FOR CHILDREN & FAMILIES | UNIVERSITY OF CALGARY



Disclaimer:

This work is for information purposes only, and not intended to be legal advice. For particular legal advice on your circumstances, the authors recommend that you seek independent legal advice.

ACKNOWLEDGEMENTS:

This paper would not be possible without the direction and support of a great many people. First, and foremost, I thank the SAGE (Secondary Analysis to Generate Evidence) leadership and team at PolicyWise for Children & Families. Jason Lau and Xinjie Cui provided excellent leadership in requesting this project and guiding its formation. Amanda Lau, Lucie Richard and Robert Jagodzinski provided important feedback to early drafts of the report. I thank the numerous external stakeholders who provided thoughtful feedback on a draft version of this paper amidst their busy schedules. These stakeholders included Chris Stinner (Office of the Information and Privacy Commissioner of Alberta), Don Fleming (ARECCI/Alberta Innovates), Katharin Pritchard (Calgary Thrives/Mount Royal University), Geoff Zakaib (Data for Good), and Robert Perry (CUPS). Although I received important feedback from these individuals, I take full responsibility for any mistakes or omissions.

I am also very appreciative of the infrastructure and mentorship support I receive from my postdoctoral team including supervisors Drs. Suzanne Tough and Xinjie Cui, funders including PolicyWise for Children & Families, and the team including the All Our Families research team.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The data-driven nature of society today involves the collection of significant, if not copious, amounts of information with the aims to share and re-use that data beyond the original purposes at collection. Not-for-profit organizations and registered charities (collectively, "NFPs") are beginning to recognize the value of, and opportunities within, data especially in the social services sector. This paper presents the legal and governance issues for, and obligations of, NFPs when trying to harness a particular data-focused opportunity: the sharing and re-use of information beyond the service delivery directing collection.

When personal information or personal health information is collected, handled, used or disclosed, privacy concerns arise and privacy legislation could be invoked. In Alberta, the three privacy-related statutes are PIPA, the Health Information Act (HIA), and the Freedom of Information and Protection of Privacy Act (FOIP). This paper details when each of these laws could apply for a NFP, as well as the best practices dictated by these laws. Those best practices centre around ensuring reasonableness in the purposes for identifying information collection, use and disclosure; exacting minimalist standards on information use and disclosure; and ensuring the connection, unless legally exempt, between purposes and consent from the individuals whom the information is about. The legal interpretations of reasonableness, use and disclosure are key to understanding privacy expectations of NFPs. This paper analyzes these interpretations from the Office of the Information and Privacy Commissioner of Alberta orders from 2012-2017.

With respect to secondary use of data, intellectual property laws especially copyright and governance expectations around research-related secondary use are considered as they apply to NFPs. Copyright licenses represent one potential, but not always applicable, forum. Copyright protects the expression of an idea, not the raw facts or data in that idea: so when sharing information at the variable-level copyright may not apply outside of the data layout. Nonetheless, in theory and in practice by one NFP, open or managed licensing agreements offer a mode of clarifying rights and obligations while making information available for secondary use. Research ethics board are a critical legal tool in the secondary use of health information in Alberta. They also act as an important safeguard for NFPs when attempting to manage access to data, as demonstrated by the Medicins Sans Frontiere data sharing policy.

NFPs currently fall into several legislative gaps with respect to secondary use of data including identifying information. For example, privacy laws do not apply to duly incorporated NFPs carrying out non-commercial activities, and research ethics boards are not obliged to review the planned secondary uses of data by NFPs if there is neither university affiliation nor health information involved. Nevertheless, best practices around data governance and privacy protection abound. Societal expectations, ethical practices, and conservative business approaches all demand that NFPs approach the secondary use of data from a legal and governance perspective. Such a perspective demands the development of a data and privacy policy. Such a policy should be formatted to include a vision statement that clearly links to recognized legal requirements and international Fair Information principles, and which details the NFP's expectations around the goals of data sharing and the tensions to balance. The content of the policy should then describe the safeguards in place, the access processes required for secondary use, and the monitoring processes for compliance. Prioritization of consent, "need to know" directives, and reasonableness would promote compliance with privacy laws. Roles and tasks could be enumerated to promote effective implementation.

"The value of data lies in their use" [1]. The data-driven nature of society today confirms the extensive implementation of this adage. Often this entails the collection of significant, if not copious, amounts of information with the aims to share and re-use that data beyond the original purposes at collection. The Government of Alberta has recognized the importance of information as "the lifeblood of social-based, client service delivery, planning and policy" [2]. Not-for-profit organizations and registered charities (collectively, "NFPs") are also beginning to recognize the value of, and opportunities within, data especially in the social services sector [3-6]. This paper will present the legal and governance issues for, and obligations of, NFPs when trying to harness a particular data-focused opportunity: the sharing and re-use of information beyond the service delivery directing collection. The parties involved in these data-focused opportunities could include the original NFP, other NFPs, researchers, and data repositories.

This paper consists of four sections. First, the background defines key terminology and delineates the general views for and against NFPs collecting, storing and using information. Second, the legal perspectives section considers the legal issues, obligations and limits that arise for NFPs in Alberta, Canada when they collect, use, and disclose information. Third, industry current or best practices will be discussed to inform how other NFPs have approached data governance. These current or best practices move beyond what is addressed by the law when NFPs collect, use and disclose information. This governance perspective builds on industry standards and best practices in Canada, and abroad, to demonstrate governance tactics and experiences that are approved or lauded by the community. Finally, the paper concludes by summarizing key recommendations for NFPs in Alberta, Canada that aim to maximize data-driven opportunities around the collection, use and disclosure of information by NFPs amongst themselves.

1. BACKGROUND

Before discussing the nuances of data-driven opportunities for NFPs, several key terms should be clarified: particularly, NFPs, data and the facets of data-driven opportunities at the centre of this paper.

1.1 KEY TERMINOLOGY

NFPs include the following, as defined by relevant Alberta legislation:

- Nonprofit organizations are formed to promote art, science, religion, charity or other similar endeav ours, or they may be formed solely for the purpose of promoting recreation for their members. They are defined by, and governed under, the Companies Act [7]. This type of NFP can include business-like, or business, activities in its operations.

- A society is an incorporated group of five or more people who share a common recreational, cultural, scientific, or charitable interest. They are defined and regulated by the Societies Act [8]. This is the most common, simplest and least-costly way to establish an NFP in Alberta. This type of NFP cannot engage in any type of one-off, or ongoing, business activities.

- A charitable organization, whether incorporated or unincorporated, (i) is formed for a charitable purpose; (ii) uses a fund-raising business; (iii) intends to or has in fact raise(d) more than $25000 in gross contributions from solicitations to individuals in Alberta; and thus (iv) is required to be registered under the Charitable Fund-raising Act [9].

For all of these entities, the common thread is that people cannot form or use them to make personal financial gain.

Data represents another key term that can be interpreted differently depending on context and stakeholders. Some define data as simply "any type of information" [10]. In the research realm, the UK's Medical Research Council defined data as "qualitative or quantitative information created or collected in the course of research. Sources may include experimental measurements, clinical measurements, observations and

information obtained via survey questionnaires, interviews, non-research documents (for example, letters) or focus groups [11]." In the NFP realm, data and information have been particularly distinguished: data is considered "raw values or facts… [which] can be qualitative or quantitative and can come in a variety of forms", while information is "made up of data… [which] has been processed or analyzed within a context to make it useful" [12].

The Nonprofit Technology Network has surveyed NFPs regarding their relationship with data, or metrics as they called it [3]. The data types discussed included (a) financial and internal operations data (e.g. expenses, income and cash-on-hand, volunteer hours, staff training); (b) marketing, communications and fundraising data (e.g. number of people added to NFP mailing list; number of new donors; number of website visitors, Facebook comments and email opens); (c) tracking programs and outcomes (e.g. actual financials vs. budget; attendance data; client demographics and geography; program participation; client/constituent outcomes; client/constituent satisfaction surveys; client recidivism; longitudinal research); and (d) external data (e.g. open government data that touches on the NFPs' or their clients' interests or needs; government data about their specific clients (if possible given limitations); aggregate data from other NFPs in the same or similar areas; individual-level data from other NFPs in the same or similar areas) [3].

Ultimately, data comes in various forms including text, images, video, sound or maps. Metadata represents the " 'data about data', [by] providing concise information about the content, quality, condition and other characteristics of datasets [11]." When all data from or about a defined group or study are collated, including data derived from the originally-collected data and metadata about the collection, governance and interpretation of those data, then that is termed the dataset [11].

Personal data or information represents a critically distinct subset of data, which is recognized as legally, ethically and practically sensitive. Alberta's Personal Information Protection Act (PIPA) defines "personal information" as "information about an identifiable individual" [13]. Similarly recognized as sensitive is "personal health information", which is similarly enumerated in the provincial Health Information Act (HIA) and the federal Personal Information Protection and Electronic Documents Act (PIPEDA); PIPEDA

defines "personal health information" succinctly as relating to an individual, whether living or deceased, and includes:

> "(a) information concerning the physical or mental health of the individual;
>
> (b) information concerning any health service provided to the individual;
>
> (c) information concerning the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
>
> (d) information that is collected in the course of providing health services to the individual; or
>
> (e) information that is collected incidentally to the provision of health services to the individual [14]."

Another categorization of data relates to level of availability: private, shared and open [12]. Private data is "currently held in the private domain, [and] … is not publicly available or shared" [12]. Shared data is "shared in a limited way, often to researchers or partners through data sharing agreements" [12]. Repositories represent centralized platforms wherein datasets are deposited and data sharing is managed. Open data is "a resource that is made available to anyone with the skills and desire to use it" [12]. To meet the principles of openness, data must be "available under an open license; available in a convenient and modifiable form; machine-readable; accessible as a whole, with little or no cost associated with its use" [12]. Similarly, open data must not include individually-identifying information [5]. This specific categorization of data correlates directly with the types of opportunities data present.

1.2 NFPS & DATA OPPORTUNITIES

The Internet has altered the perceptions and use of information: it has facilitated the availability of a vast amount of information, the speed at which it can be accessed, and the machine-readiness of the information given its digital format [5]. Internet and novel technologies have made it possible, and desirable, to re-use and re-purpose data collected for one purpose for a different, secondary purpose. Government, research funders and institutions, researchers, corporations, and NFPs are now all considering the avail-

ability and opportunity of data. Secondary use of data is the term used to describe the reuse of data for purposes outside of the original purpose at collection, as such it includes open data and data sharing initiatives.

The secondary use of data, whether internal or external to the organization, could promote innovation in the NFP sector by particularly advancing decision-making [5]. A study of 12 NFPs demonstrated that high-impact, successful organizations, amongst other things, used information to modify their tactics to increase their success [15]. Data enables the measurement of financial and operational health of an organization, identifies problems, and measures organizational impact [3]. Three effective ways to mobilize the secondary use of data include understanding needs or issues better, improving operational effectiveness (e.g. in service delivery or support functions), and improving understanding of results and impact [16]. Two major trends noted for Canadian NFPs in 2016 include (a) novel technologies and data management tactics to help NFPs maximize their impact and promote efficiency, and (b) greater reliance on shared platforms and administrative outsourcing to weather a challenging economy [4].

There are challenges for NFPs to harness the data for secondary use, both internal and external to their organization. NFPs generally "lack a capacity for numeracy" [5]. Canadian researchers are far behind other countries' researchers regarding the study and improvement of domestic NFP sectors [5]. Many are calling on NFPs that produce their own data to collect and publish data in ways that facilitate reuse, with data published in easier-to-use formats, in non-aggregated or non-summary form, with explicit permission for reuse [3-6, 12]. There are noted supply and demand issues that impede many NFPs from getting the most out of their, or others', data [16]. Supply issues include various barriers to access of sensitive data: legal barriers (e.g. the data is identifying); technical barriers (e.g. structure of databases and location of data); attitudinal barriers (e.g. resistance to sharing data with NFPs or concerns regarding misuse overriding desire to share); and resource-based barriers (e.g. lack of time, skills, and funds to create the requisite systems and processes). Demand-related issues include lack of awareness of available data; lack of capacity or resources to invest in data reuse; lack of capability to analyze data or understand results; lack of desire for fear of potentially negative or disruptive results; and lack of incentives to overcome barriers to accessing and using data [16]. The circumstances for NFPs, in the UK and likely Canada, have been described as be-

ing disincentives: "[t]he current environment – reduced funding, fierce competition for resources, more results-related payments, and a readiness to criticize charities – creates an even greater aversion to risk, which in turn is a disincentive to data use [16]."

2. LEGAL PERSPECTIVES

To harness the opportunities in the secondary use of data, NFPs must consider the applicable legal obligations and rights, as laid out in legislation and case law. Secondary data use confers two crucial legal perspectives: first, that of the data producer who originally collects information from data sources, and second, that of the data accessor who aims to reuse information for a different, secondary purpose. With both perspectives in mind, the driving legal question then becomes: how can NFPs participate in the secondary use of data that they collect? Three categories of legal issues address this question: (1) privacy issues; and (2) intellectual property issues; and (3) governance issues.

2.1 PRIVACY ISSUES

When personal information or personal health information is collected, handled, used or disclosed, privacy concerns arise and privacy legislation could be invoked. Privacy has been defined as the "right to be let alone" and the "entitle[ment] to decide whether that which is his shall be given to the public" [17]. Activities potentially harmful to privacy relate to information collection (including surveillance and interrogation), information processing (including aggregation, identification, insecurity, secondary use, and exclusion), information dissemination (including breach of confidentiality, disclosure, exposure accessibility, blackmail, appropriation, and distortion), and invasion (including intrusion and decisional interference) [18].

Provincial and federal privacy legislation, as well as case law interpreting such legislation, has been developed to recognize privacy-related rights and to discourage and sanction activities harmful to privacy. In Alberta, the three privacy-related statutes are PIPA, the Health Information Act (HIA), and the Freedom of Information and Protection of Privacy Act (FOIP) [13, 19, 20]. Very generally, privacy and access issues in Alberta's private sector are covered by PIPA, those in Alberta's public sector are covered by FOIP, and any privacy and access issues relating to personal health information in Alberta is governed by the HIA. There may be times when an organization attracts more than one piece of privacy legislation. Although highly similar, there are distinctions between the three privacy statutes in Alberta. A general aide in determining which privacy law to consider first, one must consider first the information: if it is personal health infor-

mation, HIA applies. FOIP was formed to begin where HIA ends; so the second consideration is whether a public body or its contractor is involved: if a public body is involved, examine FOIP to determine whether that the public body role triggers FOIP provisions. If personal information is at issue, then look to PIPA third to determine if any remaining activities have not been discussed or targeted by HIA or FOIP. That said, in the following, I will first discuss the role of PIPA for NFPs as this would be the most common first step in determining legal liability of provincial private sector organizations, including NFPs. I will then turn to discussing HIA and FOIP provisions and applicability, which could be triggered based on the type of professional employees or governmental contracts some NFPs may be involved with.

Canada's PIPEDA is the federal legislation that governs the collection, use and disclosure of personal information by private sector organizations in all provinces except those with substantially similar privacy legislation [14]. Alberta's PIPA has been deemed substantially similar to PIPEDA, so PIPA would govern all applicable private organizations within Alberta [21, 22]. However, once a private organization transfers personal information into or out of Alberta, whether during collection, use or disclosure, that organization may become subject to PIPEDA for the cross-border transfer of information [21, 22]. As will be discussed in more detail below, when the structure or activity of an NFP triggers PIPA applicability, then where those same structures or activities cross provincial borders out of Alberta, the information collected, used or disclosed in those activities will be governed by PIPEDA [21, 22]. Most critically, the exemption from PIPEDA applies to Part 1, not Part 2 which pertains to electronic documents. Also, in practice, the key difference for Alberta private organizations governed by PIPA is that if they act across boundaries to trigger PIPEDA, then complaints and privacy breaches must be addressed or disclosed to, respectively, the Office of the Privacy Commissioner of Canada not the Office of the Information and Privacy Commissioner of Alberta. If the privacy-related issues relate to both provincial and cross-provincial activities, then both Commissioners may be involved; with each dealing with the matter in their purview. Currently, the federal Privacy Commissioner does not possess the same power to make orders, particularly fines, as the Alberta Privacy Commissioner. Also, as will be discussed in detail below, PIPA contains exemptions for NFPs as long as appropriately incorporated and for all non-commercial activities, but PIPEDA applies to every organization that collects, uses or discloses personal information in the course of commercial activities. Commercial

activity is thus the threshold for all federal privacy law scrutiny. Private organizations otherwise subject to provincial law are not subject to PIPEDA's protection of employee personal information, which only applies to employee personal information of federal works and undertakings.

Privacy legislation does not apply when the personal information is no longer identifying or potentially-identifying.

These privacy statutes have all been guided by the Fair Information Principles, originally espoused by the Organization for Economic Co-operation and Development (OECD) in 1980 [23]. These eight principles call for the necessity of consent to lawfully collect, use and disclose personal information; for accuracy, completeness and currency to characterize personal data collected; for purposes to direct personal data consent, collection, use and disclosure; for appropriate security measures to safeguard the personal data from risks; for transparency to permit individuals to see and correct the information collected about them; and, for openness and accountability around fair data use by the data controllers [21, 23].

Importantly, neither privacy legislation nor its incumbent obligations apply when the personal information is no longer identifying or potentially-identifying, or when the individual about whom the information is about consents to the activity in question. For example, Service Alberta specifically states that PIPA "… does not apply to general information used to operate the business of the organization or to the use of non-identifiable or aggregate information such as statistical information about groups of individuals" [21]. Historically, individuals and organizations have looked to anonymization and de-identification techniques to circumvent the requirements of privacy legislation [24]. With advances in technology, some commentators question whether any information is truly unidentifiable as to avoid privacy laws [24]. Other commentators argue that de-identification is a valid tool that preserves both privacy and utility and that meets the reasonableness objectives in privacy legislation that call for privacy protection and the ability of organi-

zations to utilize the data they collect for reasonable purposes [25, 26]. In either case, privacy, identifiability and consent interrelate and will be discussed together.

Alberta's PIPA governs the collection, use and disclosure of personal information and personal employee information by private sector organizations in Alberta [13, 22]. Personal information, as defined earlier, includes name, address, telephone number, email address, picture, as well as other information about the person, their life and livelihood [13, 22]. Personal employee information refers to personal information about a potential, current or former employee of an organization, that is "… reasonably required by the organization for the purposes of (i) establishing, managing, or terminating an employment or volunteer-work relationship, or (ii) managing a post-employment or post-volunteer-work relationship between the organization and the individual" [13]. Every private organization within Alberta is subject to PIPA regarding all personal information, unless exempted by PIPA itself [13].

2.1.1 PIPA APPLICABILITY TO NFPS

An NFP is not automatically subject to PIPA, but rather becomes subject based on two key factors: the method of incorporation and the activities conducted by the NFP [13, 22].

Section 56 of PIPA particularly deals with the privacy legislation's approach to non-profit organizations. PIPA does not apply to any 'non-profit organization' (as defined by s. 56(1)(b) of PIPA), or personal information in its custody and control, unless that non-profit organization is carrying out a commercial activity [13, 22]. A 'non-profit organization' has a narrow definition under PIPA to mean an organization that is (a) incorporated under the Societies Act, (b) incorporated under the Agricultural Societies Act, or (c) registered under Part 9 of the Companies Act (s. 56(1)(b)) [13, 22]. An NFP that is not so duly incorporated is subject to PIPA for the entirety of its activities.

An NFP that meets the PIPA non-profit incorporation exceptions could become subject to PIPA for the personal information that is collected, used or disclosed by the organization in connection with "any commercial activity" carried out by the NFP (s. 56(3)) [13, 22]. Personal information of employees or volunteers of an NFP are not subject to PIPA [13, 21]. Any activities not commercial in nature would not be subject to

PIPA for a 'non-profit organization.'

Section 56(1) of PIPA contains the following definition of "commercial activity":

> (i) Any transaction, act or conduct, or
>
> (ii) Any regular course of conduct,

That is of a commercial character and, without restricting the generality of the foregoing, include the following:

> (iii) the selling, bartering or leasing of membership lists or of donor or other fund-raising lists;
>
> (iv) the operation of a private school or an early childhood services program as defined in the School Act;
>
> (v) the operation of a private college as defined by the Post-Secondary Learning Act [13];

A 2013 decision of the OIPC proffers the most guidance around whether an NFP is conducting "commercial activities" to trigger the responsibilities of PIPA [22, 27]. In this case, the Applicant requested access to his personal information held by the Legal Aid Society of Alberta (LASA) and considered their response incomplete [27]. The Applicant then complained to OIPC. The Adjudicator first considered whether PIPA applied to LASA. First, the Adjudicator recognized that the determination of whether a commercial activity occurred will be on a case-by-case basis. Second, the mere exchange of a service for a fee does not in itself indicate a commercial activity, rather PIPA intends to include trade or business-like activity. The Adjudicator noted that "… PIPA is meant to apply to non-profit organizations that are carrying out activities as though they are a business." LASA could not be distinguished "from an operational or service standpoint" from a private law practice when LASA assessed individuals for legal aid coverage, arranged for legal services to be provided, and provided legal services (para. 33) [27]. As such, LASA's collection of personal information for these purposes was subject to PIPA.

For completeness, the following are a few further discussions in OIPC decisions related to the applicability

of PIPA to NFPs and the commercial nature of the impugned activities. First, in the Lindsay Park Sports Society case, the activity at issue was the placement of security cameras in the men's locker rooms of the Talisman Centre to address an increasing number of thefts and property damage in that location [22, 28]. The organization was incorporated under the Societies Act and thus deemed a "non-profit organization" under PIPA, but it was found to collect personal information in connection to a commercial activity thus triggering PIPA scrutiny. The factors that turned this determination included the charge of an admission fee, and the primary motivation for the security cameras (and information collection) was for business reasons (i.e. to decrease theft and property damage to maintain business) [22, 28].

Second, in the Canadian Skin Cancer Foundation case, the activity at issue was that information from a Patient History form during a doctor's visit led to solicitations from her doctor, the Canadian Skin Cancer Foundation, and another entity that all shared a mailing list database despite the Complainant having opted out of the mailing list [22, 29]. The OIPC Adjudicator found that the Foundation was a non-profit organization appropriately incorporated under the Societies Act [22, 29]. The OIPC Adjudicator considered whether marketing and soliciting for fundraising was a commercial activity [22, 29]. The OIPC Adjudicator deemed that commercial activity could be a single act or a course of conduct that is of commercial character. The Foundation's fundraising was done to raise funds for charitable purposes and not for regular operations or non-charitable purposes, and was distinct from the recognized commercial activity of selling membership, donor or fundraising lists [22, 29]. As such, the Foundation was deemed not subject to PIPA. And, finally, in the Fairways Villas South Homeowners' Association case, an appropriately incorporated NFP managed and maintained the Fairways Villas lands for a monthly fee; it also sent emails to the Complainant regarding lawn care and sprinkler testing [22, 30]. Because the maintenance services were provided in exchange for a monthly fee, the Homeowners' Association was subject to PIPA for email disclosures as this was in direct connection to a commercial activity [22, 30].

2.1.2 PIPA GENERAL OBLIGATIONS

The goal of PIPA is to balance a private sector organization's needs to collect, use or disclose information for reasonable purposes against the individual's right to have their personal information protected [13].

These goals are mirrored in HIA and FOIP. PIPA has delineated the standard of reasonableness to be "what a reasonable person would consider appropriate in the circumstances" [13]. The legal interpretation of the terms "collect", "use", "disclose", and "reasonable" are critical and will be discussed more fully below at section 2.1.3; this section aims to solely overview the general obligations under PIPA.

> Only reasonable purposes and methods of collection can be consented to.

PIPA details individuals' rights and private sector organizations' obligations including the following: "identifying the occasions when private sector organizations must obtain consent for the collection, use and distribution of personal information; how consent must be obtained; how individuals may request access to and correction of their personal information; how an organization must respond to an individual's request for access to information; how personal information must be protected; and when the Office of the Information and Privacy Commissioner of Alberta (OIPC) can review complaints" [13, 22]. The details on PIPA-mandated procedures and processes for consent and personal information protection will be detailed below in section 2.1.4 (best practices dictated by PIPA).

PIPA applies to personal information whether the information is recorded or not, but the rights of access and correction only apply to recorded personal information [13, 21]. PIPA does not apply to general information used to operate a business, or to the use of non-identifiable or aggregate information (e.g. statistical information about groups of individuals). Private-sector organizations subject to PIPA are responsible for the personal information in their custody (e.g. in their offices, computers, storage devices, etc…) or control (i.e. can decide how to use, disclose and store the personal information) [13, 21]. With respect to collection, use and disclosure of personal information, Table 1 broadly presents the key requirements that must be met by a PIPA-regulated private-sector organization (note: this list is not exhaustive of all PIPA obligations).

Consent remains a crucial component to privacy protection laws: it provides a means for organizations and individuals to agree amongst themselves about the appropriate collection, use and disclosure of personal information, especially when it may move beyond the general rubric of applicable privacy laws. Un-

less PIPA specifically exempts, organizations must get informed consent to collect, use or disclose personal information [21]. In gathering consent, organizations must adequately inform individuals of the purpose for information collection, as well as the proposed and potential uses, disclosures, storage and disposal of the information [21]. Only reasonable purposes and methods of collection can be consented to; an individual cannot consent to unreasonable collection of personal information, including any extra information disclosed that is not needed for the purpose [21].

Entirety of original consent carry forward to secondary organizations.

Consent can be express (written or verbal), implied (information is volunteered in reasonable and clear circumstances), or opt-out [21]. The features of opt-out consent include that organizations provide individuals with the reasonable purpose of their need for personal information; with easy-to-understand notice provided that consent will be imputed if they do not opt-out; with a reasonable window and chance to say no and opt-out; and with assurance that the personal information is not so sensitive that it would be unreasonable to use an opt-out form [21]. Unless a legal duty or obligation would be hindered, an individual can change or withdraw consent by giving the organization reasonable notice (s. 9) [13, 21]. Individuals can place reasonable terms and conditions on their consent, such as limiting the types of uses that would be permitted under the consent and those that would not [21]. Importantly, s. 8(2.1) of PIPA indicates that if an individual consents to disclosure of personal information about the individual by one organization to another organization for a particular purpose, then the individual is deemed to consent to the collection, use or disclosure of the personal information for the particular purpose by that other organization [13]. Hence, the entirety of the original consent can carry forward to secondary organizations (including repositories or other NFPS, for example) when collected appropriately by the first organization. All organiza-

tions are limited by the particular purpose, the reasonableness of that purpose, and the limit of using the minimal amount of personal information necessary to reach that purpose. The consequences of altered or withdrawn consent should be explained to the individual, such as implications to the service or product delivery provided by the organization or NFP. Conversely, s. 12 of PIPA is clear that an organization cannot collect personal information about an individual from someone other than that individual without the individual's consent, unless that information could have been collected without consent anyways (i.e. fits under consent exemptions from ss. 13, 15 or 22). This requirement would not apply in cases where the other individual does not possess the capacity to consent (e.g. children), in which case the person who is legally able to provide consent can provide the information about them. Consent to collect, use or disclose personal information cannot be a condition for an organization to supply an individual with a product or service, if the information at issue is beyond that necessary to supply the product or service.

PIPA delimits the process for access to, and correction of, personal information held by a private-sector organization [13, 21]. With few exceptions, organizations must facilitate individuals' access to their own information and must respond openly, completely, accurately and in a timely manner. Generally, when personal information in a record that is in the custody or under the control of an organization, then the individual has the right to ask for access to it [13, 21]. Personal information is under the control of an organization if the organization's decision-making power applies to how to use, disclose and store the information, how long to keep it, and how to dispose of it [21]. Personal information is in the custody of the organization if the personal information is kept in the organization's offices, facilities, file cabinets, computers, etc… [21]. PIPA's governance of the exercise of an individual's general right of access to their information is detailed in Table 2.

When information collected by one organization is sent to another business for processing or storage, but the information's use, disclosure and storage remain in the purview of the original, collecting organization, then the information remains under the control of the first collecting organization [21]. The obligations under PIPA, including privacy protection and information access facilitation, remain with the first, originally collecting organization [21]. This introduces an obligation to ensure that the second organization protects the information in the same way as the law requires and as the original organization should do

[21]. Service Alberta indicates that "the other [second] business will still be responsible for ensuring its own compliance with the Act" [21]. With regards to information access requests, the original organization thus retains their obligation to meet information access requests. The nature of the agreements between these two parties could elaborate the access request process to include the second other business.

Complaints to OIPC can come from individuals when they think that their personal information has been inappropriately collected, used or disclosed by a private organization in Alberta (PIPA), by a public body (FOIP), or a health information custodian (HIA), or when their request for access to information has not been properly addressed by said applicable entity in Alberta [13, 22]. Investigations and orders around complaints connected to PIPA, HIA, and FOIP are in the purview of the OIPC. Where none of these pieces of legislation clearly apply but an information or privacy issue is at stake, or where it unclear which or any of the Albertan privacy legislation applies, it would be prudent to turn to OIPC for a determination of legal obligations that do apply related to information privacy. If the issue at hand does not relate to information, data or privacy, then OIPC would not likely have a role. The OIPC website and the Service Alberta website offer guides and pamphlets to assist organizations to understand and comply with PIPA. If a privacy

Obligations under PIPA, remain with the first, originally-collecting organization.

breach occurs but it involves an organization that is not within the purview of any Canadian privacy laws, then the party could attempt a private civil lawsuit arguing a breach of privacy, which would require several things including proof of harm caused by the data breach and a relationship of responsibility between the individual and the organization.

Failure to comply with PIPA can lead to a complaint by an individual, which could lead to review, inquiry and possibly an order by OIPC. Once a final order is pronounced (and there is no further right of appeal),

an organization has 50 days to comply (s. 54(1) PIPA) [13]. Beyond the costs of compliance with an order (and the incurred costs of defending against a complaint), an organization could be liable to the complainant for damages for loss or injury that results from the breach (s. 60(1) PIPA). If an organization has contravened PIPA and been found guilty of such an infraction, then the organization can be liable for fines of up to $10000 in the case of an individual, and up to $100000 in the case of a person other than an individual (e.g. corporation) (s. 59(2) PIPA). Importantly, as stated above, these fines are not currently available to the Federal Privacy Commissioner to impose. There is also the risk that an OIPC complaint or order could lead to negative publicity for an NFP and reputational losses in the long-term [22].

2.1.3 PRIVACY-RELATED LEGAL INTERPRETATIONS OF "REASONABLE", "USE" AND "DISCLOSURE"

Privacy law encompasses not only the stipulated statutes and regulations, but also the legal interpretations of those statutes and regulations by judges in courts and by adjudicators at OIPC. This case law and adjudicative decisions, respectively, provide further information and obligation around the legal rights of individuals and the legal responsibilities of private-sector organizations.

Three terms used and relied upon heavily in PIPA that require more illumination via legal interpretation include "reasonable", "use" and "disclose/disclosure." These terms set out what activities are permissible for PIPA-applicable organizations.

Service Alberta has provided a plain language guide for small businesses and organizations around how to approach and meet the requirements of PIPA [21]. Service Alberta has elaborated the "what is reasonable" test from PIPA as "what a reasonable person would think is appropriate in the situation" [21]. This is the question posed when considering the reasonableness of many activities permitted under PIPA. For example, the reasonableness must be assessed of the purpose in collecting personal information, of any implied consent, of the development and implementation of organizational privacy policies, and of the use or disclosure activity involving the personal information.

In the interpretation of "reasonable" in PIPA, there is direction from the highest court in Alberta, the Alber-

ta Court of Appeal, from the 2011 decision of Leon's Furniture Ltd. v. OIPC: "PIPA balances two competing values: the right to protect personal information and the need to use that same information. In balancing these values, PIPA employs the standard of reasonableness, allowing PIPA to be flexible for small- and medium- sized businesses. Both of these values must be balanced and neither can be given more weight than the other, as that may lead to an unreasonable result" [31]. Another legal analysis has suggested that promoting service and sector efficiency and effectiveness would be a reasonable purpose for a private sector organization, including NFP [22].

Service Alberta distinguished "use" and "disclosure" as follows:

> "**Using personal information** usually means using it internally to carry out the organization's purposes. These include providing a product or service or evaluating whether an individual is eligible for a discount. Normally, an organization or its contractors use information within the organization. It would be valid for a shipping department to use customer information that was collected by the billing department.
>
> **Disclosing personal information** means showing, sending, telling or giving some other organization or individual the personal information in question. Information is disclosed externally when provided outside the organization. To continue the example above, providing the customer's name and address when requested by Canada Revenue Agency would be a valid disclosure of personal information." [21]

The Service Alberta guidance would be highly persuasive alone in the legal interpretation of these terms by a judge or OIPC adjudicator. Importantly, it seems "use" and "disclose" are demarcated by an internal versus external barrier. It would suggest that an NFP that conducts secondary use of personal information for purposes and activities that are wholly internal to that NFP or organization would fall under PIPA for "use"-related provisions and limits. "Use" would seem to cover the activities of contractors external to an organization, but acting for that organization and the various departments of a multi-departmental organization. Meanwhile, an NFP or organization that conducts or permits secondary use of personal information alongside or by an entity completely external to the NFP or organization would fall under PIPA for

"disclose"-related provisions and delimits. It would be likely that the sharing of NFP data between distinct NFPs or with an external data repository, without any contractor-style agreement amongst them, would be considered "disclosure" under OIPC.

Further understanding on the legal interpretation and approach to appropriate "use" and "disclosure" under Alberta's privacy legislation (whether PIPA, FOIP or HIA) can be garnered by examining the OIPC adjudication decisions themselves. The online OIPC adjudicative decisions database was hand-searched using the following inclusion criteria: (1) decision issued in last five years (2012-2015); (2) issues do not solely consider complaints around requests for information access or correction; and (3) adjudicator considers issues related to "use" or "disclosure" of information. Table 3 provides a detailed analysis of the 36 included OIPC adjudicative decisions, with an emphasis on determining what is considered appropriate and allowable "use" and "disclosure", and what is not.

Several key findings can be surmised from this analysis. First, generally, the legal approach to issues of "collection" and "use" are determined together, while "disclosure" is interpreted separately while being highly informed from the legal analysis of "collection" and "use." Second, with respect to complaints, OIPC examines collections, uses, and disclosures of personal information very specifically and very broadly. The findings do not turn on, or consider, the possible negative impact of the disclosure (or collection or use). Such impact is not a consideration of whether the disclosure was authorized or not. Similarly, personal information is "used" when it is available for consideration, not in the narrower circumstance of being given any, little, lots or no weight in a determination; information does not have to be relied upon to be used. "Disclosure" occurs when someone external to the necessary parties could view the personal information; whether they actually viewed such information does not impact the "disclosure" analysis.

Third, PIPA and FOIP are distinguishable not only for the entities that they govern. These two Acts have different purposes and PIPA's definition of "personal information" is considered much broader than that of FOIP because PIPA's definition is simply "information about an identifiable individual." While PIPA aims to balance personal privacy with organizational activities, FOIP carries an additional aim to promote the transparency and accountability of public bodies. FOIP provides a list of types of identifiable information,

thus information must be listed or be qualitatively similar to the enumerated to be considered identifiable information. "Personal information" that triggers privacy legislation scrutiny and protection turns on the term "about"; information that is related to someone is not necessarily about them. "About" is a highly significant restrictive modifier, while "related" is narrower; information associated with someone or their activities is connected to them but is not necessarily "about" them under privacy laws. It is important to remember that as technologies and society evolves, the scope of what constitutes personal information, or not, is similarly dynamic. The list of identifiers is continually growing, and this is recognized in law, by courts and the OIPC.

The three key, interrelated factors: consent, purpose, and reasonableness.

Fourth, the three key, interrelated factors that should guide organizations in their collection, use and disclosure of information are consent, purpose, and reasonableness. There should be a reasonable purpose in collecting the information; there should be consent or statutory exemption to consent that is connected to the reasonable purpose; the information should only be used and disclosed to extent necessary to meet that reasonable purpose; the connections between purposes and activities should be reasonable and direct. Where an organization has no authority to collect and use particular personal information, then it necessarily has neither a reasonable purpose for such information collection and use nor the possibility of collecting or using that information to a reasonable extent. Where use or disclosure of personal information is examined relative to the proviso of only to the extent necessary to meet the previously-established reasonable purpose, the critical term is extent and it should be the minimal extent required to reasonably meet the reasonable purpose. The minimal amount of personal information should be used or disclosed (even if authorized to collect more). As will be discussed again below, the HIA dictates that custodians should only collect, use or disclose "individually identifying health information" after considering whether aggregate or other non-identifying health information would adequately achieve the intended purpose [32]. This adage appears to be applied by OIPC Adjudicators when considering use and disclosure of personal information covered by PIPA and FOIP. The parties both internal or external to the organization or the organization's impugned activity should be the minimal number and type of parties necessary. Everyone

should be on a "need to know" basis or assessment: Does each party who could view, examine, or interpret the personal information reasonably need to know that facet of personal information?

Fifth, databases contain a wealth of personal information and should be safeguarded appropriately, from nefarious, rogue and negligent infringements of privacy protection laws. Access to information in databases, and the reasons for such accesses, should be appropriately logged; and all parties who do, or could, partake in such accesses should be properly trained in privacy protection requirements and monitored for compliance.

Sixth, contracted employees of public bodies can be considered employees for the purposes of FOIP and bring FOIP scrutiny to their activities, especially where they perform functions of, and on behalf of, the public body.

Finally, privacy protection laws do not aim to limit information exchange with anonymity provisos around service delivery itself; but do aim to put limits, constraints and safeguards beyond the point of care. This may translate to NFPs that any initial point of care and service delivery involves information collection as necessary; but any secondary use of information must involve the highest degree of anonymity possible.

2.1.4 BEST PRACTICES DICTATED BY PIPA

NFPs engaged in non-commercial activities are not legally bound by PIPA requirements. It is, however, highly recommended that NFPs should adhere to PIPA's guidelines and best practices such as instituting a privacy policy; appointing a privacy officer to ensure compliance with the policy; ensuring consent is obtained from individuals for the collection, use and disclosure of personal information; ensuring the purposes of information collection, use and disclosure are clear and reasonable; and, ensuring the adequate security of information collected and stored. It has been argued that adhering to PIPA would not present a significant cost to organizations; would avoid the inefficiency of carrying out different information handling procedures when an NFP carries out some commercial activities (triggering PIPA) and some non-commercial activities (not covered by PIPA); and would limit the risk of negative publicity and lost public trust related to personal information complaints (to OIPC or to the media simply) [22].

Section 2.1.1 above presents the general obligations for information handling procedures by PIPA. Table 4 summarizes and supplements that section to act as a reference for NFPs of the best practices dictated by PIPA; this along with Table 1 should provide NFPs with a fair understanding of the activities to follow in order to be compliant with the tenets and requirements of PIPA.

2.1.5 FOIP & HIA CONSIDERATIONS

Although PIPA remains the primary legislation denoting the privacy and consent obligations for NFPs around the collection, use and disclosure of personal information, there may be some NFPs by virtue of their activities or alliances that fall under other Alberta privacy laws, particularly FOIP and HIA. As stated above, fair information principles guide all privacy legislation in Alberta, the rest of Canada and all other countries. A privacy-conservative NFP that follows the PIPA requirements should feel relatively confident in their collection, use and disclosure of personal information. In what follows, a more considered analysis is provided regarding the triggers of HIA and FOIP applicability and the limits of their jurisdiction, as well as any notable (but not exhaustive) distinctions from the previously discussed PIPA.

2.1.5.1 FOIP APPLICABILITY

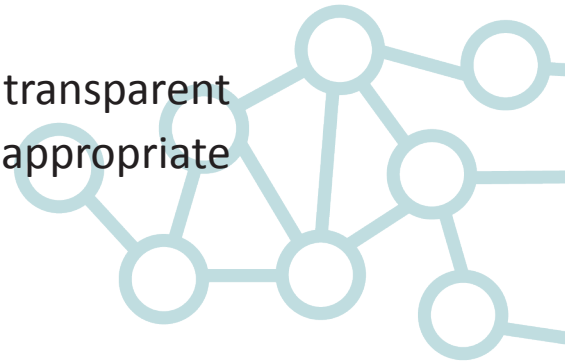
First, NFPs working with a public body should consider the privacy and information-handling requirements of FOIP [19, 22]. In some cases, an NFP will work with a public body via contract, in which case the public body will likely retain control of any records and FOIP would apply to all records [21, 22]. The contractual terms should reflect the legislative requirements of FOIP. The Alberta Privacy Commissioner has criticized the gap in protection when public bodies work with NFPs that are not subject to privacy legislation (i.e. in their non-commercial activities) [22]. The Alberta Privacy Commissioner has recommended that FOIP be amended so that when public bodies and NFPs are sharing personal information as partners in cross-sectoral initiatives, the public bodies are responsible for the collection, use and disclosure and protection of that personal information by the NFP [22].

The contractual terms should reflect the legislative requirements of FOIP.

Second, the HIA could be triggered when NFPs collaborate with or employ HIA custodians. Four criteria trigger HIA: a custodian collects, uses or discloses health information; the information at issue meets the definition of personal health information; the collection, use or disclosure relates to the provision of a health service; and the health information is recorded [32]. Importantly, when the information at issue falls under FOIP or HIA, then that respective Act would apply, not PIPA [13, 21]. For example, when a government department discloses personal information to a contractor carrying out work for that department, FOIP applies to the information (and thus the directly-related activities of the contractor) [21]. Similarly, FOIP has been clearly considered to begin where HIA ends. An organization could be subject to more than one privacy legislation.

FOIP was created to promote an open and transparent government alongside the promotion of appropriate stewardship of personal information to which the government is privy during its public functions.

FOIP was created to promote an open and transparent government alongside the promotion of appropriate stewardship of personal information.



In this way, it differs from PIPA and HIA, whose language and purpose is much more towards protecting individuals' identifying information in a reasonable balance with the needs of private-sector organizations and health services delivery professions and organizations to realize their delivery of goods and services. PIPA and HIA focus on ensuring individuals have access to information about themselves held by organizations or custodians, while FOIP considers individuals access to information held about public bodies and programs in addition to individual-level information about themselves.

2.1.5.2 HIA APPLICABILITY

The HIA, which limits the collection, use and disclosure of health information, applies to "custodians" of

"health information" and to their "affiliates" [20, 32]. The three highlighted terms demarcate the extent of HIA applicability.

A "custodian" is defined in s. 1(1)(f) of the HIA to include the operators of the majority of organizations and entities that provide health services in Alberta, such as the board of an approved hospital; the operator of a nursing home; an ambulance operator; a provincial health board; a regional health authority; a subsidiary health corporation; any board, council, committee, commission, panel or agency created by a listed custodian or designated in the regulations; a licensed pharmacy; as well as the Department and the Minister [20]. In addition, a "custodian" includes a health services provider designated by the regulations to include professionally licensed and regulated pharmacists, optometrists, opticians, chiropractors, physicians, midwives, podiatrists, denturists, dentists, dental hygienists, and nurses [32, 33].

Section 1(1)(a) of the HIA defines "affiliates" to include custodian's employees; those with contractual, volunteer, appointee or student relationships with the custodian; health services providers exercising the right to admit and treat patients at a hospital; an information manager; and, any person designated under the regulations as an affiliate [20]. Importantly, custodians are not defined to include all individuals or entities that may collect or use health information in the course of their work [32]. Rather, custodians are those individuals and entities that are viewed to be, and are positioned to be, trusted "gatekeepers" of an individuals' health information. They can be trusted because of their public foundation or their professional membership and role; mostly, they can be trusted because there is a level of accountability and compliance to HIA attached to their roles.

The applicability of the HIA to NFPs, thus, hinges on whether the NFP is legally included as a "custodian" or its "affiliate." Unlike with PIPA, there is no exception or delimitation of applicability of HIA to NFPs. Many enumerated custodians could be NFPs due to their incorporation or charitable status (e.g. hospital or nursing home operators such as Covenant Health). The HIA would come into effect when a listed health services provider provides a health service while working for an NFP, even if the NFP does not fit within the custodian definition in and of itself. Similarly, if an NFP enters into a contractual, volunteer or other collaborative relationship with an enumerated custodian, then the NFP would be deemed an affiliate and

thus bound by the rules for the collection, use and disclosure of health information.

Because they are not defined as health services providers equal to custodians in the HIA, allied health professionals such as psychologists, social workers, physical therapists, occupational therapists, and respiratory therapists must consider their employment context, contractual relations, and governmental relations to determine whether the HIA applies. Importantly, many of these allied health professionals are employed by NFPs to deliver services; thus, NFPs must also be aware of when HIA scrutiny and obligations are attracted. If an allied health professional is employed by an NFP, and that NFP is neither a custodian nor an affiliate of a custodian, then the information collected, used or disclosed about an individual (even if it is individually identifying health information) would not trigger the HIA (although PIPA could be triggered). A specifically enumerated example to HIA in this area relates to psychologists who work for a Director of the Child, Youth and Family Enhancement Act, their work and particularly any assessments that they conduct are not considered health services and considered exempt to the consent requirements of the HIA.

"Health information" is the other major determinative factor in assessing HIA applicability. Any and all of two types of information are included in "health information": "diagnostic, treatment and care information" (s. 1(1)(i)) and "registration information" (s. 1(1)(u)) [20]. The former is broadly information about an individual's health and health services provided to the individual, while the latter includes six categories including specified demographic information about an individual collected during provision of health services (e.g. address, billing information). Importantly, it is the context of provision of health services that trigger the HIA protections and limitations around "health information." "Diagnostic, treatment and care information" is deemed the most sensitive information about an individual, and thus the most stringent rules apply to this information. Table 4 provides details which categories of information are included in these two types of health information.

If, or once, HIA applicability (or the possibility of its applicability) is determined, then one must consider what activities are permitted, restricted or banned by the HIA as related to the collection, use and disclosure of health information.

2.1.5.3 HIA, CONSENT & DISCRETIONARY DISCLOSURE

Rather than dictate all the HIA requirements herein, the following will focus on the key and notable requirements of HIA in the context of fair information principles, the recognized sensitivity of health information, and the approaches to privacy protection brought along by PIPA and FOIP.

The HIA is clear that personal health numbers are protected as is health information [20, 32]. Also, individuals have right to access their own health information, to ask for corrections to be considered; and to know why it is being collected [20, 32]. There are limits to collection, use and disclosure of health information; and one must always use the least amount of information at highest degree of anonymity (ss. 57, 58) [20, 32].

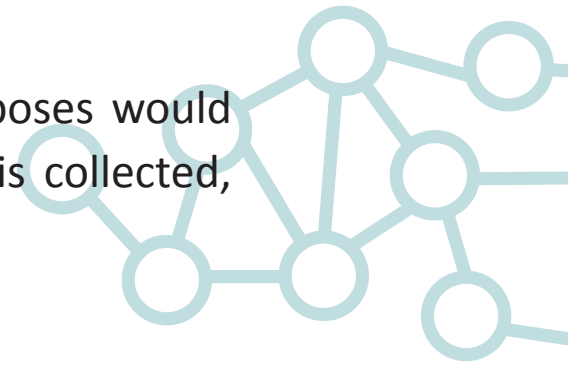
"Non-identifying health information" is information from which identity cannot be readily ascertained.

As stated earlier, custodians are expected to first consider whether the collection, use or disclosure of "aggregate health information" would be adequate for the intended purpose; if adequate, only aggregate health information should be collected, used or disclosed [20, 32]. "Aggregate health information" means non-identifying health information about groups of individuals with common characteristics [20, 32]. Such information is generally statistical information of the type that is virtually impossible to identify to the single individual, unless the cell or sample size is very small (< 10) [20, 32].

If aggregate health information is not adequate for the intended purpose, the custodian must then consider other "non-identifying health information" and whether it would be adequate for the intended purpose [20, 32]. "Non-identifying health information" is defined as information from which the identity of the individual who is the subject of the information cannot be readily ascertained from the information [20, 32]. Removing an individuals' name and personal identifiers before information is disclosed and by not providing other contextual information, information can be essentially anonymous or non-identifying [20, 32]. If such information would suffice, only that should be made use of [20, 32].

Only when aggregate and other non-identifying health information is inadequate for the intended pur-

pose, can the custodian collect, use or disclose individually identifying health information, but only if such activity is authorized by HIA and if such activity is carried out according to the HIA [20, 32]. "Individually identifying health information" means that the identity of the individual who is the subject of the information can be readily ascertained from the information (e.g. name, address, birthdate, full postal code etc…) [20, 32]. "Readily ascertained" is also defined in the HIA to mean "the identity of an individual (e.g the individual's name or other identifiers or distinguishing characteristics associated with an individual) can be determined or deduced without having to apply a sophisticated technical method or process, or without having any particularly technical expertise to do so [20, 32].



Allowing a case-by-case assessment of purposes would ensure the minimal necessary information is collected, used, and disclosed.

This guidance on the order of consideration in the collection, use and disclosure of personal health information is crucial to all custodians under the HIA, and provides a rubric for all organizations to follow the minimal extent of collection, use and disclosure of personal information dictated by PIPA and FOIP. It would be a crucial consideration for all NFPs when determining what data to make available for secondary use and how. Allowing a case-by-case assessment of purposes for the activity involving the information (e.g. through controlled access by the NFP or a repository) would ensure the minimal necessary information is collected, used and disclosed (with collection historically having a bit more lee-way regarding what is minimally necessary, for public bodies at least).

Custodians, a term unique to the HIA, can collect, use and disclose non-identifying information for any purpose, whether it is anonymized health information or aggregate information [20, 32]. As with other privacy legislation, the legal limitations come to bear on the individually identifying health information. Here, as always, purpose matters [20, 32]. Only those purposes authorized under s. 27 sanction custodians

to collect and use individually identifying health information, including providing health services to the individual; determining eligibility for services under Alberta Health Care Insurance Plan; and conducting investigations or practice reviews of health professionals [20, 32]. The Minister, the Department and AHS may use individually identifying health information for planning and resource allocation; health system management; public health surveillance; health policy development, for within geographic area they have jurisdiction [20, 32].

The principles of highest degree of anonymity does not strictly apply to the collection, use or disclosure of health information when using this information for the purpose of providing "health services" or for determining or verifying the eligibility of an individual to receive a "health service" [20, 32]. Privacy laws do not aim to limit information exchange with anonymity provisos around service delivery itself; but do aim to put constraints and safeguards beyond the point of care. This may translate to NFPs that any initial point of care and service delivery involves information collection as necessary; but any secondary use of information must involve the highest degree of anonymity possible.

Generally, an individual's consent is needed before disclosure of individually identifying health information (s. 34 HIA) [20, 32]. However, HIA is not as primarily consent-driven as PIPA; custodians possess a significant ability to collect, use and disclose health information without consent. Exceptions to consent (ss. 35, 37.1, 37.3, 38, 39 40, 46, and 47) relate to legally approved discretionary disclosure [20, 32]. Custodians can

Activity in question must be research to require REB scrutiny before conduct.

disclose individually identifying diagnostic, treatment and care information without individual consent to specific persons and for specific purposes listed in the legislation and regulations [20, 32]. These discretionary disclosures include to another custodian for s. 27 purpose; to the person responsible for giving

continuing care to the individual; to family members or others with a close personal relationship, unless the individual expressly requests that family and friends not be informed; and, to police to prevent or limit fraud or abuse of health services or to protect public health and safety [20, 32].

The HIA permits individually identifying health information (both diagnostic and registration categories) to be disclosed for research purposes by a custodian, without consent, under Part 5, Div 3 conditions [20, 32]. Those conditions include a research proposal assessed by a research ethics board (REB) designated by Minister; the researcher must agree to comply with conditions in s. 53 (i.e. meet the conditions of the custodian for access; obtain consent from participants if demanded by the REB); and the researcher must enter into agreement with custodian (s. 54 conditions) [20, 32].

Data management, in health information and elsewhere, is crucial to good data governance and for compliance with privacy laws. Custodians must enter into agreements with information managers to assist in the appropriate care and storage of the information under its control. Section 66 of the HIA defines an "information manager" as "a person or body that (a) processes, stores, retrieves or disposes of health information, (b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or (c) provides information management or information technology services" [20, 32]. A written agreement between the custodian and the information manager must be entered into to ensure privacy protections and compliance with HIA [20, 32]. When those agreements are in place, consent of the individuals who are the subjects of the information is not required, for the purposes authorized by the agreement. The purpose of the agreement dictates what the information manager may do with the health information [20, 32]. As with other affiliations and contracts, the custodian continues to be responsible for HIA compliance regarding the information [20, 32].

2.2 INTELLECTUAL PROPERTY ISSUES

Intellectual property (IP) issues are separate from privacy and national security issues [34]. Intellectual property falls under federal or national jurisdiction; thus, while inter-provincial activities are covered by the same IP laws, international ones may not [34]. Because IP law covers important ownership, usage and manipulation rights of particular forms of information, it represents an important component to any

discussion on secondary use of data. As will be demonstrated, it is an important but very limited legal obligation and right in Canada regarding secondary use.

In IP, just as in other key legal arenas including privacy law, permission is key [34]. If a data source (e.g. researcher, repository, NFP) gives permission to reuse data and one's intended use fits within scope of the permission, the permission provides the legal basis for data reuse and potential IP-based barriers are removed [34]. But, if intellectual property or other legal rights on original data remain, the secondary user or NFP must not infringe on those. This presents legal uncertainty of when, where and how these other rights from the original data will play out [34]. Primary data sources need to clearly determine the scope of the permission granted downstream when making "their" data available. The rights that may apply to research or NFP data include trade secrets (confidential information), copyrights and the special database rights established in only EU member countries, Mexico and South Korea (and which apply only to databases created or maintained in their borders) [34].

Trade secrets are proprietary or confidential information [34]. According to international standards, national laws treat information as a trade secret if it derives economic value from not being generally known or readily ascertainable, so long as the information has been subject to reasonable measures to keep it secret [34]. Most research data, and likely NFP data, meet this definition, at least in the early stages of collection and generation [34]. Public disclosure of information removes any associated trade secret protection [34]. Thus, data sharing or publication would remove trade secrets in research data [34]. This could be an issue for NFPs or other private sector organizations that have taken reasonable steps to keep some information secret, while also taking part in secondary use. If this is a concern, the NFP should provide for the management of trade secrets in their agreement's terms including timing and scope of information disclosure. Discussions should occur early and often at the agreement negotiation stage, and not at later times of publication or dissemination tactics [34].

Copyright grants author(s) of an original work the exclusive rights to reproduce the work, to publicly distribute copies, to publicly display, publicly perform, or otherwise communicate the work to the public, and to make adaptations of the work [34]. Copyright only becomes an issue for secondary data use if it

is likely or plausible that the creator, owner or repository in which data resides is likely to seek to limit copying, distribution or other reuses of the data [34]. Copyright imposes no restrictions on sharing of the basic building blocks of knowledge (i.e. facts and ideas), which are part of the public domain and which make a lot of the data at issue in secondary use discussions [34]. Raw observations and experimental data are "facts" for copyright purposes and are free to be shared and reused without copyright restriction [34]. Copyright applies to original works of authorship as an author makes creative or editorial decisions about how ideas and facts are expressed [34]. Separate copyrights attach to data items, organizational structures and metadata [34]. In this way, copyright can sit on some but not all levels or layers of a work; the layers that involve expressive choice generally trigger copyright protection [34]. Tables or figures are likely copyrightable; copying a whole dataset will involve copying the copyrighted layer [34]. Most data expressed as numeric values are likely to be "facts" that are in the public domain [34]. Thus, even if copyright exists at an organizational level, numeric values can be copied and reused without any copyright restrictions [34]. Separate copyright can arise in the manner that data are selected and arranged (e.g. organization of Excel spreadsheet if researcher exercised discretion in selecting field names and arranging their order but copyright is limited to this layer of the dataset; no infringement of copyright if secondary researcher republished data with renamed and reorganized fields in spreadsheet) [34]. Annotations, visualizations and other forms of metadata can receive separate copyright protection if sufficiently original [34]. If we use the principle of "discretionary decisions about expression", then copyright applies. Copyright then becomes an issue for the user seeking to reuse these forms of original expression.

There can be users' rights expressed as exceptions to copyright or limits to copyright owner's rights. In the UK, Canada and other Commonwealth countries, the law conducts a fair dealing analysis to determine exceptions to copyright: (1) determine whether the use fits within one of a list of categorically eligible types of use (e.g. using copyrighted work for noncommercial research or private study or criticism or review, which are examples of categorically acceptable uses); (2) balance similar considerations about purpose of use, extent of work used and effect of use on copyright owner [34]. By contrast, in the US, Israel and other non-Commonwealth countries, the fair use doctrine is applied by courts, which "considers [the] nature and purpose of use, how much authorship is in the source work, how much of author's expression has

been taken in the use, and whether the use has an adverse effect on copyright owner's ability to economically exploit the work" [34]. Some countries provide some level of moral rights in authorship, which are personal to author and cannot be transferred [34]. These moral rights include that authors have the right to be attributed; and authors have the right to not be attributed if they no longer wish to be associated with the work.

In recognition of the growing data deluge and its inherent opportunities, the "UK law recently amended its copyright to explicitly permit researchers to content mine the research literature because its Parliament was uncertain whether the existing limitations and exceptions would permit the copying necessary to engage in content mining" [34]. As stated earlier, in Europe, Mexico and South Korea, a Sui Generis Database right was created for databases created or maintained in these borders and if the use of these databases take place in these borders [34]. These special rights apply to any database that requires a "substantial investment" to assemble or maintain the database; so the investment must be in obtaining the data not creating the data [34]. This special database right is limited to recognizing the required investments in obtaining data (not in creating data) [34]. This copyright lasts 15 years [34]. These protections are against extraction or reutilization of substantial parts of a protected database and frequent extraction of insubstantial parts of a protected database [34]. Non-commercial research is not subject to this database right [34].

Usually the person who creates or generates the IP is the initial owner of these rights [34]. When the creator is an employee, rights holding is more complicated and national variation reemerges as an issue [34]. All IP rights are transferable (except moral rights in copyright), so the initial owner may not necessarily be the rights holder [34]. Employers generally own trade secrets developed by employees within the scope of employment [34]. In the absence of agreement or policy, student or independent researchers would own any trade secret rights associated with their data [34]. Sponsored research agreements and university or hospital IP policies generally establish rules of ownership and disclosure for trade secrets [34]. Because of the secret nature of trade secrets, there is no activity required to create it other than the reasonable measures to keep secret. Copyright is initially owned by author(s) of the copyrighted work; the author made creative or editorial decisions about how to express the underlying facts and ideas [34]. "If there is a copyright layer to a dataset or database, the owner(s) of the copyright(s) associated with this layer would be the one(s)

who chose how to organize, arrange, annotate, or visualize the data rather than the one(s) involved in its generation or collection [34]." The Sui Generis Database rights are held by the person or entity that makes substantial investment in collecting data from other sources or maintaining database; so, the rights fall to data aggregators and repositories, not individual researchers, teams, organizations or NFPs [34].

Contracts, licenses and agreements represent a crucial tool for IP rights holders to disclose and share the data protected by (or connected to) their IP rights under terms that meet their rights and obligations, including IP rights and privacy policies. Owners of rights can grant permission for reuse through a non-exclusive license [34]. Or, owners can enter into exclusive licenses with secondary users where they give up the rights to use the IP usually in return for compensation [34]. If the data elements being shared are largely uncopyrightable, then an agreement may not be necessary. But, agreements are important tools in data governance to ensure all rights are met and followed. A crucial example of this is in Table 5, which contains the terms of the copyright license for data shared by Statistics Canada.

2.3 GOVERNANCE ISSUES

Privacy laws are just one area of law that governs the use of information collected by organizations. Another crucial governance tactic relates to data governance and research ethics. Data governance relates to overall management of data, its collection, use, storage and the like. Responsible data stewardship requires a clear and appropriate data governance plan. However, there is no set piece of legislation that sets out the rules and laws for obligations around data governance. It falls within the previously discussed privacy legislation, as well as other important normative tactics such as research ethics. Secondary use of personal health information for research purposes is governed by the HIA; and institutional REBs are recognized by law as the entities that determine whether such research can proceed. REBs thus have become legal instruments around the governance of secondary data use. This section will cover research ethics boards, while the broadest topic of data governance will populate the subsequent section on the ethical analysis. Ethics builds upon the law, but remains distinct from it.

2.3.1 RESEARCH ETHICS BOARDS

The Tri-Council Policy Statement on Research with Human Subjects (TCPS2) is a crucial research policy guidelines in Canada, and it demarcates what is allowed in research with human subjects (whether as individuals, groups, parts of individuals, or information about individuals) [35]. REBs are defined in the TCPS2 as "a body of researchers, community members, and others with specific expertise (e.g. in ethics, in relevant research disciplines) established by an institution to review the ethical acceptability of all research involving humans conducted within the institution's jurisdiction or under its auspices" [35].

In Alberta, there are three REBs designated under the HIA in Alberta, each with a few sub-committees to focus on areas of specialization. First, there is the Conjoint Health Research Ethics Board (CHREB) of the University of Calgary, which reviews applications from Researchers affiliated with the University of Calgary faculties of Kinesiology, Medicine and Nursing. Second, the Health Research Ethics Board (HREB) of the University of Alberta, administers the ethics review process for all faculty, staff and students of the University of Alberta health sciences faculties, Alberta Health Services (in Northern Alberta including Edmonton), and Covenant Health. There are four sub-committees of the HREB, which generally focus on qualitative research, interventional research, non-invasive health research, and invasive biomedical research. Finally, there is the Health Research Ethics Board of Alberta (HREBA), which is housed at the provincial research funder Alberta Innovates, which consists of three sub-committees: Cancer Committee (HREBA-CC), Clinical Trials Committee (HREBA-CTC), and Community Health Committee (HREBA-CHC). The HREBA-CHC is a multi-disciplinary committee with members from both rural and urban Alberta that provides scientific and ethical review of health research proposed to be conducted in communities across Alberta.

When an individual or organization falls under the purview of an REB, REB review and approval is required before research commences when (1) research involves living human participants, or (2) research involves human biological materials (including human embryos, fetuses, fetal tissue, reproductive materials and stem cells) whether from living or deceased individuals (TCPS Article 2.1). The term "involves" is more broadly interpreted than the restrictive "about" that triggers privacy law scrutiny. The bar will not be as high for REB approval as say PIPA or FOIP applicability. Applicants to REBs must complete ethics applications which include detailed descriptions of the research, of adherence to TCPS2 requirements, and

of the research protocol. REBs review these applications and make determinations on whether research should be permitted to proceed, if modifications are required before REB permission is granted, or if research cannot proceed without significant changes requiring a new application.

Failure to comply with the REB process or decisions (i.e. to conduct research without appropriate REB approval) would lead to an institution's loss (not just that of the infringing research group) of all funding from the three national Tri-Council public research funders: the Canadian Institutes of Health Research, the Social Sciences and Humanities Research Council, and the Natural Sciences and Engineering Research Council. This heavy sanction promotes a community of compliance with the TCPS2.

Activity in question must be research to require REB scrutiny before conduct.

The applicability of the TCPS2 and REB review process to an NFP engaging in secondary data use is influenced by several points. First, if any of the parties involved in the data sharing enterprise have affiliations that fall under any of the three Albertan REBs, then the REB process may be triggered. For example, if a university-affiliated researcher is involved in the NFP's plans to collect, use or disclose personal information (or even aggregate or non-identified personal information), then the conversation should be had to examine whether REB approval is necessary. Generally, northern-Alberta university affiliates fall to the HREB; southern-Alberta university affiliates fall to the CHREB; and, cancer researchers, clinical trial researchers, and community-organization researchers fall to HREBA. Other factors may exempt a researcher from REB approval, but affiliation is an important trigger to liability that must be fully considered at the start. Second, the activity in question must be research to require REB scrutiny before conduct; other activities, which could be called quality assurance, program evaluation, or business intelligence, that involve collection, examination and analysis of information do not require REB approval. In the subsequent section, I provide more detail on the distinctions between research attracting REB review and quality-assurance-like activities that do not attract such review and attention.

2.3.2. RESEARCH VS. QUALITY ASSURANCE

The CHREB looks closely at the TCPS2 to ascertain the limits of the definition of research: "where "re-

search" is defined as an undertaking intended to extend knowledge through a disciplined inquiry or systematic investigation. This includes pilot studies (Article 6.11). The term "disciplined inquiry" refers to an inquiry that is conducted with the expectation that the method, results, and conclusions will be able to withstand the scrutiny of the relevant research community" [36]. Quality assurance work does not require REB approval as long as "you are a legal custodian of any personal health information that will be used in the project or already have specific consent from the patients to access their information." These exempt activities are listed in Article 2.5 of the TCPS2 to "include quality improvement, program evaluation initiatives, performance reviews, which are understood to be those things relating to the assessment, management or improvement of a local program" [35]. Under the HIA, REB mandates relate to personal health information, and not all personal information. If one wants their quality assurance work to be considered research (e.g. for funding purposes) under the HIA (s. 27(2)), then the organization or individual must apply to the REB [36]. The CHREB considers research involving human participants that requires ethics review to be "an effort to produce new, generalizable knowledge" [36]. Where a competitive grant is involved, the project is research that requires REB approval (even if the granting agency is not a Tri-Council funder) [36]. On the other hand, quality assurance or quality improvement work can be a published work; so striving for, or achieving, publication on its own will not require REB approval. In cases where a quality assurance, or similar, project has changed focused into research, then it must stop and apply for REB approval: no retroactive REB approval is possible [36].

Research involving human participants that requires ethics review to is "an effort to produce new, generalizable knowledge"

The HREBA-CHC and Alberta Innovates have spurred an initiative entitled ARECCI: A pRoject Ethics Community Consensus Initiative [37]. This initiative has developed a tool and recommendations to support integration of ethics considerations across a range of knowledge-generating health projects, including research, quality improvement, quality assurance, and program evaluation [37]. The goal has been to promote confidence in assessing and managing risks to participants in any knowledge-generating project. ARECCI aims to assist those pursuing knowledge-generating health projects by determining appropriate level of

ethics review, which includes assessing the level of risk to participants and researchers [37].

The Dalhousie University REB has provided a definitive and highly respected table to also assist in distinguishing research from quality assurance and program evaluation (which I will collectively term quality improvement (QI)) [38]. If there is a dual purpose to data collection (both research and QI) and if QI is first, then research use would be a secondary use of data (different purpose than original collection) and one would need REB approval for that secondary use [38]. The Dalhousie table compares research from QI, and considers several factors including: facets and role of hypothesis, aims, audience, theory, transferability/generalizability, participant burden, data collection, presumption of risks and benefits, recruitment tactics, "study" compared to regular services, and response to the question 'would this be done anyways?' [38].

When a study test or question is clearly stated and grounded in theory and existing literature, it is research; meanwhile, QI relates to existing practice or aimed at program innovation or how a program is working [38]. When the primary purpose is to publish results through scientific publication to expand knowledge, then it is research; meanwhile, QI aims to gain information to improve practice or service delivery in particular location [38]. When the primary audience is scholars, practitioners, and organizations beyond immediate affiliation, then it is research; meanwhile, QI audiences are the organization or system being assessed [38]. When generalizability is a clear intention, then it is research; meanwhile, QI is not intended to be generalizable with results focused mainly on specific services or processes, but QI may eventually

Dalhousie University REB has provided a definitive and highly respected table to also assist in distinguishing research from quality assurance and program.

be shared descriptively as experience for learning [38]. When the role of theory is high such that the goal of research is to develop or test theory, then it is research; meanwhile, QI study goals are not focused on theory, although there may be a small role for evaluation or improvement of a program with theory assist-

Projects that do not involve health information and do not have any affiliation to a university fall into a gap wherein no provincial REB is directly responsible.

ing in designing the study [38]. When the additional burdens on participants are present such that participation must be voluntary because additional activities are required, then it is research; meanwhile, QI often involves less such burdens on participants such that participants continue to engage in routine care [38]. When data collection is novel compared to the usual project (although secondary data analysis is research), then it is research; meanwhile, QI data collection is typically not beyond what data is already routinely collected, although some extra data could be collected for internal or external reporting [38]. When the assumption of benefit does not exist because research assumes no benefits, then it is research; meanwhile QI often presumes programs to be effective or beneficial [38]. When the likely beneficiaries are no one or similar individuals in the future once knowledge attained and translated, then it is research; meanwhile, QI aim to benefit participants and the local setting [38]. When participants are from multiple sites and/or use control groups, then it is research; meanwhile, QI involves participants from the practice setting being evaluated [38]. If results would not apply to anywhere else, then the project would not continue as research as research seeks to produce results that would apply more broadly; meanwhile, the QI project would continue as it aims to use information to improve or evaluate that setting [38].

Ultimately, the necessity of REB approval for NFPs projects would need to be determined on a case-by-case basis, accordingly to the facets and factors listed above. Unless a university-affiliated researcher is involved in the project, it would be likely that health-related NFP research projects would need to go to HREBA-CHC for approval. NFP projects that do not involve health information and do not have any affiliation to a university fall into a gap wherein no provincial REB is directly responsible. The goals, methods, activities, information involved, and organizations involved in any data-driven, secondary use opportunity involving personal information originally collected an NFP would inform the discussion as to whether REB approval is required. In cases of uncertainty or clear gap, it would be best practice to either partner with a university-affiliated researcher and utilize their REB, or go to ARECCI and request a review. Also, at the

NFP's that aim to mobilize the data at their disposal should do so with a clear understanding of their legal obligations and legally informed best practices.

start of a larger- or broader- scale secondary use opportunity (e.g. involving more than one NFP, and/or involving a long-term data mobilization vision), consultation with ARECCI would be prudent as it, along with compliance with provincial privacy laws, would ensure a strong, legal foundation for the opportunity and would promote public trust in the NFPs as well as their data-mobilizing tactics.

3. CURRENT OR BEST DATA GOVERNANCE PRACTICES

If one sticks to the letter of the law, there may be many circumstances in which an NFP is not governed by any privacy legislation in its activities, and thus the identifying information provided to it by individuals or the public would be available to them to do so as they please. This capacity to use data can be quite powerful, in many different ways. The data can act as an asset and resource that the NFP could mobilize to better its services and better meet its aims and objectives. In a world where data is considered an innovation and asset, and where many commercial entities especially in social media harvest the data provided to them and leverage it for profit, the public generally and individuals alone are becoming increasingly concerned about their information, who has access to it, and what people are doing with it. The fine balance between privacy and utility is something that all data purveyors have had to contend with for many, many years – even before the invention of many of today's popular social media sites.

There is a vulnerability of data subjetcs which creates new risks with siezing data opportunities.

NFPs that aim to mobilize the data at their disposal, should do so with a clear understanding of their legal obligations and legally-informed best practices. The above legal analysis aimed to clarify those current obligations and practices. This section further elaborates on data governance best practices by providing information on thoughtful, rigourous approaches to data governance and management in the NFP sector. Canadian and international examples are provided; the latter because of the soundness and rigour of the approach to developing such guidance. After detailing the responsible data approach that was derived from a review of several humanitarian organizations' data policies, specific organizational approaches will be introduced to detail the breadth of options and issues to consider for NFPs in determining their data governance approach.

3.1 OVERVIEW OF THE RESPONSIBLE DATA APPROACH

In 2016, a comparative review of data governance approaches was conducted within the humanitarian context [39]. This review particularly considered seven United Nations agencies, seven international organi-

zations, two governmental agencies, and one research institution [39]. The authors argued that "…to create an adequate level of trust and ensure the effectiveness of data-driven innovations across the humanitarian sector, data policies, guidelines and implementation safeguards need to be developed and rigorously tested" [39]. In humanitarian spaces, as well as for most NFPs, there is a vulnerability of data subjects which creates new risks with seizing data opportunities [39].

Organizational data policies can generally focus on the impact of data use, or on responsible use of data to protect data subjects and their rights, prevent liability risk and harm, or ideally both [39]. Although lacking from the reviewed organizational data policies, data policies with value and impact indicators were recommended [39]. These measures would allow organizations to determine whether data use was justified based on the intended deliverables, and fosters appropriate, longitudinal risk assessment, especially when sensitive data is accessed [39].

A data audit system is also recommended in the data governance framework. Data handling must be described to determine risks and to better enforce organizations and users that thoughtfully justify their access and use of data [39]. Development of the audit system allows the organization to determine what data are needed to meet goals or solve problems. Implementation of the data audit system primarily aims to prevent the collection, use or disclosure of data that is unnecessary or nefarious, which increase risks to data subjects and organizations. Data auditing could be via stipulated guidelines (e.g. level of anonymization) or via a data custodian, controller, or auditing body with oversight and accountability responsibility [39].

Risk assessment and mitigation strategies comprise another important component to a data governance policy [39]. Risk assessment fosters the promotion of proportionality between risks and benefits [39]. The available risk assessment strategies in data policies range in likely effectiveness and burden [39]. The least burdensome, but likely least effective, assessment strategies involve statements of the importance of considering risk in data-related activities [39]. Slightly more burdensome and likely more effective strategies would reference particular risk assessment tools [39]. Finally, the most burdensome and likely most effective risk assessment strategy would incorporate and mandate the use of concrete risk assessment tools [39].

Similarly, risk mitigation strategies range in possibilities: prohibitions on types of data use; preventing and limiting data access; security safeguards to avoid unsanctioned data violations; consent requirements; and, the promotion of appropriate data management [39]. Risk mitigation can be at both the organizational and technical level [39]. Further technical procedures to mitigate risks include physical security, access control, data classification, security and encryption [39]. Further organizational procedures in data governance include standard operating procedures; ensuring legal requirements such as reasonable purpose and consent are met; data sharing protocols; and governance mechanisms [39]. Organizations must also include specific measures for protecting privacy of data subjects using technology and agreements to protect against surveillance, inappropriate aggregation, exclusion, confidentiality breaches, inappropriate accessibility, unsanctioned identification of individuals or groups, unapproved secondary use of data, and avoiding data duplication [39].

Data policies should include recognition of the Fair Information Principles and the laws that cover the NFP's jurisdiction [39]. This recognition promotes the definite consideration of legal requirements in the policy and ensures best practices are grounded in community standards set by law [39].

Policies and rules are only as effective as the compliance to them. Data policies should, thus, also contemplate and include mechanisms for monitoring adherence to the policy [39]. Monitoring, like other strategies, can include one or more different facets. The policy should describe these facets. There could be technical monitoring in the database systems as part of the audit system; there could be periodic reports provided to the organizational leaders on data use metrics and any potential risks to data or subjects; and, there could be surprise assessments of the data access process in the line of "secret shoppers" to ensure compliance with policies. Monitoring compliance can root out problems as well as demonstrate successes in data governance and data use.

Another facet to data policies where data is collected directly from subjects includes provisions on dispute resolution and data withdrawal [39]. Data policies should consider the process that will be triggered if data subjects wish to withdraw their data from the organization, either entirely or for secondary data use. This process should include how data subjects will be informed of this policy; how they may make their

preferences known; the implications for previously-collected and to-be-collected data; and, the organizational process to effect this preference. Dispute resolution may be another area to be addressed in the data policy. As described in Albertan privacy law, designation of a privacy or data officer would introduce a point of contact for organizations to deal with disputes. Similarly, the data access protocols should include processes when potential data secondary users wish to dispute access decisions.

The format of the data governance policy is itself quite critical. Enumerating the tasks and responsibilities for enacting the policy and monitoring it are critical [39]. When all actors possess clear roles, it prevents duplication and promotes implementation [39]. Also, in drafting the data policy, tradeoffs must be considered [39]. Greater detail brings clarity, but risks inapplicability to novel circumstances; so, a balance must be found between detail and vagueness [39]. Simplicity is in tension with complexity: the former promotes readability and compliance, but leaves room for questions and possibly divergent policy implementations [39]. Generally, leaning towards greater elaboration of the strategies and values of the policy, in a step-by-step format, promotes understanding, and thus increases the likelihood of implementation [39].

3.2 SPECIFIC ORGANIZATIONAL APPROACHES TO DATA GOVERNANCE

Data governance best practices for NFPs is a novel point of discussion. Many organizations work individually, rather than collectively, to determine their approach to data stewardship and governance to balance privacy protection with organizational and sector utility. The diversity and commonality of these organizations' approaches would be informative to the diverse NFP sector, where organizations vary on resources, data capacity, and data interests. Ideally, organizations will consider the following four examples and the entirety of this report to determine the best, most feasible, approach to data governance as they move forward in seizing data-driven opportunities.

First, Medicins Sans Frontieres (MSF) is a humanitarian, non-governmental organization that adopted a data sharing policy for routinely collected clinical and research data in 2012 [40]. The aim of this policy was to ethically promote the sharing of MSF, and ideally other humanitarian and non-governmental organizations', data with public health researchers for the benefit of the populations that they work with [40]. The precursor to this policy was a public, institutional repository of MSF research publications in the context

of scientific journals prioritizing open access to data [40]. Before this policy was instituted in 2012, MSF used a case-by-case approach to share their data [40]. This policy was developed in consultation with the MSF's own independent Ethics Review Board. Thus, an REB is available to MSF in policy development and in oversight of policy compliance.

Qualified is further defined as having authored relevant peer-reviewed articles and still working in the relevant specialty.

Briefly, the MSF data sharing policy consists of a statement of vision and principles, and then elaborates the data access process [40]. The vision and principles describe the MSF mandate to promote health data sharing, to accrue social benefit in opening up access to data, to move MSF towards greater online data collection, and to prioritize safeguards of patients so that no patients or communities are harmed in the facilitation of data sharing [40]. With the overriding objective to not do harm, the policy mandates that sharing should not occur simply for the sake of sharing, but rather when there is the potential for greater health benefits for populations [40].

The policy begins by defining the data at issue: all health data generated in MSF programs or sites where MSF is the data custodian [40]. This data includes data from patient records, surveys, health information systems, research, and human biological material [40]. The data access process is then the focus of the data sharing policy. Those who can apply for data access include any appropriately qualified researchers from academia, charitable organizations, and private companies [40]. Qualified is further defined as having authored relevant peer-reviewed articles and still working in the relevant specialty [40]. Preference is given to researchers from the countries or communities where MSF works, and especially where the datasets originated [40].

While the policy plans for eventual open access data repositories, managed data access is the policy de-

fault [40]. The procedure for managed access is planned to be proportionate to the risks associated with the data, to avoid undue delay or restrict access [40]. The managed access process includes applications to facilitate assessment of researcher qualifications; consideration of consent issues; and appraisal of scientific merit, potential benefits and risks. The MSF Ethics Review Board must review the applications when the data includes either (a) identifiable data and/or human samples, even when consent was obtained at original data collection; or (b) non-identifiable research data for purposes outside the original consent agreements [40]. For (b), MSF must then attempt to return to study participants to expand their original consent, or if that is not possible, MSF must secure the consent of the community where the study took place [40]. This multi-pronged approach to ethics review and consent appears to be MSF's attempt to ensure valuable previously-collected data is not lost to data sharing while also being respectful of participant and community vulnerability and trust in MSF.

The policy maintains that data sharing must be a cost-neutral exercise, such that data recipients are required to cover all the costs of retrieving, processing and dispatching MSF datasets [40]. Cost exceptions could be possible when data recipients demonstrate insufficient funds [40]. This data sharing policy does not deal with all issues of data governance, but rather establishes a strong foundation for further discussions on data sharing. This policy sets the stage for the use of standard templates including consent to support the development of data sharing plans and proposals [40]. Data policies and approaches must also consider the need to promote data quality and the protection of data from corruption or obsolete software [40]. Data sharing policies must also consider extant agreements that could limit or direct data sharing, such as contractor agreements with public funding bodies (which also introduce other privacy laws).

Second, another exploration of data governance approaches specifically targeted NFPs [41]. Appropriate data governance by NFPs should promote the availability of data that is accessible and current to needs; the usability of data for sound decision-making; the integrity of data that confirms trustworthiness; and the stewardship of data that protects privacy and complies with legal requirements [41]. A data governance framework could be divided into three key components: people, policy and technology. The people-focused facets demarcate authority, accountability and roles in the implementation of data governance, as well as the fostering of a cultural attitude and collaborative environment with respect to data oppor-

tunities [41]. The policy-focused features delineate how information flow is managed; how data policies themselves are managed; how issues are resolved; and how data-related communication is realized [41]. The policies guide decision-making and advance rational outcomes [41] Finally, the technology-focused discussion targets management of data quality, compliance monitoring, data business rules, and process management [41]. The development of a data governance approach should include team identification, as well as a lifecycle-style process wherein goals are identified, policies developed, strategies implemented, progress evaluated, and progress communicated so that the cycle may begin again to consider goals [41]

Third, another organizational data strategy is that of the Ontario Nonprofit Network [6, 42]. This strategy aims to foster data-drivenness and data sharing amongst NFPs in Ontario (and beyond) [6, 42]. This type of policy begins with enumeration of the principles that guide the strategy, including the promotion of effective data use by NFPs, the assurance of responsible and ethical data collection and access to respect privacy, recognize vulnerability and promote safety of the data subjects, and the accrual of public benefit when enabling data access [6, 42].

The succinct data strategy then describes the four components to this strategy: standards, policy, skills and resources, and leadership [6, 42]. The strategy aims for standardization across Ontario NFPs in the publication of their data and metadata, to better facilitate secondary data use. The strategy demarcates the rules and recommended legislation that govern what can be done to the data (or not); that clarify data ownership and cost allocation amongst NFPs; and that secondary data use must benefit public work. The strategy considers tactics to build NFP sector capacity in data use and management. Finally, the strategy aims to foster commitment from leadership at the individual NFP level and at the sector level on investing time and resources to promote data readiness and data sharing.

And, finally, the Vancouver Foundation has taken a copyright licensing approach to promote secondary use of its data and outputs [43, 44]. The substantive portion of the policy itself is succinct: the foundation itself and all grantees must share materials and knowledge via open license under the Creative Commons Open Licenses [43, 44]. This directive is accompanied by a vision statement and policy development history. The Vancouver Foundation intends to promote "sector-wide, intentional sharing of socially innovative

ideas, information and resources among our peers and the public" [43]. Stakeholder consultation and legal analyses were solicited in policy formation [43]. Provisos to the open licensing policy are also elaborated therein including the mandate to not do harm with open access and the recognition of privacy protection, charities' financial viability, and the need to protect traditional and cultural rights [43].

4. CONCLUSIONS

This paper has aimed to provide NFPs in Alberta with an understanding of their legal and governance obligations when considering the secondary use of data that they collect or that they would like to reuse. These findings demonstrate that the law has somewhat limited direct imperatives for NFPs to follow, but this does not mean that NFPs can do as they wish with the data that they collect. Best practices can be derived from the clear legal obligations of other more-regulated sectors, including private sector businesses, public bodies, and health information custodians, as well as from the industry standard best practices from the NFP sector itself.

Data governance and privacy protection represent the two key considerations for NFPs when contemplating the collection, use and disclosure of identifying information, for the purposes of service delivery and possibly secondary use. Privacy laws worldwide are based on the fair information principles, which can be distilled to some key messages: (a) use the minimal information necessary to complete your task; (b) have consent whenever possible for that use; (c) have administrative, technical and physical safeguards to protect the information; and (d) individuals possess the right to access information about themselves and to request corrections of it. Similarly, the trifecta of purpose, reasonableness and minimal extent appear throughout the allowances made by privacy laws in Alberta.

When looking for the exact applicable legislation, a flexible order of importance of privacy laws in Alberta is available:

1) If health information at issue, HIA applies.

2) If personal information at issue (but not health information) and a public body is involved (whether actual or via contracted affiliate), then FOIP applies.

3) If personal information at issue (but not health information) and a private-sector organization is involved, then PIPA applies.

a. When there are cross-border transactions, PIPEDA applies to the cross-border transactions

while PIPA applies to the intraprovincial activities.

b. If the private-sector organization is duly incorporated as a NFP and it was involved in activities of a commercial nature, then PIPA applies to those information-related activities during the commercial activity.

c. If the private-sector organization is duly incorporated as a NFP and it was not involved in any activities of a commercial nature, then PIPA does not apply.

Once the relevant legal obligations are determined, NFPs must then consider current and best practices to data governance. NFP clientele place great trust in their organizations when seeking services and supports. That trust could be severely damaged or lost, if there were privacy breaches or risks of harms because NFPs did not consider client preferences and protections in their use and disclosure of the data. NFPs should develop a data policy that details the goals, vision, activities, and responsibilities the NFP and its staff undertake when collecting, using and disclosing identifying information. These policies vary between NFPs, based on sectors, services, data types, resources and capacities.

Intellectual property laws and privacy laws represent distinct pathways towards data sharing. Copyright licensing represent a valid avenue to make data available, but if blanket policies they may not provide the individual protections necessary when identifying information is at issue. Privacy laws offer guidelines to how to reasonably, and thus equally, balance the individual's right to privacy to the organization's need to use the data that they have. One should not give way to other. In this way, secondary data use when aimed at improving service delivery or outcomes within the NFP sector and its client population, respectively, can be realized without sacrificing individual privacy and organizational trust.

NFPs currently fall into several legislative gaps with respect to secondary use of data including identifying information. For example, privacy laws do not apply to duly incorporated NFPs carrying out non-commercial activities, and research ethics boards are not obliged to review the planned secondary uses of data by NFPs if there is neither university affiliation nor health information involved. Nevertheless, best practices around data governance and privacy protection abound. Societal expectations, ethical practices,

and conservative business approaches all demand that NFPs approach the use and disclosure of data from a legal and governance perspective. Such a perspective demands the development of a data and privacy policy. Such a policy should be formatted to include a vision statement that clearly links to recognized legal requirements and international Fair Information principles, and which details the NFP's expectations around the goals of data sharing and the tensions to balance. The content of the policy should then describe the safeguards in place, the access processes required for secondary use, and the monitoring processes for compliance. Prioritization of consent, "need to know" directives, and reasonableness would promote compliance with privacy laws. Roles and tasks could be enumerated to promote effective implementation.

Table 1. Key Obligations of *PIPA*

Ten Key Obligations to Meet Under *PIPA*

1. Personal information handling practices, policies and procedures should be developed to protect personal information, which should cover
   a. What personal information is collected (and ensuring that collection is for a reasonable purpose and only information is collected that is reasonable for carrying out those purposes (s.11));
   b. How is consent obtained for the collection, use and disclosure of personal information;
   c. How will personal information be used and disclosed;
   d. How will adequate storage and security measures be implemented;
   e. How will personal information be disposed of;
   f. How will access and correction requests be handled; and,
   g. How will enquiries and complaints be responded to?
2. The privacy and information handling policies should be reviewed periodically, and should address ongoing and new activities that involve personal information collection, use, disclosure or storage.
3. The privacy and information handling policies should be available and communicated to employees, volunteers and other organizational staff, as well as to the public including the audience or clientele of the organization. Such communication could include staff training, pamphlets and brochures, and website information.
4. A privacy officer should be recognized, designated and supported to exercise the authority to address privacy issues related to the organization and its operations. Internal and external communications should make the identity and contact information of organizational privacy officer readily available, especially at the time of garnering consent for information collection.
5. All contracts and agreements should include a privacy protection clause, so that any contractor of the organization protects personal information according to the organization's privacy and information handling policies.
6. Unless *PIPA* specifically exempts, organizations must get informed consent to collect, use or disclose personal information. In gathering consent, organizations must adequately inform individuals of the purpose for information collection, as well as the proposed and potential uses, disclosures, storage and disposal of the information. Only reasonable purposes and methods of collection can be consented to; an individual cannot consent to unreasonable collection of personal information, including any extra information disclosed that is not needed for the purpose. Consent can be express (written or verbal), implied (information is volunteered in reasonable and clear circumstances), or opt-out (organizations provide individuals with the reasonable purpose of their need for personal information; with easy-to-understand notice that consent will be imputed if they do not opt-out; with a reasonable window and chance to say no and opt-out; and with assurance that the personal information is not so sensitive it would be unreasonable to use an opt-out form). Consent can be changed or withdrawn by the individual by giving the organization reasonable notice, unless a legal duty or obligation would be interfered with (s. 9). The consequences of altered or withdrawn consent should be explained to the individual. Consent to collect, use or disclose personal information cannot be a condition for an organization to supply an individual with a product or service, if the information at issue is beyond that necessary to supply the product or service.
7. As per fair information principles, organizations should limit the collection of personal information, by amount and type, to the minimum necessary to carry out the organization's obligations.
8. As with information collection, private sector organizations may only use or disclose personal information for reasonable purposes and must limit information use to the minimum necessary to reasonably carry out those enumerated purposes.
9. Some exceptions to the necessity of consent prior to information collection, use or disclosure include when consent cannot reasonably be obtained in a timely manner or an individual would not reasonably be expected to refuse consent but it would

reasonably be considered in the individual's interests; when another statute or regulation requires or allows for information collection without consent; when the information is provided by a Public Body by law; when information collection is reasonable for the purposes of a legal investigation or proceeding; when the information is determine suitability for an award or honour; when the personal information is publicly available; when collection is by an archival institution or for reasonable archival purposes; when information pertaining to debt collection from, or debt repayment to, the individual; and, when information given to credit reporting agency to create credit report and individual originally permitted such disclosure. A few additional exceptions to consent for disclosure exist, which include when disclosure is required to comply with a subpoena, warrant or court order; when a Public Body or police service require assistance in investigation related to a law enforcement proceeding; when disclosure is in response to an emergency that threatens the life, health or security of an individual or the public; when disclosure is required to contact a family member or friend of an injured, ill or deceased person; when disclosure is reasonable as relates to the surviving spouse, adult partner or relative of a deceased individual; when disclosure protects against, prevents, suppresses or detects fraud.

10. Where personal information relates to employees and is what is reasonably needed to establish, manage or end a work or volunteer, that information can be collected, used and disclosed without consent for reasonable purposes related to recruiting, managing or terminating personnel. Managing personnel is related to human resource management duties and responsibilities as well as administering personnel (e.g. payroll, succession planning). Personal information not related to the work relationship is not subject to this employment-related exception to consent. The work relationship covers both when the individual is an employee, and when recruiting a potential employee. While consent is not required, notice is required when collecting employee information for employees; such notification is not required during recruitment [13, 21].

Table 2. *PIPA* Requirements around Access to Information Rights

Issues	Details
Requests	• Individuals who make requests for access are applicants. • Applicants must provide enough information to the organization, so that the organization can make a reasonable effort to find the information. • Normally requests are made in writing, especially for larger organizations. Organizations can choose to accept oral requests, if the applicant cannot put the request in writing or if they are a smaller organization. • Requests for access to information include either viewing/seeing the information or receiving a copy of the information. • Requests do not have to include a reason for the request.
Organizational Response to Requests	• The organization must respond within 45 calendar days of receiving the request. • Organizations may implement a process for access requests, including an office to receive requests and a time limit for processing a request would not begin until the request arrived at the designated office. • Unless the record does not exist or there is a statutory refusal available, the Organization must (1) give the individual access to his or her personal information; (2) tell the individual what the information has been or is being used for, and (3) tell the individual to whom, and in what situations, the information is being or has been disclosed by the organization. • The organization must be guided by reasonableness in their dealings with an access request. This includes being open, complete and accurate in your response to applicant. • Reasonable fees can be charged for access to personal information or to information about the use or disclosure of that information. But, organizations cannot charge employees for access to employment information. Written fee estimates must be provided before organizations process a request. Deposits can be required. Records can be withheld if fees are owing. • The 45-day clock stops once an estimate is provided to the applicant, and does not start until estimate accepted and deposit received. If the applicant does not respond within 30 days of when the estimate was given, then request considered withdrawn.
Authorized Representatives	• Those over 18 years of age can exercise all rights under *PIPA*. Minors can act on their own behalf if they understand their rights and powers, and the consequences of exercising them under *PIPA*. • An authorized representative is another person who has the authority to do what the individual can do under *PIPA*. They include (a) a guardian of a minor; (b) an executor or administrator of the estate of an individual who has died; (c) a guardian or trustee of a dependent adult; (d) an individual acting with the written authorization of an individual; and (e) an individual who is acting under a power of attorney.

Exceptions to Giving Access	• An organization can refuse access in select situations, such as:
	  • When information is protected by any legal privilege
	  • When disclosure would give away confidential business information, and it is not unreasonable to hold back the information
	  • When the information was collected for an investigation or legal proceeding

- When disclosure might result in that type of information no longer being supplied and it is reasonable for the organization to need the type of information
- When a mediator or arbitrator collected the information

- An organization MUST refuse access if disclosure:
  - Could reasonably be expected to threaten the life or security of another individual;
  - Would show personal information about another individual; or
  - Would identify the individual who gave you an opinion about someone else in confidence and the individual giving the opinion does not consent to the disclosure of his or her identity. You can hold back the identity of the person who wrote the opinion while still giving access to the opinion itself, unless the applicant could figure out who gave the opinion by reading it.

Table 3. OIPC interpretations and uses of "use" and "disclose" in *PIPA*, *FOIP*, or *HIA* complaints' adjudication.

OIPC#	Year	Defendant	Complaint	Discussion on "collect"	Discussion on "use"	Discussion on "disclose" or "disclosure"
F2012-05	2012	Workers' Compensation Board	• Public Body (PB) collected and used information from third party about Complainant. • That information was used to determine Complainant was (a) not "dependent" under legislation; and thus (b) unentitled to deceased husband's pension.	• PB investigators under *Workers' Compensation Act* "may collect any information that could reasonably be said to be related to the matter under investigation and potentially relevant. It need not ultimately be proven to be relevant in fact." [para. 30]. If investigators working in good faith, then should be free to collect all potentially relevant information. • Indirect collection was authorized under the *WCA* [para. 33].	Arguments: • PB argued that information was not "used" because it was not "relied upon to make the determination" at issue (dependency issue). • Complainant argued that PB continues to "refer" to contested information and thus cannot argue that did not use. Decision • When information included in the writing of the decision letter, contested information was "used", even if given little to no weight in decision [para. 39]. • This use was either to make determination or to at least thoroughly document evidence reviewed [para. 41]. • The use was logically related to the purpose for which the information was collected (investigation of Complainant's claim under *WCA*) [para. 41]. So, authorized "use" under *FOIP* [para. 42].	• Disclosure of personal information is either specifically authorized under *FOIP* or is not; "the possible negative impact of the disclosure is not a factor in determining whether the disclosure was authorized" [para. 47]. • When PB discloses information to a representative in their capacity as agent for the Complainant (Complainant authorized representative to act in their stead and request PB to communicate via representative), then it is an authorized disclosure [para. 49]. • Signed authorization form equates to consent [para. 50]. • Disclosure by PB to Appeals Commission upon request, which was directly authorized by the *WCA* [para. 51].
F2013-31	2013	Central AB Child & Family Authority (Region 4)	• Complainant complained her PB employer collected, used and disclosed her personal information contra *FOIP*.	• PB collected personal information directly from Complainant (doctor's notes), so in compliance s. 34 *FOIP* [para. 9]. • Managing employees is "an operating program or activity of the PB" per s.	• "Same considerations apply whether it is a use or a disclosure" [para. 13]. • Very strict inquiry into whether information used or disclosed, not the	• The sharing of the first Dr's note from original recipient (Office Administrator) to Office Manager and to Complainant's Supervisor was disclosure [para. 20]. It was for valid purpose of

			• Notes from physician excusing Complainant from some physical tasks due to her medical condition were shared with PB supervisors, only one of whom was supervisor of unit where Complainant asked to work (but couldn't). And, Complainant was asked questions about her medical condition that refused to answer; meeting with Supervisor and Office Administrator.	33(c) *FOIP* [para. 10]. Personal information in Dr's notes related to medical condition and what condition prevent her from doing; so directly related to job duties. • No personal information collected in meeting because (a) personal information in *FOIP* is recorded information, and no recorded information collected in meeting; (b) Complainant refused to answer questions so no collection [para. 11].	official protocol in place or not [para. 19]. • Same considerations regarding use and disclosure (i.e. for purpose of managing or administering personnel; at minimal necessary). • Proper use of personal information.	managing personnel [para. 20]. • Similar disclosure for second Dr's note when provided to other management. Again valid purpose of managing personnel [para. 21]. • Inconsistency between PB Supervisor witness testimony and Complainant speculation that second Dr's note shared with other (horizontal) Supervisors. OIPC took witness testimony that note contents not discussed, rather just limited information that Complainant could not cover other duties and to plan staffing accordingly. Managing personnel purpose valid.
F2013-32 & F2013-33	2013	City of Edmonton	• PB showed Complainant's neighbor copy of building plans for Complainant's new house and provided copy of plans. • Complainant complained this infringed *FOIP*. • This decision involved first OIPC adjudication; judicial review; second OIPC adjudication.	• Re: access: PB must search for records that are in its custody and control [para. 10].	• Not applicable.	• Judicial review of first OIPC adjudication indicated that cannot use *PIPA* definition of "personal information" to interpret *FOIP* "personal information: the two Acts have different purposes and *PIPA*'s definition defined to be much broader than that of *FOIP* [para. 23]. • *PIPA* PI = information about identifiable individual. *FOIP* PI = recorded information about identifiable information including several specific parameters.

						• *FOIP* intended to foster open and transparent government [para. 26]. • Judicial review also found that "exclusion from the presumption of "unreasonable invasion of personal privacy" does not necessarily mean inclusion in the definition of "personal information" [para. 29]. • Issue more if building plans were personal information under *FOIP*: second OIPC adjudication found they were not personal information because "… the particular external features of the building that are revealed in the plans … are sufficiently commonplace … that they do not reveal anything sufficiently personal about [Complainant] to make the plans more 'about' her than they are 'about' the building." [para. 34]. • Since the information is not PI, then no need to determine if disclosed contra *FOIP*. But, first OPIC adjudication found that building plans were PI and in showing to neighbor, it was disclosed contra FOIP.
F2015 -42	2015	Alberta Human Services	• The Complainant made a complaint to the Commissioner that the PB had collected his personal	•	•	• The Adjudicator found that the Public Body had contravened Part 2 of the FOIP Act when it collected the Complainant's personal information from the

			information from the JOIN database. • He complained that the PB had collected information about an offence taking place when he was a youth and historical allegations about him that did not result in convictions. • The Complainant alleged that Human Services then used the information it obtained from the JOIN database to make decisions regarding his employment. • He complained that the PB disclosed his personal information to its human resources department and to a member of the Edmonton Police Service (EPS). He complained that the PB's use and disclosure of his personal information are in contravention of Part 2 of the FOIP Act.			JOIN database, when it had used this information, and when it disclosed this information to its Human Resources Division. She also found that the Public Body had not established that its disclosure of the Complainant's personal information to the EPS member was in compliance with Part 2 of the FOIP Act. The Adjudicator ordered the Public Body to stop collecting, using, and disclosing the Complainant's personal information in contravention of the Part 2 of the FOIP Act.
F2014 -42	2014	Calgary Policy Service	• PB policy officer revealed information	• Not applicable.	• Not applicable.	• Section 4(1) of *FOIP* excludes some

			about the terms of a Recognizance, a Certificate of Analyst, and a Notice of Intention to Complainant's parents. • Complainant argued his PI disclosed in contravention of *FOIP*.			information from *FOIP* information related to court file (judges and courts) (a) and related to prosecution that has not been completed (k). • AB Court of Appeal and this OIPC adjudicator both agree that s. 4(1) exemptions apply to entirety of *FOIP*, so both access to information and protection of privacy provisions. • Recognizance was signed by a justice of the peace; information relayed to parents by policy officer orally but source was Recognizance; thus, policy officer disclosed information; but the information and disclosure both exempted from *FOIP* per s. 4(1)(a) [para. 18]. • The Certificate of Analyst and Notice of Intention from Crown prosecuter via PB: "… serving the Applicant with these records was a step taken to further an ongoing prosecution and … the records relate to the prosecution" [para. 19]. • Prosecution was ongoing. Section 4(1)(k) intended to ensure that prosecutions may proceed without interference. Information in latter two records related to prosecution not yet complete. So, records and disclosure fall within s. 4(1)(k) exemption to *FOIP* [para. 22].

F2016-62	2016	Alberta Health Services	• An invoice containing Complainant's PI was given to her by a co-worker. Then PI about her leave/suspension was shared with other PB employees (carrying an unsealed envelope for delivery). PB was her employer. • Complainant argued these were uses or disclosures of PI in contravention of *FOIP*.	• Not applicable.	• Analysis by OIPC adjudicator was around whether this was disclosure, authorized or not?	• Information at issue was PI (name, title, salary, information on suspension/leave). • Disclosure is about whether the other [coworker in this case] "was able to view the information", not whether they actually did view the PI or not [para. 12]. • First disclosure to coworker in carrying invoice was not authorized because coworker did not need to see details of invoice to reimburse Complainant or even to advise Complainant that claim approved [para. 21]. • Second disclosure to communications and education personnel in preparation of newsletter. This was use and disclosure as it was information sharing [para. 25]. • Second disclosure was more information than reasonable to meet its purpose: goal to take down article about Complainant on site and replace article so they did not need to know of her suspension/leave [para. 32].
F2012-22	2012	AB Justice & Solicitor General	• AB Justice & Solicitor General (JAG) disclosed 3 letters of Complainant's medical information and information of WCB claims to AB	• Not applicable.	• Not applicable.	• Initial burden of proof on complainant to adduce evidence regarding what PI was disclosed and how it was disclosed. The public body has budento show disclosure was according to *FOIP*.

			Corporate Human Resources (CHR). • Complainant argued this was improper disclosure per *FOIP*.			• Obtaining an individual's consent for disclosure is only one of the ways a PB can have the authority to disclose the individual's PI [para. 18]. • JAG was authorized to disclose PI to CHR in letters because relevant to determine whether and how to request further medical assessment, which CHR could assist JAG with. Information sharing related to human resources management between JAG human resources staff and CHR similar staff. This reasonable purpose and fits under *FOIP* [para. 21].
F2012-23	2012	Alberta Corporate Human Resources	• Connected to F2012-22 • AB Corporate Human Resources (CHR) collected 3 letters of Complainant's medical information from AB Justice & Solicitor General (JAG) and provided this PI to LifeMark Occupational Services/LifeMark Health Services (LM). Letters detailed medical information and claims information regarding her claim to WCB. • Complainant argued this contravened *FOIP*.	• CHR's collection of Complainant PI from JAG had not contravened *FOIP*. CHR has authority to collect PI under s. 33(c) as information related directly to and was necessary for an operating activity of CHR. CHR is responsible for advising and assisting government departments in human resource matters; herein JAG required advice and assistance on assessing Complainant's functional capacity to determine her ability to perform previous tasks [paras. 16-17]. • "… a public body is entitled to considerable latitude in deciding that the collection of personal information is necessary in a given case, and that its decision should not be interfered with unless	• Not applicable.	• PB is authorized to disclose PI, in absence of individual's consent, on basis of any of the purposes or circumstances set out in s. 40(1) *FOIP*. • "Even if the exchange of information within a PB might be characterized as a use of information, LM is a third party vis-à-vis CHR. [para. 31]" CHR argued LM was employee of CHR, but Adjudicator found LM as a third party service provided. • ".. when deciding whether the purpose of a use or disclosure of PI is the same as or consistent with the purpose of collection, one should examine the specific purpose; otherwise, a PB would have too wide a latitude to use and disclose PI simply

				patently unreasonable. [para. 17]" • The letters consist of PI because contain name, information about health and health care history, information about employment history, and others' opinions about her [para. 12]. • This collection was indirect (via JAG), which is in compliance with s. 34 (PI may be collected indirectly or must be collected directly from the individual in question) [para. 23].		by characterizing the purposes broadly enough." [para. 34]. • While collection of the PI in the letters enabled the CHR to provide advice and assistance to JAG, the adjudicator found "that disclosure of the information to LM was not necessary in order for CHR to actually arrange, and obtain the results of, the [functional capacity examination]." [para. 36]. LM's assessment was relatively limited, so it did not require so many details about Complainant's medical condition or anything about her WCB claims to carry out the FCE. • This disclosure to LM had no reasonable and direct connection to CHR's specific purpose of arranging the FCE; at most an indirect connection existed. CHR collection from JAG was to determine if FCE appropriate; once FCE determined appropriate, CHR disclosure to LM was only reasonable to extent to actually arrange FCE [para. 37]. • Disclosure was not consistent with purpose for which they were collected from JAG, per s. 41 *FOIP*. • Complainant signed consent form with LM to collection of health history; but, this consent

						only covered collecting information from her in course of FCE, not from CHR prior to FCE [para. 40].
F2012-28	2012	Edmonton Police Service	• Complainant name and license plate number used to run queries on police information systems by various PB members in 2008 and 2009. 72 queries, mostly 2 queries in single occasion. • Complainant alleged some queries lacked authorization by s. 39 *FOIP*.	• PB may use PI for purpose it was collected or complied, or for us consistent with that purpose (s. 39(1)(a)) [para. 6]. • Here, appropriate purpose would be law enforcement purpose or for purpose relating to and necessary for an operating program of PB. Also, extent of its use must be necessary to enable PB to carry out its law enforcement purposes in a reasonable manner. • In this case, Complainant had altercation with police officer; steps taken for officer's safety; related to Complainant driving. • Several queries had law enforcement purposes as they related to officers moving the claim against Complainant forward or to determine Complainant identity etc.. to ensure he complied with not going near high school he was not to go near and to assess him because he was listed as an officer safety concern. • Most contentious queries by police officer victim who queried Complainant on date of Complainant acquitted of charges. Adjudicator said actions somewhat premature for law enforcement purpose and not extent necessary to carry out law enforcement	•	• Second issue, rather than framed as appropriate use/disclosure was whether PB made reasonable security arrangements against such risks as unauthorized use. • "remarks" fields in database for query should be given because superior evidence to that of a plausible explanation as to why query conducted, together with an attestation of usual or invariable practice of conducting queries for authorized purposes [para. 40]. • OIPC required a great deal of oral testimony and discussion on the recording of specific reasons for the query because that is "an important element of reasonable security measures, in that it both requires the reason to be formulated clearly before the query is done (which could dissuade inappropriate queries), and enables an audit after the fact that can draw on direct evidence of the reasons, as opposed to conjecture. .... If the reasons, or absence of reasons, cannot be determined, there is no disincentive for members

				purpose in a reasonable manner [para. 20]. • 21 queries where no reason provided but affidavits that they were assigned to patrol or canine unit; that not acquainted with Complainant; that there were usual reasons why queries conducted; and that their usual and invariable practice was to conduct queries only for police purposes. None of queries for vehicle stops. But, the timing and order of the queries suggests they were innocuous in a way that refutes suggestion that Complainant was specifically and inappropriately targeted [para. 35].		to use the tool for inappropriate purposes" [para. 63]. • For Complainant, all queries were proper and nothing of these queries suggests the system is failing, so no reason to question whether s. 38 being met [para. 67].
F2013-55	2013	Workers' Compensation Board	• PB collected, used and disclosed information from medical consultants within PB in determinations for an ongoing claim with the PB regarding workplace injury. Questions regarding injury and ability to return to work. • Complainant argued PB not authorized (or ought not to be authorized) to rely on the opinion of medical consultants in making a determination regarding her claim.	• The medical consultants are contract not salaried employees of PB; they perform functions of PB on behalf of PB; and memos written on letterhead of Medical Services area of the PB. Thus, they are PB employees for purposes of *FOIP* [para. 16]. • Collection of Complainant PI by medical consultants is collection by PB, as performed in course of job duties [para. 16]. • Must give deference to PB to determine what information necessary to properly determine claim; indirect collections permitted with this deference as they relate to claim determination [para. 29].	• PB sought out opinions from medical consultants. "Even if these opinions were given little to no weight in reaching a decision about the Complainant, they were incorporated into the Complainant's claim files; I find that the opinions were used for the purposes of *FOIP* Act" [para. 32]. • Section 41 *FOIP* lists when use or disclosure of PI is consistent with purposes for which it was collected (reasonable and direct connection to that purpose; necessary for performing legally authorized duties) [para. 34].	• Similar argument for disclosure as for us. PB disclosed Complainant's PI to medical consultants for consultants to form informed opinion regarding Complainant's injury. Deference given. All disclosure for reasonable purpose and not more than necessary [paras. 37-39].

					• No evidence that PB used Complainant's medical information in authorized manner or beyond extend necessary to make claim determination [para. 35].	
F2012 -27	2012	Holy Family Catholic Regional Div No. 37	• PB lawyer revealed information (PI via doctor's referral letter) to Complainant's lawyer about matter before OIPC when lawyer was not representing Complainant in that matter. The lawyer represented Complainant in separate employment-related court action; while the issue before the OIPC related to an access request for a referral letter and wherein the Complainant was self-represented. • Complainant argued this was disclosure of his PI contra *FOIP*.	• When the PB received the Complainant's letter to the FOIP Coordinator, it collected the personal information that the letter contained (including fact that Complainant made access request for referral letter and fact involved in OIPC file) for the purpose of court action, and also for purpose of OIPC file [para. 28].	• Not applicable.	• Complainant did indicate that he sought access to the referral letter to give to his lawyer regarding the court action. Also, the referral letter was for use in a proceeding before a court to which the PB was a party, so authorized under s. 40(1)(v) *FOIP* [para. 8]. • PI under *FOIP* must be "about" an individual. "The term "about" in the context of the definiton is highly significant restrictive modifier, in that "about" an individual is a much narrower idea than "related" to an individual; information that is generated or collected in consequence of some action on the part of, or associated with, an individual – an that is therefore connected to him or her in some way – is not necessarily "about that individual. [para. 13]" Where PB lawyer discussed the OIPC file as resolved in the letter is about the file, not about the Complainant so not PI. Only PI disclosed by PB were that he made access request and involved in a OIPC file; but, these were authorized [para. 16].

						• Complainant letter to FOIP Coordinator referred to the court action; thus, Complainant linked these two actions. Correspondence by PB lawyer must only be to Complainant lawyer (Lawyer's Code of Conduct) and would only be coherent and understandable if referred to referral letter and OIPC file [para. 26]. • The disclosure was consistent with one of the purposes for which the Complainant's letter was initially collected (the court action), thus the PB was authorized to disclose under s. 40(1) (c) [para. 28]. • The disclosure was only to the extent necessary to enable the PB to respond to the Complainant's letter in a reasonable manner (it complete the discussion) [para. 31]. No superfluous or extraneous information that PB should have redacted; and, letter references the only coherent and sensible way to address points Complainant had made [para. 32]. • While direction of communication between lawyers guided by Law Society of Alberta Professional Code of Conduct; the content of the discussion and any disclosure of PI guided by s. 40(1)(c) of *FOIP* in that

						disclosure must be for purpose consistent with purpose for which information was originally collected from the Complainant. With these both, PB authorized to disclosure information to Complainant lawyer [para. 40].
P2013-03	2013	Project Porchlight	• Complainant employer traced personal telephone calls made using a Blackberry device provided to him by the organization. Complainant alleged that breached *PIPA* along with alleged failure to secure his PI contained in his employment offer letter and tax forms.	• Organization was incorporated under Ontario legislation as not-for-profit non-share capital corporation; but, not in Alberta, so it was not a not-for-profit and thus not exempt from *PIPA*. It is an organization; thus subject to *PIPA* regarding all PI that is collected, used and disclosed by it [para. 16]. • Organization called certain numbers on the Complainant's call list invoice so as to ascertain the recipients of the calls and the nature of the calls [para. 23]. This was collection of information [para. 26]. Organization used this information because arranged meeting with Complainant to chastise him for making the telephone calls [para. 26]. • This information was personal information (not personal employee information) because it included identities of certain recipients revealed to be his friends and/or family and the nature of at least one call revealed one of his interests of a highly personal nature. This information was	• Same analysis for collection and use. • "If an organization does not have the authority to collect and use particular personal information, it necessarily collects and uses the information for purposes that are not reasonable, and there can be no possibility of collection and use to a reasonable extent." [para. 59] • Also discussed reasonable security: "An organization has the burden of proving that it made reasonable security arrangements to protect the personal information that is in its custody or under its control, as it is in the best position to provide evidence of the steps that it has taken." [para. 68] Asking an employee to recomplete an annual form does nto mean that it has lost/misplaced/insecurel y handled previous information. Organization maintains personnel records in a secure file location at its head office. That sufficed	•

				"about" the Complainant as an identifiable individual [para. 27]. • Adjudicator found there was no "acceptable use" policy that restricted the ability of the Complainant to make personal calls using the Blackberry, and there was therefore no such policy incorporated into his employment agreement. This meant, there could be no possible breach of the Complainant's employment agreement, no investigation, and no ability for the Organization to rely on ss. 14(d) and 17(d) to collect and use the Complainant's PI [para. 41]. • An organization might be able to collect and use information regarding recipients and nature of phone calls made by employee using employer-issued communications device (ss. 15, 18 *PIPA*) if (a) it is reasonable for organization to collect and use the information for the particular purpose; and (2) the collection and use of information in question must relate to the employment relationship or be for purposes of managing the employment relationship [para. 46]. • Just because employer unilaterally chooses to do something regarding an employee does not automatically make the employer's act something relating to employment	for reasonable security for adjudicator [para. 70].	

				relationship or management of that relationship [para. 47]. • No consent or prior notice had occurred in this case to permit collection and use of PI. [para. 52] • • Organization ordered to stop collecting and using PI in contravention of *PIPA*.		
P2013-01	2013	Professional Drivers Bureau of Canada Inc.	• Organization Gathers information about truck drivers from their employers, and then makes this information available by subscription to its clients, which include other employers or prospective employers of truck drivers. • Complainant requested access to her PI; and asked OIPC to review Organization's response to her and made complaint regarding the Organization's collection, use and disclosure of her PI.	• The information at issue was PI as it contained her license number, date of birth, social insurance number, height, weight, etc… . The Organization provided no submissions for this inquiry. • That "… the Organization has custody of the records establishes that the Organization has collected and used the Complainant's personal information within the terms of s. (1)(k) [of *PIPA*]" [para. 20]. • Although the personal information was originally collected and used for purposes of either establishing or managing employment relationship, there was no employment relationship between Organization and Complainant. So, this is not personal employee information. So, no exceptions to consent for disclosure available (i.e. ss. 14, 15 and 21). [paras. 22-23] • Although the Organization calls itself an association, the organization is a corporation, and distinct	• Same as collection discussion.	• The evidence contained on Organization's website base finding that Organization has collected, use and disclosed the PIof the Complainant (and other truck drivers) [para. 25]. Organization gathers employment history about truck drivers and gives access to this information to trucking companies that pay subscription fee [para. 27]. Information kept in paper files and in a database [para. 29]. Reports they produce contain driver's employment history with employers, the employer's opinions, the employee's driver's license, and birthdate [par. 29]. "The Organization collects personal information about truck drivers from trucking companies, uses this information, by creating a file and adding it to its database which it will offer for purchase, and discloses the PI to clients when they request a report and pay for it" [para. 29].

				from the organizations that submitted the Complainant's PI to it [para. 30]. • The Organization did not obtain consent from Complainant in circumstances where it was necessary that it do so, and had not provided notice of its collection [para. 35]. The consents Complainant entered into when applying to a trucking company were not extended to the Organization and did not authorize the trucking company to disclose the Complainant's PI to the Organization so that the Organization could use it for its business or disclose it further [para. 35]. Authority to check references does not authorize this third-party Organization to collect, use or disclose PI. • A hand-written consent after the Organization has collected PI did not suffice for OIPC Adjudicator. Also, the consent for Organization to conduct reference check "cannot be interpreted as authorizing the Organization to collect the kinds of information that it has collected" (very personal information such as height, weight, SIN) [para. 39]. • No statutory exemptions applied to Organization getting consent. • Reasonableness of collection requires that collection actually meet the purpose for which it is intended		• Organization had not established that it had collected, used, and disclosed only the personal information necessary for meetings its purposes. So, Organization had breached *PIPA* in all regards and ordered to cease collecting, using and disclosing personal information of Complainant in contravention of *PIPA*. • Because no evidence that established a reasonable purpose for collection and use of Complainant's PI, then no evidence to establish that disclosures were for reasonable purpose.

				[para. 50]. Because Organization did not make submissions for inquiry; website and records alone could not correlate the information that was collected with the purpose in collecting it. Cannot find that Organization trying to combat fraud in collecting PI, so distinguishable from legal cases (e.g. *Leon's*). [para. 52]. • Organization had not established that it had collected, used or disclosed the Complainant's personal information only for reasonable purposes. Because Organization did not explain purpose, then cannot establish a reasonable purpose [para. 55]. • Since Organization collects PI from trucking companies not Complainant directly, then must be within s. 12 (information at issue may be collected without consent of individual under s.. 14, 15 or 22). Since consent must be obtained for PI at issue, then contravene s. 12 [para. 68]. • Section 13 requires notice of purpose of collecting PI and name of someone who answer's for Organization any questions about collection.		
F2013-06	2013	Service Alberta	• Employee of Sentinel Registry disclosed the Complainant's address to an individual who had then gone to the address with the	• Not applicable	• Not applicable.	• The PI at issue disclosed from a registry maintained by PB; so if information is in the control or custody of a public body, such as Service Alberta, then *PIPA* does not apply. *FOIP*

			intention of harassing or confronting the Complianant. OIPC previously determined that *FOIP* applied. • Complainant complained of improper disclosure. • GET FROM PAPER AT HOME.			applies as this is personal information disclosed from MOVES database. • Registry employee disclosed PI without authorization, contrary to PB's policies and procedures. SO, PB did not disclose Complainant's PI. Disclosures by rogue employee, not PB [para. 10]. • PB had not taken adequate measures to monitor manner in which Registry employees accessed PI from MOVES database.
F2013-01	2013	Edmonton Police Service	• PB's previous policy included that website posted copies of disciplinary decisions involving its members. • Applicant ongoing request to PB for copies of disciplinary decisions not posted on website. PB responsed but severed large portions per FOIP.	• Information at issue was personal information as it related to content of disciplinary decisions, 3 parties' names, ages, sex, marital status, h/c and employment history, and opinions about them [para. 8].	•	• In its decision as to whether to withhold or disclose records responsive to request, PB not taken into account all relevant factors especially that disciplinary decisions in this inquiry were read aloud, publicly, at hearing's conclusion. • S. 17 FOIP relates to disclosure harmful to personal privacy (withhold because disclosure would be unreasonable invasion of the third parties' personal privacy). • Much of severed information was not medical information (which would be unreasonable invasion if disclosed). • S 17(5) requires consideration of any overriding factors weighing in favour of disclosure. Previous decisions found that

						desirability of subjecting actions of a police service to public scrutiny overrode presumptions against disclosure and any possible reputational harm [para. 19]. • Verbally disclosing content of written record = disclosure under FOIP [para. 33]. Thus, PB disclosed decisions to any member of public present, member of media present, who may have then disseminated this information further. • BC OIPC decision: prior public disclosure by PB of info sought in access request overrides presumption that disclosure would be unreasonable invasion of a third party's personal privacy. [para 36-37] • ABQB: principle that when police disciplinary hearings are held in public, there is no expectation of privacy. • Any reputational harms or future employment harms to subjects of the disciplinary hearings (affected 3rd parties) on disclosure would have been there anyways because of the disciplinary hearing and not unfair to disclose if they had in fact breached police regulations/codes. So these factors did not mitigate the disclosure.
F2013 -02	2013	Grande Yellowhead	• Complainants successfully sued for	•	•	• Implied undertaking not to use information

		Public School Division No. 77	defamation by Alberta Teachers' Association, principal and teacher at school their son attended. • Complainants complained PB disclosed their PI to ATA contract FOIP.			disclosed through a pre-trial discovery process applied to much of the information at issue. OIPC only dealt with info in Complainant's possession as result of access request made to PB by Complainants. • Info given by PB to ATA as part of the pre-trial discovery process. Consider PI becaue Complainants' names, marital status, opinions about Complainants and Complainants' personal views or opinions. • Issues with submissions from PB. • Justification for disclosures made at trial of defamation claim by PB because Notice to Attend submitted. BUT, not justify disclosure of records prior to the trial. • OPIC found that Complainants' PI was disclosed to ATA by PB employees (either superintendent or principal) [para. 38]. Both members of ATA but only principal was party to litigation. • FOIP: governs the actions of public bodies, not individuals. So when individual acting as head of a public body, then FOIP applies but not when acting in personal capacity [para. 44]. • Teachers' rights to not be defamed, weigh

						powerfully in favour of disclosure of PI. [para. 58] Disclosure important to determination of rights.
P2013-08	2013	Sobeys Group Inc.	• A foreman of Organization called her to ask about her absence from work; foreman told her that he had read her personnel file and read to her information from the file about her disability claim made to her insurance company. A friend of Complainant also called her after foreman had told friend about Complainant's disability claim. • Complaint that Organization had improperly collected, used and disclosed PI while Complainant on medical leave. • Organization did not participate in the inquiry.	• use	• Complainant's description of conversations with foreman and friend met initial burden of proof regarding use and disclosure [para. 12]. • PI/PEI used when foreman accessed her personnel file and discussed the disability claim status with Complainant. • Because no submissions, unclear why foreman would need to see entire insurer letter and details; rather than limited to know that disability claim denied. [para. 29]. • But, this info also PI. Could be exempt from consent under s. 17 PIPA under specified circumstances. But, no evidence from Organization so found that no authority to use PI without consent.	• Foreman disclosed PI/PEI when foreman told her friend/coworker that the Complainant's claim had been denied [para. 34]. Possible that foreman disclosed information for purpose of managing Complainant's employment; but no submissions so not sure. But, in any case, not reasonable to disclose the status of the Complainant's disability claim [para. 35]. • But, this info also PI. Could be exempt from consent under s. 20 PIPA under specified circumstances. But, no evidence from Organization so found that no authority to collect PI disclose consent.
P2014-03	2014	Morpheus Theatre Society & Storybrook Theatre Society	• Marketing email from Storybook Theatre Society. He complained to Storybook, which stated that an error in its database that shared with Morpheus Theatre Society causing Storybook to have access to Morpheus patron information.	• Complainant's past sponsorship of Storybook makes the collection of PI by Storybook no longer an issue [para. 8]. • PI includes name and email address. So, PI at issue. • Storybook is a NFP incorporated under Societies Act, so an NFP under PIPA.	• Storybook sent Complainant an email advertising a Storybook program. So, Storybook used the Complainant's name and contact information in sending that email. [para. 20]. • Based on past decision (P2013-D-01): "A commercial activity is any transaction, act, conduct or regular course	• Complainant was a past sponsor of Storybook, which is why Storybook had the Complainant's PI. So Morpheus did not disclose information to Storybook. [para. 8]

			• Complaint that Morpheus disclosed PI without consent and Storybook collected and used information PI inappropriately. Morpheus complaint withdrawn.		of conduct that is of a commercial character. … the definition is meant to capture activities that are more or less commercial, or appear to be commercial by most accounts. …. PIPA is meant to apply to Non-profit organizations that are carrying out activities as though they are a business." [para. 23] • Selling tickets or registration for theatre programs has commercial nature and is commercial activity under PIPA [para. 24]. Marketing Storybook's programming is commercial activity using PI [para. 25]. • Storybook argues that it inadvertently used Complainant's information for marketing purposes. SO, cannot claim had authority to use PI under s. 17 exemptions to consent [para. 27]. • Storybook discussed the database collection means and reasons that information is used. It did not argue that it had obtained consent, in any form, from the Complainant to use his personal information. So found that no consent existed [para. 30]. No authority to use Complainant's PI to email him marketing materials [para. 31].	

					• Storybook ordered to delete Complainant's information from database.	
F2014-07	2014	Bow Valley College	• Public Body severed personal information from records when responding to access request. Complainant asked to have that severing reviewed. • Complainant complained that PB had disclosed PI contra FOIP.	• Information at issue included referral letter by program coordinator of PB including possibility of mental health assessment of Complainant.	•	• Not sufficient evidence to establish that the PB had used or disclosed his PI. • Complainant submitted that • PB argued that shared consent form and referral forms with nurse. Since no assessment conducted; no reporting or sharing of information about Complainant between any health professional and PB. PB did not have any evidence to show PB disclosed his PI to medical professionals, students or to Iranian Government. No evidentiary burden met by Complainant.
F2014-30	2014	Appeals Commission for Alberta Workers' Compensation	• Applicant made access request under FOIP to PB for statistics regarding number of appeals conducted by PB addressing specific policy and how many of those appeals were granted. • PB responded there were no records responsive to Applicant's request and sent them to CanLII website. • PB argued that it maintains database of decisions but not to level of detail that Applicant's request required and also	•	•	• An adequate search requires a public body to take every reasonable effort to search for the actual records requested [para. 7]. • PB argued that creating a responsive record for Applicant would amount to conducting research for a party appearing before it: "… conducting research that may support a particular appeal or type of appeal has the potential to create a reasonable apprehension of bias and is beyond the scope of its role as an independent decision-maker." [para. 15].

			argued that creating record from its electronic database would unreasonably interfere with its operations.			• Requestor's identity is not to influence how request is processed [para. 16]. • "Where a PB can create a record from information currently existing in electronic form by essentially manipulating the data, it has an obligation to do so in response to an access request, as long as it can be done using the PB's normal hardware, software and technical expertise and where creating the record would not unreasonably interfere with the PB's operations." [para. 20]. • Adjudicator agreed with PB that steps required (about 1 employee working fulltime for 1 month) exceed FOIP requirements. • However, there may be another avenue to search the records, which was not fully explored by PB. PB ordered to explore that possibility [para. 34].
P2014-02	2014	Consumer Choice Awards	• Organization forwarded chain of emails between Organization and Complainant to 3rd party company. Complainant argued this was disclosure contra PIPA. • Organization did not have authority to disclose Complainant's PI.	• Information at issue included name, work email and opinion on company. Name is clearly PI and personal opinion could be PI. Work email was PI because communication not part of job duties.	• N/A	• Organization stated it had consent. No exceptions to consent from PIPA applied. No authority to disclose without consent [para. 19]. • For s. 8(2) to apply (if give information without consent voluntarily and reasonable that person would voluntarily provide information), must be obvious in circumstances that Organization would

						disclose information to 3rd party company [para. 23]. The Complainant must know the purpose before section 8 is triggered [para. 27]. • Organization informed Complainant that they would get in touch with company, but it was not obvious to him that his PI would also be shared. Reasonable interpretation of Organization's statement [para. 24]. It could have been a reasonable interpretation that Organization would share both name and complainant. Here key is that there was more than one reasonable interpretation. Given the room for misinterpretation, it was incumbent on Organization to clarify before relying on the Complainant's failure to object to its stated plan [para. 27]. Section 8(2) test is objective[para. 28]: "showing that it was not unreasonable for the Organization to think it had consent is not the same thing as showing that it did have consent." • Express consent entails "you may disclose this information" [para. 26]. • Organization could not rely on both having consent and using the notice option (opt-out) consent. There was no time limit provided to

						Complainant to stop disclosure of PI. Notice that is subject to different interpretations is not notice that Complainant could have reasonably been expected to understand [para. 31].
F2014-21	2014	Alberta Human Services	• Service provider contracted by PB. Complainant complained that service provider collected, used and disclosed his PI contra FOIP when arranged referrals for assessment and rehabilitation services to assist him re: medical condition. • Complainant argued that service provider acted as PB.	• Service provider = a particular society that helps individuals with a particular type of medical condition through education and referrals to community resources for assessment and rehabilitation (doesn't provide the assessment or rehabilitation services itself). Complainant learnt about service provider in course of receiving services form Alberta Works (= PB). • At relevant time, Memorandum of Agreement for Services between PB and service provider. PB acknowledges it is responsible for the collection, use, and disclosure of the Complainant's PI by service provider given latter contracted by PB. So, references to service provider or its staff is indirect reference to PB [para. 2]. • PI at issue because included name, address, contact information, marital status, personal health number, health and employment history and opinions about him. [para. 5]. • Service Provider contracted to perform services as part of provincial initative; thus	• Complainant alleged PB made improper use of his PI. But, did not clearly explain that improper use. Hence adjudicator viewed the complainant of improper use was more regarding fact PI disclosed to certain third parties. [para. 41] • PB may both use and disclose individual's PI for purpose for which PI was collected or compiled or for a use consistent with that purpose [para. 43].	• In making referrals, Service Provider disclosed Complainant's PI [para. 27]. • All disclosures for purpose of arranging assessment and rehabilitation services as part of an operating program or activity of PB. Reasonable and direction connection to the collection of the PI in the first place. Necessary for operating a legally authorized program of the PB. • Some agencies no referral made, just contemplated so no disclosure. [para. 32]. • Referrals only disclosed fact that referral sought, reason for referral, and that Complainant being assisted by Service Provider. Minimal information necessary. Consistent with purpose of collection. [para. 39].

				initiative = operating program of the PB. • Service provider collected PI on initial contact intake form. • Complainant stated only wanted employment assistance not rehabilitation; so, felt that some health PI collected was beyond what necessary. • "… even if the Complainant sought employment-related services only, it was still part of the PB's program or activity to consider arranging referrals, assessment or rehabilitation in order to determine what type of employment best suited the Complainant. [Adjudicator] therefore found that the collection of all of the PI of the Complainant… was authorized by s. 33(c)." [para. 12]. • While consent form contemplated collection of PI from certain agencies and individuals, in this case no information collected in actuality. [para. 17]. • Service provider, as contracted by PB, can fall under FOIP exceptions related to "employees" and information sharing when for purpose of delivering common or integrated program or service. [para. 22].		
F2014-28	2014	Alberta Health	• Complainant = former employee of PB. Complained that supervisor had	•	•	• PB claimed that sent email for purpose of managing and administering personnel, but conceded

			emailed all members of PB executive team and disclosed that he would be away from office for personal reasons. • Claimed breach of FOIP. • Also, believed that email had been forwarded beyond original distribution list.			that not authorized to disclose nature of Complainant's leave. • PB disclosed more PI than necessary to meet its stated purpose. SO contravened s. 40(4) FOIP. Disclosure of leave was reasonable and authorized; but disclosure of the reason for the leave was not authorized. Another more generic term possible. No indication of confidentiality in email so that forwarded occurred. • PB must only disclose as permitted by FOIP and must make reasonable security arrangements to protect PI. • Disclo
F2014-36	2014	Alberta Health	• Individual made access request to PB under FOIP for all policies, past and present, in regards to the closing of health facilities. • PB provided 8 pages of records and withheld 44 pages in entirety. • Applicant argued policies outline process for making decisions on a particular matter, and do not contain information that can be withheld.	•	•	• Withheld records were not responsive to Applicant's request. • Withheld records "draft internal correspondence and analysis." Records do not pertain to completed policies, which Applicant sought so not applicable. [para. 11].
F2015-15	2015	Alberta Energy	• Access request to PB for studies, reports or documents comparing AB	•	•	• Numerical information in graphs or charts in the records at issue fell under s. 16(1) of FOIP as

			royalty rates and regime for non-renewable energy resources costs to royalty rates and regimes in other jurisdictions. • Some responsive records included information on a private sector organization (3rd party). PB gave access to Applicant; 3rd party requested review of decision arguing disclosure would be harmful to business interests.			information was trade secret and supplied in confidence. Disclosure could result in harm enumerated in s. 16(1)© if disclosed. • 3rd party's name could not be withheld as it did not fall into any of categories of info in s. 16(1)(a).
F2015 -17	2015	County of St. Paul No. 19	• Complainant states Grazing Reserve sent email containing his PI to PB; PB gaven email to law firm representing a Commission of which PB a member for Commission to use in proceeding before Environmental Appeals Board. Commission not Grazing Reserve party to proceeding. • Email : information regading unresolved bill for a grazing fee charged to Complainant. • Complainant argued inappropriate collection and disclosure of PI due to lack of authority.	• Information was about Complainant's agricultural operation, not about him as individual. Thus FOIP does not apply. • Public Lands Act supported claim that person to whom grazing allotments are granted are operating a business. Membership information including payment for membership is information about that business, not PI. [para. 9] • Previous OIPC orders found that disclosure of name not unreasonable invasion of privacy per s. 17 where associated information reveals only that individual acting in a formal, representative, professional, official, public or employment capacity, unless that information also has a personal dimension. [para. 10].	•	•

				• In farming context, OIPC previously stated that PI "is recorded information about an identifiable individual, which means a human being acting in his or her natural capacity." PI distinct from information about individual's business, no matter how set-up (e.g. sole proprietorship, partnership, unincorporated association, corporation or other entity). [para. 11] • If membership fees owed, owned by Complainant as an organization, not as an individual [para. 13].		
F2015 -27	2015	Alberta Justice & Solicitor General	• Former employee of PB complained that PB CUD his PI contra FIOP when searched his name in AB Community Offender Management database (ACOM) while employed. • PB did search to verify Complainant's honesty and integrity.	• Search was of PB's own database, so not a collection of Complainant's PI. • In applying for job, submitted criminal record check, which showed no criminal convictions. • Later PB concerned about Complainant honesty, so checked ACOM and found one result of some contact/involvement.	• PB did not have authority to use Complinant's PI from ACOM databased because information used in way not consistent with purpose for which it was collected. • Purpose of original collection was to track offenders serving in community and to assist employees of PB involved with these offenders. PB access in this case to verify Complainant's past and honesty. Thus, purposes in collection and use not consistent. Complainant not offender serving time in community and checking honesty not part of ACOM database. • Need consistency between use and purpose for collection.	• Complainant did not consent to use and/or disclosure of his PI. •
F2015 -26	2015	Calgary Police Service	• Complinant believed that her PI and that	• Adjudicator found that PI was collected for purposes of	•	•

			of her kids was collected by PB contra FOIP. • PB received call that young child and infant left alone in motor vehicle in shopping centre parking lot for 10 minutes at time of call. When police arrived, car gone. Caller gave license number. • PB team attended Complainant house to discuss case and issue. Submitted police reports on investigative findings. • Complainant felt PB should not have collected her PI.	law enforcement and was therefore permitted under FOIP. • Safety concerns for children. Need for treat assessment, and thus was law enforcement matter. • After a potential law enforcement matter is concluded, records of what transpired should still be made. Transparency of these interactions is critical for upholding rights.		
F2016-41	2016	Service Alberta	• The Canada Revenue Agency (the CRA) made a request to the PB for the Applicant's physical address. • The Public Body provided the address it had on file; however, this address proved to be a mailing, rather than residential, address. • When the Applicant applied to renew her motor vehicle registration, the PB required her to provide proof of the address of her residence (the Applicant's "physical	• The Applicant complained that the Public Body had contravened the FOIP Act when it disclosed her personal information to the CRA. The Adjudicator determined that section 4 applied to some records, as these records were created from information in the office of the Registrar of Motor Vehicle Services. However, she found that section 20 did not authorize the PB to withhold any of the information to which it had applied this provision and she ordered disclosure of this information. • The Adjudicator determined that the PB had two purposes for collecting the Applicant's physical address:	•	•

			address" within the terms of the Operator Licensing and Vehicle Control Regulation). • When she provided the requested proof, an investigator of the PB contacted the CRA to inform it that the Applicant had provided a new physical address and supporting documentation. • The CRA then requested the physical address and the PB provided it. After the CRA obtained the physical address, the CRA obtained a Court order to obtain the physical address and the supporting documentation the Applicant had provided. The CRA subsequently initiated legal proceedings against the Applicant. The Applicant made a request for her file from the PB under the Freedom of Information and Protection of Privacy Act (the FOIP Act). • The PB refused access to the file on the basis of sections 4 (Application) and 20 (Disclosure Harmful to Law Enforcement). The Applicant sought	the first was for ensuring that the Registrar had sufficient information to make a determination as to whether the Applicant was a resident of Alberta and the second was to assist the CRA. • The Adjudicator determined that assisting the CRA was not a purpose for which the PB was authorized by the FOIP Act to collect personal information. The Adjudicator determined that the PB had disclosed the Applicant's personal information on four occasions. She found that the first three disclosures were not authorized by the FOIP Act, but that the fourth disclosure, which was made to comply with a Court order, was authorized. The Adjudicator ordered the PB to disclose the information to which it had applied section 20 and ordered it to cease collecting, using, and disclosing the Applicant's personal information in contravention of the FOIP Act.		

			review of this decision.			
F2016 -26	2016	Edmonton Public School District No. 7	• Complainant is female transgender student at school run by PB. • Complained that PB disclosed her PI contra FOIP when teachers displayed or called out her legal name, which is a typically male name. • Complainant and parents met with school officials; officials told that they could advise Complainant's teachers that she was transgender but did not want school body aware of this. School officials agreed and assured information privacy. One accommodation was to use paper list for roll call (with preferred name) not computer list (with legal not chosen name). On number of occasions, legal name displayed on screen at front of classroom visible to class; one 2 occasions teacher or student read legal name; 1 occasion supply teacher loudly discussed process for name change. • Many of incidents involved supply teachers; Complainant advised	• PI at issue (name, sex, and that gender identity different form her sex at birth). • Legal name not changed and reflected that she was born physically male. • Because Complainant requested that information not be disclosed, then disclosing it not unreasonable invasion of her privacy. • Disclosure was not prudent or necessary in the circumstances, so contra s. 40(4) FOIP.	•	• PB agreed it had breached FOIP and had not made proper security arrangements to protect Complainant's PI. • PI Disclosed in breach of s. 40 of Act. • PB failed to make proper security arrangements, but noted that draft policy created after these breaches addressed concerns raised by Complainant. Draft policy includes informing students that their chosen name and gender can be changed confidentiality in computer school records with signed parent consent and discussion; without District letter school will ensure student's chosen name and chosen gender correctly entered into hard copy; supply teachers will be informed via info package and verbally to use only last name for students' in roll call and not use screen; principal to instruct staff to only use last names.

			that binder is created for supply teachers and contains info that teacher must take attendance from paper copy of class list.			
P2016-07	2016	Redi Enterprises Society	• Organization requested written account of Complainant's criminal conviction. • Complainant argued that was contra PIPA.	• Employee situation. • Did not determine if PIPA applied because NFP, parties agree to go forward assuming it did apply. • Information was never provided, just requested. • "PIPA balances the right of an individual to privacy of their PI with the need for an organization to CUD PI. If an organization can demonstrate the collection of PI is necessary to enable it to meet certain reasonable purposes and it is collected in a reasonable manner, then the collection may be allowed under the Act." [para. 10]." • Organization had policy of requiring a written, signed account of the criminal activities of its employees. [para. 18]. • This information is a requirement to share [para. 23]. Collection is solely for employment related purposes. Evidence that information contained in employee file and used only to manage employment relationship. This reasonable explanation: Organization gave sufficient notice, used to manage employment relationship, works with vulnerable	•	•

				population and seeks safe and secure environment, treated as confidential information. • Organization in compliance with s. 15 PIPA.		
P2016-08	2016	Alberta Assessors Association	• Organization disclosed her PI by using a data matching database to analyze demonstration report submitted to UBC. Complainant's name and student number included in demonstration report. • Organization took disciplinary measures against Complainant on basis of analysis of demonstration report. • Complainant complains these actions contra PIPA>	• Organization = NFP per s. 56 PIPA. Not a professional regulatory organization. • Organization CUD Complainant's PI as part of its regulatory and disciplinary function. • Commercial activities typically those involving buying, selling, or exchange of goods or services [para. 13]. • PIPA did not apply because CUD not in connection with commercial activity. • Organization CUD PI through application of software for purpose of regulating member of assessor profession, not in connection with purchase of software. [para 19]. • Fines are not goods or services, and they are not bought, sold or exchanged [para. 20]. In assessing the fines and costs, the disciplinary committee was not providing a good or a service, or requiring that the Complainant purchase a good or a service. Assessment of fines does nto have a commercial character.	•	•
H2016-02	2016	Alberta Health Services	• Complainant requested disclosure logs for her AB Electronic Health Records (NetCare).	• Custodian conceded that Complainant's health information had been used without authorization.	•	• Adjudicator required Custodian to put in place safeguards that protected Complainant's HI from specific identifiable risk.

			She discussed that individual (Affiliate) had reviewed her HI. Complainant knew Affiliate and knew they had no reason to review her record. • Complainant believes Affiliate may have obtained information in records and used it to contact Complainant's employer and another individual.	• Breach of s. 25 HIA occurred by Custodian's affiliate [para. 4]. Affiliate accessed HI on one occasion with no need to know. Used it to contact Complainant employer to complain about Complainant; day later they were remorseful and withdrew that complainant.		• Current safeguards included training and awareness procedures; IT policies limiting CU to authorized personnel; policies providing for education, training and auditing of compliance with policies; policies outlining reporting and breach discipline; policies re: monitoring and auditing of IT resources. • Custodian recognized risk that employees and affiliates may use or access HI without authority; policy measures outlined intended to protect against such unauthorized use or access. [para. 12]. • All security steps must be reasonable: mitigation strategies do not need to be perfect; information security and breaches may still occur even when reasonable safeguards have been implemented [para. 13]. • Custodian found to have taken reasonable steps to maintain safeguards to generally protect HI confidentiality and generally protect against reasonably anticipated unauthorized UD or access to HI [para. 15]. • But, not clear that reasonable steps taken to mitigate risk from identifiable individual (Affiliate). [para. 16]. No information regarding review of Affiliate's access in Meditech and Netcare

						[para. 19]. OIPC not told dates that review period covered nor that there would be further reviews. • Affiliate faced sanctions from governing professional body including mandatory completion of modules on ethics and privacy. [para. 21]. • Custodian masked Complainant's Netcare information so additional layer of privacy to her information from all employees and affiliates of Custodian (not just this Affiliate). • Affiliate had to write letter of apology to Complainant and her employer. But letter of apology different from facts to professional body. To professional body, admitted access for personal use, not "no reason" as to OIPC. [para. 25]. • Found that Custodian not demonstrated how to protect against any reasonably anticipated unauthorized use, disclosure or access to Complainant's or others' HI by Affiliate [para. 27]. • Complainant described harm she suffered from Affiliate's actions including significant reticence to access healthcare.
H2016-06 (not	2016	Alberta Health Services	• The Complainant made a complaint that two physicians	• She found that the physicians had gained accessed to the	• She determined that affiliates may use or disclose health	• The two physicians also disclosed the health information they had

printed)			gained access to her health information from Alberta Netcare in contravention of the Health Information Act (HIA). • Alberta Health Services (AHS), which operated the facilities at which the accesses occurred, and the two physicians involved conceded that the two physicians had gained access to the Complainant's health information in 2008 for the purpose of addressing a complaint to the Department Chair that had been made about care they had provided to the Complainant, and again in 2012 for the purpose of defending themselves in a related hearing conducted by the Alberta College of Physicians and Surgeons (the College).	Complainant's health information for their own personal purposes, rather than those of AHS, and that AHS had, by operation of section 62(2) of the HIA, contravened section 25 (prohibition regarding use of health information) of that Act on those occasions when the two physicians did this. Although the Adjudicator ordered the two physicians to meet their duty to comply with the HIA and its regulations when they use and disclose health information, the Adjudicator decided that she could not order the two physicians to comply with AHS's policies and procedures, given that doing so would not ensure the confidentiality of the Complainant's health information.	information only at the direction of, under the authority of, or on behalf of, the custodian with whom they are affiliated.	obtained to the College. The Adjudicator determined that AHS was the custodian in this case, and that the two physicians were affiliates of AHS. • The Adjudicator also determined that the Complainant's health information had been disclosed to the College by the two physicians for the purpose of defending themselves in a complaint. She found that affiliates may disclose health information only under the authority of, or on behalf of the custodian with whom they are affiliated and are subject to the same limitations to which the 2 custodian is subject when they do so. • She determined that AHS would have had no authority to disclose the Complainant's health information in the circumstances in which the two affiliates disclosed it, as AHS was not a party to the complaint conducted by the College, and had not received a formal demand for the records. • The Adjudicator concluded that these accesses and disclosures caused AHS to contravene sections 25 and 31 of the HIA. The Adjudicator determined that AHS's policies and procedures were not adequate to

						protect the Complainant's health information from the risks of unauthorized use and disclosure, as they appeared to permit affiliates to use and disclose health information for their own personal purposes, rather than purposes of AHS that are authorized by sections 27 and 35 of the HIA. While the Adjudicator found that use and disclosure of the Complainant's health information by the two physicians had led AHS to contravene the HIA, it appeared that the two physicians had not contravened AHS policies and procedures when they used and disclosed the Complainant's health information for their own personal purposes. • The Adjudicator ordered AHS to cease using and disclosing the Complainant's health information in contravention of the HIA. She suggested that compliance with the order could be achieved by revising the policies and procedures for affiliates such that they would convey the following: 1) only AHS is the custodian and authorized custodian at sites it operates, 2) the HIA authorizes only an "authorized custodian" to use or disclose health information via the

						Alberta EHR, and 3) affiliates may use or disclose health information via the Alberta EHR at AHS's sites only where AHS would have authority to use or disclose health information. The Adjudicator also determined that AHS should review its policies to ensure that they create enforceable obligations for affiliates to collect, use, or disclose health information under the authority of AHS, in compliance with the HIA, such that section 62(4)(b) is engaged should an affiliate use or disclose health information in a way that contravenes the HIA
F2016-01	2016	Bow Valley College	• Complainant complained that PB used or disclosed his PI contra FOIP when Academic Preparation Coordinator emailed number of employees of PB to advise them of ongoing conflict between Complainant (student) and another student. • Complainant had successfully sued other student around issue.	• Information collected was necessary for an activity of PB. Necessary to use name because student at PB so necessary for operating program and activity [para. 15]. • Context of email and use of Complainant's first name = PI under act. [para. 11]. • Academic Preparation Coordinator wrote emails to two supervisors and another employee of PB stating that talked to other student including that would be receiving warning letter; that not have contact with Complainant; and to inform PB if Complainant contacted him. Other student informed them of litigation.	• Information was used when sent via email. Could be seen as disclosure between one employee to others. OIPC Adjudicator treated it as use and disclosure, with results being same. [para. 12] • Information used for reason consistent with why information was collected. • Resolving issues between students and related concerns arising from campus-related activities is responsibility of PB. [para. 17]. • Emailing Complainant's PI to limited number of employees had a	• PB found to have made reasonable security arrangement against the risk of unauthorized access, CUD of Complainant's PI: email accounts remain within PB computer network; network monitored by IT services department for things such as security threats, viruses and unauthorized access; employee email accounts are password protected and all employees must follow PB IT policies [para. 22]. • PB met is duty under s. 38 when emailed Complainant's PI.

					reasonable and direct connection to the purpose of the collection and was necessary for operating a legally authorized program of PB [para. 19]. No contravention of Part 2 of FOIP.	
P2016-02	2016	Grandin Manor Ltd.	• Condo unit owner complained that Organization put up surveillance system not in complainance with PIPA. Complained that no signs notifying individuals of extent of surveillance and extent that cameras in use. Complained that Condo board reviewed footage and used info from footage to review bylaw infractions and to enforce compliance with condo bylaws. Complained that Organization collected his PI with cameras when he scribbled comments on notice posted by elevator and when use info to send him warning letter about conduct.	• Owners had passed resolution to increase surveillance in condominium. They acted as Organization. • When visitors visit condominium they have sufficient notice of presence of surveillance that they may be deemed to consent to Organization's collection of PI for purposes of maintaining security of building. Purpose of deterring vandalism and promoting security in building; also to increase value of property and make residents feel safe. • Surveillance cameras capture PI of individuals indiscrminantly.	• When Organization reviewed surveillance footage for purpose of deterring the Complainant from scribbling comments on notices in the future, it did so for purpose for which PIPA requires it to obtain consent and to provider notice prior to collection. • Organization must cease collecting and using PI from surveillance cameras for purposes other than obvious purposes for having surveillance unless it first provided appropriate notice under PIPA of its intention to collect and use information for these purposes. • Adjudicator unable to say that scribbling notes on notices is criminal vandalism, so nto sure that fits in notice/purpose.	•

Table 4. Best practices dictated by *PIPA*

Privacy policy	▪ Need policies and procedures in place to cover all personal information that is in your custody (stored) or control (decide how to use, disclose, store and for how long keep).
	▪ Policies should cover
	  ▪ What personal information is collected?
	  ▪ How obtain consent for collecting, using and disclosing personal information?
	  ▪ How use and disclose personal information?
	  ▪ How ensure that adequate security measures are in place?
	  ▪ Where is information stored?
	  ▪ How is it secured?
	  ▪ Who has access to or uses it?
	  ▪ How is information disposed of?
	  ▪ How process access requests?
	  ▪ To whom is it disclosed?
	  ▪ How is disclosure decided?
	▪ How respond to enquiries and complaints?
	▪ The reasonableness test indicates that review privacy and info handling procedures for both new and on-going activities

Privacy officer	▪ Need to designate:
	  ▪ 1 or more individuals to make sure that the organization follows the rules in *PIPA*
	  ▪ 1 or more individuals to be the contact person(s) for answering questions about *PIPA*, taking access requests and complaints related to *PIPA*
	  ▪ Delegate alternate individuals as back up.

Consent	▪ Need consent of individual to
	  ▪ Collect personal information (from individual or someone other than individual)
	  ▪ Use personal information, or
	  ▪ Disclose personal information
	▪ Usually get consent at information collection
	▪ Consent only valid if collection is reasonable. Consent does not permit unreasonable collection of information.
	▪ Consent can be express (written or verbal; electronic or hard copy, but electronic copy should be turned into hard copy), implied (volunteer information for an obvious purpose and reasonable to volunteer; don't have to give notice because obvious collecting information; if not obvious then need express or opt-out) or not opting out.
	▪ If individual volunteers more personal information than needed for purpose, organization cannot collect, use or disclose the extra information.
	  ▪ Based on reasonable expectations in circumstances and given sensitivity of information
	▪ Consent must be informed so that enough information provided by organization on collection on the purpose of collection and proposed use of information to make an informed decision.
	▪ Opt-out consent is possible when

	▪ Organization informs individual about the purpose in collecting, using or disclosing information ▪ Give easy-to-understand notice before or at time of collection, use or disclosure ▪ Individuals have reasonable chance to say no (re: format, procedure, time) ▪ The personal information is not too sensitive ▪ Individual can change or withdraw consent by giving organization reasonable notice (as long as it does not interfere with legal duty or obligation between any 2 parties) ▪ Individual can put reasonable terms and conditions on their consent ▪ Organization cannot make consent regarding personal information collection, use or disclosure a condition to supply a product or service, if asking for the information is beyond what is required to give service. ▪ The consent will be deemed illegal and invalid if false or misleading means were purposively used to obtain the consent.
Security	▪ Take reasonable steps to make sure that personal information collected, used or disclosed is accurate and complete. ▪ Updating information to the extent reasonable for its use, rather than routinely is acceptable. So, frequently used information should be updated more frequently than information used rarely. ▪ Use reasonable safeguards (physical, administrative and technical) to protect personal information from unsanctioned access, misuse, theft, loss, destruction. Safeguards should be appropriate to the sensitivity of the information. ▪ Examples of physical safeguards include ▪ Locking file cabinets and areas where files are stored when no one is there. ▪ Allowing only employees who need access to storage areas or filing cabinets to have access to them ▪ Clearing files and records containing personal information off your desk at the end of the day ▪ Shredding papers containing personal information rather than placing them in a garbage bag or recycling bin. ▪ Examples of administrative safeguards include ▪ Training employees on policies and rules for protecting personal information and the consequences of not following them ▪ Ensuring that personal information, especially sensitive information, is accessible only to those employees who need to know the information ▪ Storing only as much personal information as necessary on mobile devices (e.g. laptops, USB flash drives) ▪ Using cover sheets when faxing personal information, and establishing protocols to ensure only authorized recipients receive fax (especially for sensitive information) ▪ Having employees take an oath of confidentiality ▪ Conducting audits to ensure employee compliance with safeguard procedures. ▪ Examples of technical safeguards ▪ Using equipment or software that truncates debit and credit card numbers on receipts

	▪ Using password-protected screensavers so visitors cannot see information on computers ▪ Using firewalls and anti-virus programs on computers ▪ Using passwords to make sure only certain workers have access to information on computers and changing passwords often ▪ Encrypting mobile electronic devices containing personal information (e.g. laptops, USB flash drives) ▪ Erasing computer hard drives before you sell or donate them ▪ Retention policies must also be established and executed appropriately. Personal information should only be kept as long as reasonable to carry out business or legal purposes. ▪ Where approved based on financial, legal, operational, audit or archival requirements, organizations may follow those approved retention periods or schedules. ▪ Even if an individual has changed or withdrawn his or her consent for collecting, using or disclosing information, an organization may keep that information if there are legal or business reasons to do so (but cannot use or disclose that information).
Access and correction requests	**See Table 2**

Table 4. The categories of "health information" under *HIA*.

"Diagnostic, treatment and care information"	• The physical and mental health of an individual
	• A "health services" (definition *HIA* s. 1(1)(m)) provided to an individual for the purposes of:
	  • Protecting, promoting or maintaining physical and mental health;
	  • Preventing illness;
	  • Diagnosing and treating illness;
	  • Rehabilitation; or
	  • Caring for the health needs of the ill, disabled, injured or dying;
	• Donation by an individual of a body part or substance, including information derived from the testing or examination of a body part or bodily substance;
	• A drug as defined in the *Pharmacy and Drug Act* provided to an individual;
	• A health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization;
	• The amount of any benefit paid or payable under the *Alberta Health Care Insurance Act* or any other amount paid or payable in respect of a health service provided to an individual; and
	• Any other information about an individual that is collected when a health service is provided to the individual but does not include information that is not written, photographed, recorded or stored in some manner in a record.
	• The following information about the health service provider attending to the individual:
	  • Name;
	  • Business title;
	  • Business mailing address and business electronic address;
	  • Business telephone number and business facsimile number;
	  • Type of health services provider;
	  • License number or any other number assigned to the health services provider by a health professional body to identify that health services provider;
	  • Profession;
	  • Job classification;
	  • Employer;
	  • Municipality in which the health services provider's practice is located;
	  • Provincial service provider identification number that is assigned to the health services provider by the Minister to identify the health services provider;
	  • Any other information specified in the regulations.

"Registration information"	• Basic information collected when individuals register to receive health services. The information is primarily used to determine eligibility and for billing purposes. This information would include:
	  • Demographic information, including the individual's personal health number;
	  • Location information;
	  • Telecommunications and information;
	  • Residency information;
	  • Health services eligibility information; and
	  • Billing information, including an individual's account number.

Table 5. Copyright License particulars for Statistics Canada

- As of February 1, 2012, information published by Statistics Canada (SC) automatically covered by the Open License with the exception of Statistics Canada's postal products and Public Use Microdata Files (PUMFs).
- License agreement can use SC information without restrictions on sharing and redistribution, for commercial and non-commercial purposes. Must always acknowledge SC as source of data and adhere to conditions of SC Open License.
  - By using data, one accepts all terms and conditions of Open License.
  - Give full credit to SC if used or referred to in study, articles, papers or other research works.
- Aggregate data available through CANSIM and Census website = Open Data, governed by SC Open License Agreement
  - Worldwide, royalty-free, non-exclusive license to use/reproduce/publish/freely-distribute/sell the information/value-added products, and sublicense.
- PUMFs subject to Data liberation Initiative (DLI) License (possibly identifiable data), which has following key terms of license such that Microdata files:
  - Shall be used for statistical and research purposes. No other purpose unless prior written consent of SC
  - Shall be used by educators, students and staff. Shall not be reproduced and transmitted to outside person or organization.
  - Shall NOT be merged or linked with other databases for purpose of attempting to identify an individual person, business or organization
  - Shall not be presented in a manner that gives appearance that user may have received, or had access to, information held by SC about any identifiable person, business or organization.
  - Provided software shall NOT be disassembled, decompiled or in any way reverse engineered.
- Publications of any information based on PUMFs must use stipulated accreditation.

Found at http://libguides.usask.ca/copyright/stats.

REFERENCES

1. Committee on Transborder Flow of Scientific Data NRC. Bits of power: Issues in global access to scientific data. 1997.

2. Alberta Go. Information Sharing Strategy - Supporting Social-Based Service Delivery. 2016 November 1, 2016. Report No.

3. Idealware. The State of Nonprofit Data. Portland, OR: 2012.

4. Cave J. A shifting sector: emerging trends for Canada's nonprofits in 2016. The Philanthropist. 2016.

5. Lenczner MP, S.;. From Stories to Evidence: How Mining Data Can Promote Innovation in the Nonprofit Sector. Technology Innovation Management Review. 2012:10-5.

6. Network ON. Towards a Data Strategy for the Ontario Nonprofit Sector. Toronto, ON: 2015.

7. Companies Act, Stat. C-21 (2000).

8. Societies Act, Stat. S-14 (2000).

9. Charitable Fund-raising Act, Stat. c. C-9 (2000).

10. Center IK. Data Sharing Concepts and Terminology. 1990, 2014. In: z/OS MVS Programming: Sysplex Services Guide [Internet]. IBM Corporation.

11. Council; MR. Data Sharing Glossary London, UK: Medical Research Council.

12. Van Ymeren J. An Open Future: Data priorities for the not-for-profit sector. Toronto, ON: The Mowat Centre's Not-For-Profit Research Hub, 2015 February, 2015. Report No.: Contract No.: Mowat Re search #107.

13. Personal Information Protection Act, Stat. P-6.5 (2003).

14. Personal Information Protection and Electronic Documents Act, Stat. c. 5 (2000).

15. McLeod Grant HC, L.R.;. Creating High-Impact Nonprofits. Stanford Social Innovation Review. 2007;Fall 2007:32-41.

16. de Las Casas LG, T.; Pritchard, D.;. The Power of Data: Is the Charity Sector Ready to Plug In? London, UK: 2013.

17. Warren SDB, L.D.;. The Right to Privacy. Harvard Law Review. 1890;4(5):193-220.

18. Solove DJ. A Taxonomy of Privacy. University of Pennsylvania Law Review. 2006;154(3):477-560.

19. Freedom of Information and Protection of Privacy Act, Stat. F-25 (2000).

20. Health Information Act, Stat. c. H-5 (2000).

21. A Guide for Businesses and Organizations on the Personal Information and Privacy Acti. Edmonton, AB: Service Alberta, 2008.

22. McKinley A. The Effect of Privacy and Anti-Spam Legislation on Charities and Non-Profits. Advising Charities, Not-for-Profits and Social Enterprises 2013/2014 (Seminar); December 4, 2013; Calgary, AB: Legal Education Society of Alberta; 2013.

23. Development TOfEC-oa. Thirty Years After: The OECD Privacy Guidelines. Paris: 2011.

24. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review. 2010;57:1701-77.

25. El Emam K, Buckeridge D, Tamblyn R, Neisa A, Jonker E, Verma A. The re-identification risk of Canadians from longitudinal demographics. BMC medical informatics and decision making. 2011;11:46. Epub 2011/06/24. doi: 10.1186/1472-6947-11-46. PubMed PMID: 21696636; PubMed Central PMCID: PMCPMC3151203.

26. Malin BA, Emam KE, O'Keefe CM. Biomedical data privacy: problems, perspectives, and recent advances. Journal of the American Medical Informatics Association : JAMIA. 2013;20(1):2-6. Epub 2012/12/12. doi: 10.1136/amiajnl-2012-001509. PubMed PMID: 23221359; PubMed Central PM CID: PMCPMC3555341.

27. Legal Aid Society of Alberta. Office of the Information & Privacy Commissioner of Alberta: Office of the Information & Privacy Commissioner of Alberta; 2013.

28. Lindsay Park Sports Society. Office of the Information and Privacy Commissioner of Alberta; 2007.

29. Canadian Skin Cancer Foundation. Office of the Information and Privacy Commissioner of Alberta; 2008.

30. Fairways Villa South Homeowners' Association. Office of the Information and Privacy Commissioner of Alberta; 2011.

31. Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner). ABCA; 2011. p. 94.

32. Alberta Go. Health Information Act: Guidelines and Practices Manual. Edmonton, AB: 2011.

33. Health Information Regulation, Stat. 70/2001 (2001).

34. Carroll MW. Sharing Research Data and Intellectual Property Law: A Primer. PLoS biology. 2015;13(8):1-11. doi: 10.1371/journal.pbio.1002235.

35. Canada; CIoHRNSaERCoCSSaHRCo. Tri-Council Policy Statement: Ethical Conduct of Research Involving Humans. 2010.

36. Board; CHRE. Comparison of the Characteristics of Research and Quality Improvement/Quality Assurance/Program Evaluation Activities. 2017 January 30, 2017. Report No.

37. Solutions AI-H. A pRoject Ethics Community Consensus Initiative (ARECCI). Edmonton, AB: 2015.

38. Guidelines for differentiating among Research, Program Evaluation and Quality Improvement: Dalhousie University; [February 22, 2017].

39. Berens JM, U.; Verhulst, S.;. Mapping and Comparing Responsible Data Approaches. GovLab and Centre for Innovation, Leiden University, 2016 June 2016. Report No.

40. Karunakara U. Data Sharing in a Humanitarian Organization: The Experience of Médecins Sans Frontières. PLoS medicine. 2013;10(12):e1001562. doi: 10.1371/journal.pmed.1001562.

41. Folkes C. Understanding Nonprofit Data Governance LinkedIn2013 [cited 2017 May 15, 2017]. Available from: https://www.slideshare.net/CathyFolkesCFRE/understanding-nonprofit-data-governance.

42. Network; ON. Data Strategy Toronto: Ontario Nonprofit Network; 2016 [cited 2017 March 24, 2017]. Available from: http://theonn.ca/our-work/our-partnerships/data-strategy/#1467045087069-8c6d1de7-a236.

43. Foundation; V. Open Licensing Initiative Vancouver: Vancouver Foundation; 2015 [cited 2017 Mar 22, 2017]. Available from: https://www.vancouverfoundation.ca/our-work/initiatives/open-licensing-initiative.

44. McCort K. Open Policies Unlock Our Full Potential Vancouver: Vancouver Foundation; 2015 [cited 2017 March 22, 2017]. Available from: https://www.vancouverfoundation.ca/whats-new/open-policies-unlock-our-full-potential.

POLICYWISE

PolicyWise for Children & Families exists to improve well-being by leading, creating, enabling and mobilizing research and evaluation for evidence-informed policy and practice.

PolicyWise was established as a not-for-profit corporation in 2003 and is a partnership between Alberta's universities, the community and the Government of Alberta. We are a provincial organization, governed by a Board of Directors, managed by a President and CEO and supported by a team of individuals with expertise in applied research, data science, knowledge mobilization, communications and administration.

PolicyWise distinguishes itself through its focus on mobilizing evidence to inform social policy, collaborative approach and organizational structure: a formal bridge between government, academia, and the community.

SAGE

SAGE (Secondary Analysis to Generate Evidence) is a collaborative data repository platform that aims to connect stakeholders through secondary use of data. Research data, community service data, and administrative data related to health and social well-being is managed and shared through SAGE. SAGE increases the value of data by providing the infrastructure, processes and governance to bring stakeholders together to use data in new ways and inform social policy and practice.

SUGGESTED CITATION

Manhas, Kiran Pohar. Law & Governance of Secondary Data Use: Obligations of Not-for-Profit Organizations in Alberta. Edmonton, AB: PolicyWise for Children & Families, 2017.

Released: August 22nd, 2017

CONTACT US

info@policywise.com

(780) 944 8630

www.policywise.com

601, 9925-109 Street

Edmonton, AB, Canada T5K 2J8

PolicyWise
for Children & Families