

Information and Data Governance



Literature review and exploration
of models to support the First Nations
Data Governance Strategy



FIRST NATIONS OF QUEBEC
AND LABRADOR HEALTH
AND SOCIAL SERVICES
COMMISSION

AUTHOR

CÉCILE PETITGAND, CEO and founder, Data Lama

CONTRIBUTORS

SUZY BASILE, Professor, School of Indigenous Studies, Université du Québec en Abitibi-Témiscamingue

MARIE-PIER BOUCHARD, Research Agent, First Nations of Quebec and Labrador Health and Social Services Commission (FNQLHSSC)

ÉMILIE GRANTHAM, Research Sector Team Leader, FNQLHSSC

NANCY GROS-LOUIS MCHUGH, Research Sector Manager, FNQLHSSC

AUDREY LAFOND, Research Agent, FNQLHSSC

GUILLAUME PLANTE, Technical Research Assistant, FNQLHSSC

ANNIE-CLAUDE VEILLEUX, Research Agent, FNQLHSSC

MEMBERS OF THE REGIONAL WORKING GROUP FOR THE IMPLEMENTATION OF THE REGIONAL INFORMATION GOVERNANCE STRATEGY

SHUKAPESH ANDRÉ, Director, Research, Development and Innovation, Institut Tshakapesh

ALAIN BÉDARD, Interim Director, First Nations of Quebec and Labrador Sustainable Development Institute (FNQLSDI)

CATHERINE BÉLAND, Planning Coordinator, FNQLSDI

JEAN-DENIS GILL, Governance Advisor, FNQLHSSC

GUY LATOUCHE, Urban Planner and Housing and Infrastructure Advisor, Assembly of First Nations Quebec-Labrador (AFNQL)

CARL SIMARD, Information Resources Manager, FNQLHSSC

MARIE-CHRISTINE TREMBLAY, Team Leader – Communications and Strategic Projects, First Nations of Quebec and Labrador Economic Development Commission (FNOLEDC)

TIM WHITEDUCK, Technology Director, First Nations Education Council (FNEC)

GRAPHIC DESIGN

Karine Potvin

All rights reserved by the FNQLHSSC.

An electronic version of this document is available in English and French at cssspnql.com/en. No part of this document may be reproduced, translated or disseminated, in any form or by any means, without the prior permission of the FNQLHSSC. However, reproduction or use for personal and non-commercial purposes is permitted provided the source is acknowledged by the following:

First Nations of Quebec and Labrador Health and Social Services Commission. 2024. Information and Data Governance: *Literature review and exploration of models to support the First Nations Data Governance Strategy*, 56 pages. Wendake: FNQLHSSC.

All requests must be sent to the FNQLHSSC by mail or by email, at the following addresses:

FIRST NATIONS OF QUEBEC AND LABRADOR HEALTH AND SOCIAL SERVICES COMMISSION

250 Place Chef-Michel-Laveau, Suite 102, Wendake, Quebec, G0A 4V0

info@cssspnql.com

ISBN (Web version): 978-1-77315-494-7

© FNQLHSSC 2024

TABLE OF FIGURES

FIGURE 1: How Information Extracted From Data Analysis Can Help an Organization Achieve Its Goals (Bennett, 2017)	8
FIGURE 2: Data Lifecycle According to the American Health Information Management Association (AHIMA, 2022).....	10
FIGURE 3: Data Governance Institute Data Governance Model (Data Governance Institute, 2020)	12
FIGURE 4: DAMA International Data Governance Model (Earley et al., 2017)	13
FIGURE 5: ARMA Information Governance Model (2022)	14
FIGURE 6: Sibenco Information Governance Model (2023).....	15
FIGURE 7: Seven Phases of the Data Governance Lifecycle (Data Governance Institute, 2020)	16
FIGURE 8: Hierarchy of Data Governance Roles (AHIMA, 2022)	19
FIGURE 9: The Five Safes Framework	21
FIGURE 10: Typology of the Data Governance Ecosystem (Lis and Otto, 2021)	24
FIGURE 11: Alternative Data Governance Models (Gagnon-Turcotte et al., 2021)	27
FIGURE 12: The Data Spectrum (Open Data Institute, 2023)	29
FIGURE 13: Extract of a Dynamic Map on the Sociodemographic Profile of Hawaiian Communities	40
FIGURE 14: Building a First Nations Health Information Management System.....	42
FIGURE 15: Objectives Underlying the Creation of the Papakilo Database	46
FIGURE 16: Trade-off Between Control Over Data and the Benefits of Opening It Up to a Wider Range of Users (developed by the author)	48

1. INTRODUCTION

First Nations have long made data sovereignty the cornerstone of their drive for self-determination and the ability to regain control over their social, territorial, and cultural heritage (Gentelet and Bahary-Dionne, 2021). In fact, data is essential for appreciating the wealth of a territory and a nation, while highlighting the problems and gaps that exist in the policies, programs, and services provided to the population (FNIGC, 2020).

Despite the benefits drawn from information, there are still many barriers limiting First Nations access to their own data (Trevethan, 2019). What's more, the governance and management of these information assets are not fully under the responsibility of First Nations authorities (Taylor and Kukutai, 2016). This obviously runs counter to the core principles that should govern information governance for Indigenous communities, such as the **OCAP® principles (Ownership, Control, Access and Possession)** (FNQLHSSC, 2016) and the **CARE Principles** (Collective benefit, Authority to control, Responsibility, and Ethics) (Carroll et al., 2021).

In response to this issue, the **First Nations Data Governance Strategy** came into effect in March 2020, spearheaded by the First Nations Information Governance Centre and its regional partners. Based on core principles and values, the strategy proposes a roadmap for implementing concrete actions to foster information governance in which Indigenous communities will be active stakeholders (FNIGC, 2020).

The strategy involves the creation of a **national network of regional information governance centres** responsible for accessing and managing First Nations data. Such centres would ensure that the information heritage of First Nations is developed according to their own principles and for the benefit of their communities. In this respect, several governance models are conceivable for setting up such centres and structuring their organization as a network (Bruhn, 2014).

The aim of this literature review is precisely to **present possible options for the adoption of one or more information governance models** that are consistent with the strategy adopted in 2020 and to promote its implementation. This document begins by outlining the key concepts involved in defining data and information governance, so as to properly consider all the pillars that should make up such a strategy. Subsequently, the literature review details several data governance models, focusing in particular on those aimed at producing social benefits. Lastly, the document explores ways of reconciling these models with the principles of Indigenous information governance, presenting examples of First Nations and Indigenous structures and organizations in Canada and internationally.

Ultimately, this literature review seeks to stimulate reflection and discussion around governance models that are compatible with First Nations principles and values, and that serve **their objectives of access, sovereignty, and control** over their information heritage.

2. INFORMATION AND DATA GOVERNANCE

The literature on information and data governance has been growing since the 2000s (Alhassan et al., 2016; McCraig and Davar, 2021; Smallwood, 2019). Yet it's not always these academic publications that have proved authoritative in public and private organizations, given that the models proposed are relatively theoretical and complex (Abraham et al., 2019). Rather, it is the reports and recommendations of consulting firms and professional associations that hold sway when it comes to information governance. Their vision has influenced the way in which information and data governance are defined, structured, and implemented in organizations.

2.1 DEFINITIONS

To begin with, it's important to stress that there is no single, common definition of information governance. In fact, its variations are numerous and diverse, even if some definitions are more widely recognized and adopted than others.

Due to their preponderance in scientific and grey literature, we have chosen to present the three following definitions of information governance.¹

A. Definition by Gartner (private international research and consulting firm)

"Gartner defines information governance as the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals." (Gartner, 2023)

B. Definition of the Information Governance Initiative (think-tank and community of information governance professionals)

Information governance is defined as "[t]he activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs." (Bennett, 2017)

¹ Emphasis added by Data Lama.

C. Definition from ARMA (international association of information management professionals)

“Information governance is the overarching and coordinating strategy for all organizational information. It establishes the authorities, supports, processes, capabilities, structures, and infrastructure to enable information to be a useful asset and reduced liability to an organization, based on that organization’s specific business requirements and risk tolerance.” (ARMA, 2023)

The ARMA definition is the one that covers most aspects of information governance: regulatory mechanisms, decision-making power, processes, infrastructure, and risk management. However, Gartner’s definition refers specifically to roles and policies, as well as measurement indicators, which are key to ensuring the effectiveness of governance and measuring its impact within an organization.

Information Governance and Data Governance - What’s the Difference?

Although the terms “data” and “information” are often used interchangeably, they do not have the same meaning. In its original form, data is a set of bits and bytes, a series of 0s and 1s which, by virtue of their nature and composition, can be understood and processed by computer systems.

Information, on the other hand, is produced from data, once it has been organized, analyzed, and presented in such a way that it can be used. Thus, the value of data is not inherent in the data itself (McCraig and Davar, 2021). In fact, it stems from the creation of one or more data sets, the process of analyzing the data and generating information that can be used to guide decision making and achieve better outcomes (Alhassan et al., 2016). This is illustrated in Figure 1 below (Bennett, 2017).

Consequently, data governance is a key subset of information governance. Its aim is to implement efficient data management that ensures high-quality, accurate, and reliable data. Data governance programs are based on the implementation of policies and processes to manage, cleanse, and store data according to strict standards and procedures (AHIMA, 2022).

In this respect, two definitions of data governance can be adopted, as they are considered benchmarks in the field.

According to the Data Governance Institute:

"Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods." (Data Governance Institute, 2023)

According to AHIMA (American Health Information Management Association):

Data governance is "[t]he overall administration, through clearly defined procedures and plans, that assures the availability, integrity, security, and usability of the structured and unstructured data available to an organization." (Oachs and Watters, 2020, p. 1023)

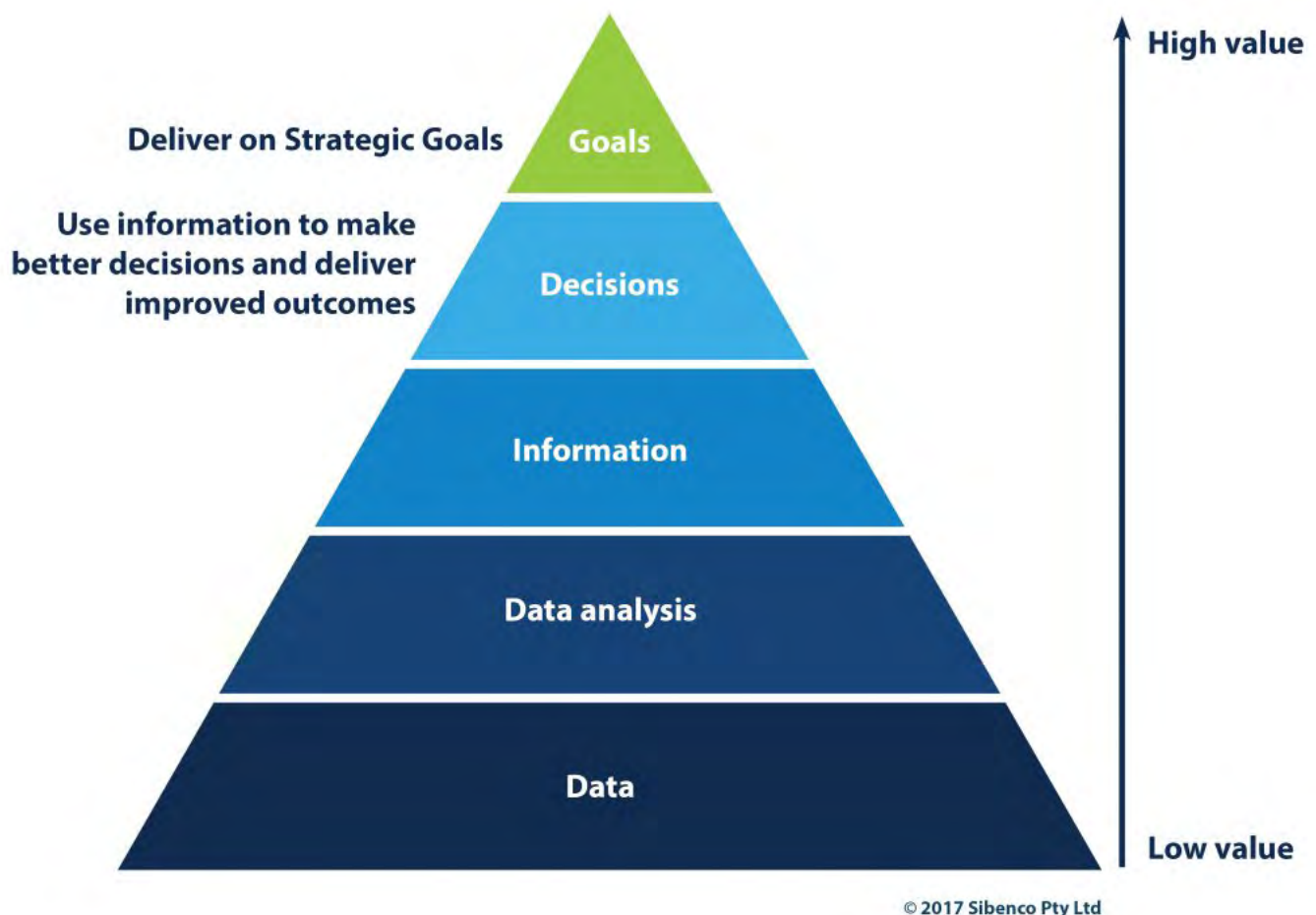


FIGURE 1. How Information Extracted From Data Analysis Can Help an Organization Achieve Its Goals (Bennett, 2017)

2.2 PRINCIPLES

Having proposed definitions of information governance and data governance, which is an essential and underlying part of our discussion, we now turn our attention to the standards and principles that govern them nationally and internationally.

In this respect, the literature reveals that ISO standards remain the benchmark for organizations wishing to implement state-of-the-art best practices in the field of data and information governance (Bennett, 2017; Smallwood, 2019).

Firstly, the **ISO/IEC 38505 standard**² defines the principles of good data governance as part of the management of an organization's information systems. There are the five principles of good data governance:

1. **Responsibility** for data use throughout its lifecycle (Figure 2).
2. **Data management strategy** aligned with the organization's overall strategy, including a plan for data use and a list of the people and departments responsible throughout the data lifecycle.
3. **Data acquisition** by collection, purchase, or generation during a business activity (e.g., analysis of consumer behaviour).
4. **Compliance**, measured by high-performance indicators in line with external obligations and appropriate internal policies.
5. **Human behaviour** that needs to be identified and managed appropriately, for example with regard to compliance with policies concerning the accepted uses of data and systems throughout the organization.

2 To access the standard: www.iso.org/fr/standard/56639.html.



FIGURE 2. Data Lifecycle According to the American Health Information Management Association (AHIMA, 2022)

In addition, **section 9 of ISO/IEC 38500**³ defines essential features of data governance to ensure accuracy and reliability in order to produce valid information. These include:

- **Quality** — how well the data match the facts they are meant to represent.
- **Timeliness** — which may or may not enable decision making.
- **Contextualization** — which enables valid, usable information to be obtained from the data.
- **Volume** — a large amount of data increases confidence in an analysis or the resulting forecasts.
- **Risk management** — which relies on risk-based data classification schemes and appropriate security protection measures.
- **Constraints or conditions** — including legislation, regulations, and contractual obligations concerning data access, use, storage, or sharing. These constraints also include the concerns of members of the general public about how data is used and how decisions are made based on this data.

3 To access the standard: www.iso.org/fr/standard/62816.html.

Finally, **the ISO 24143 standard**,⁴ from 2022, presents a preliminary version of the principles that should structure information governance.

The principles mentioned in standard 24143 (section 5) are as follows:

- Recognizing information as an organizational, strategic asset.
- Designing Information Governance as a key element of organizational strategy.
- Integrating Information Governance into the organization's governance frameworks.
- Securing senior management's leadership and commitment.
- Building Information Governance in a collaborative way.
- Ensuring Information Governance supports legal compliance and any mandatory requirements.
- Aligning Information Governance with performance objectives.
- Ensuring Information Governance supports information security and privacy.
- Ensuring Information Governance supports information quality and integrity.
- Fostering a collaboration and knowledge-sharing culture.
- Adopting a risk-based approach.
- Ensuring the availability and accessibility of information to authorized stakeholders.
- Governing information throughout its lifecycle.
- Support organizational culture.
- Support sustainability.

These principles are admittedly general, but they nevertheless provide guidelines for building governance frameworks that leave no structural pillar untouched. Information governance takes on a number of highly varied and composite dimensions, so that frameworks are needed to assemble them, sequence them over time, and derive meaning from their composition.

⁴ To access the standard: www.iso.org/fr/standard/77915.html.

2.3 FRAMEWORKS

In the literature, there are numerous information and data governance frameworks, which tend to evolve according to the nature of the organizations involved (public or private, for example) (Brown and Toze, 2017; Health Data Hub, 2021; Tallon et al., 2014). However, leading international associations offer relatively comprehensive frameworks for putting forward the essential elements that a data and information governance strategy should include.

As data is the basis of information, we begin by presenting two frameworks that the literature describes as benchmarks in data governance (Bennett, 2017). These are the frameworks of the **Data Governance Institute** (Figure 3) and **DAMA International**, a non-profit professional association specializing in data management certification (Figure 4).

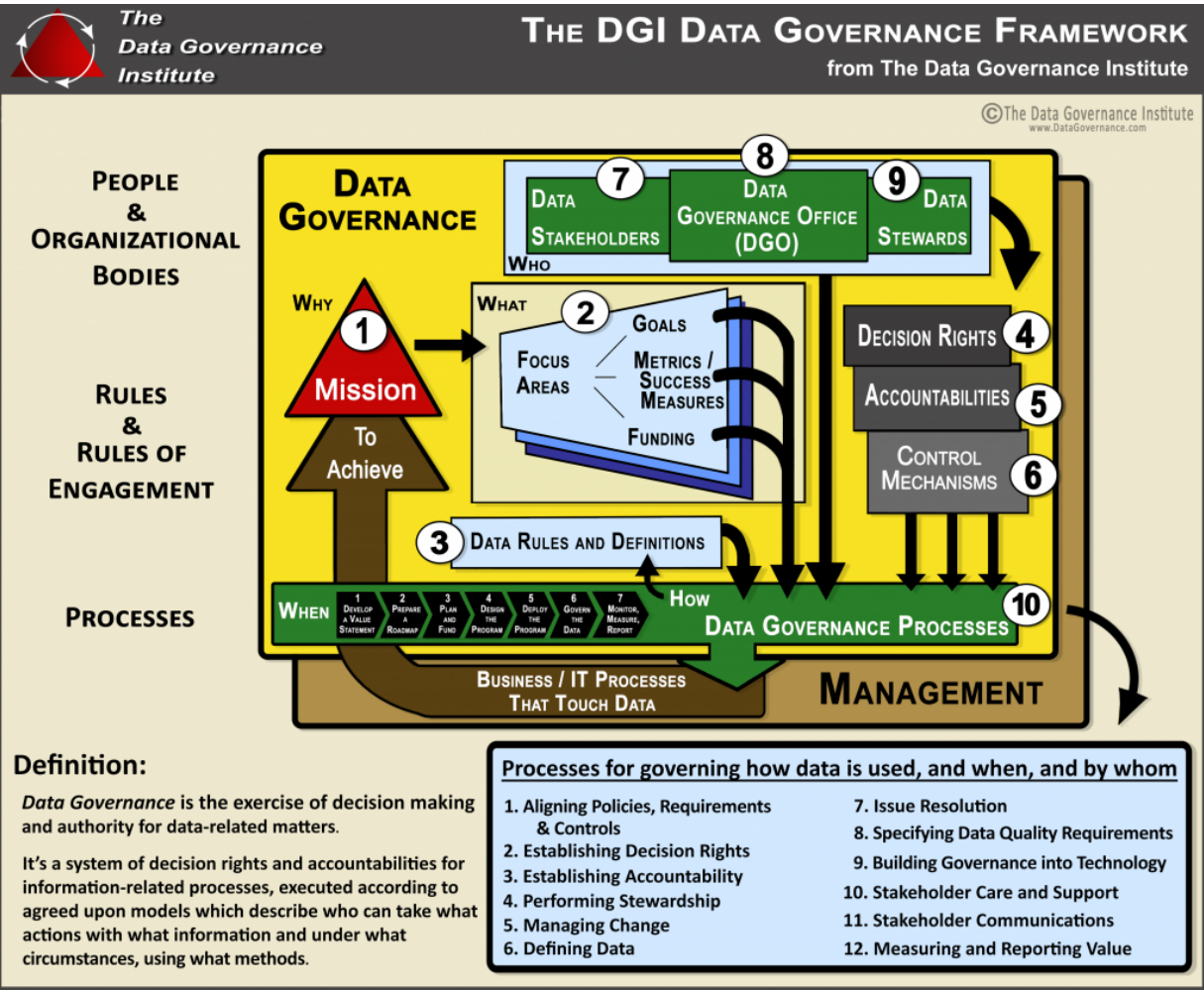


FIGURE 3. Data Governance Institute Data Governance Framework (Data Governance Institute, 2020)

The Data Governance Institute Framework is rich in concepts and terminology. Although it may appear complex, it offers a clear logic for action, presenting a process-based vision of data governance. Indeed, the reader is invited to take a step-by-step look at the major actions to be taken, with a view to ensuring that none of the structuring dimensions of governance are overlooked, and that human, technical, and legal considerations are properly aligned.

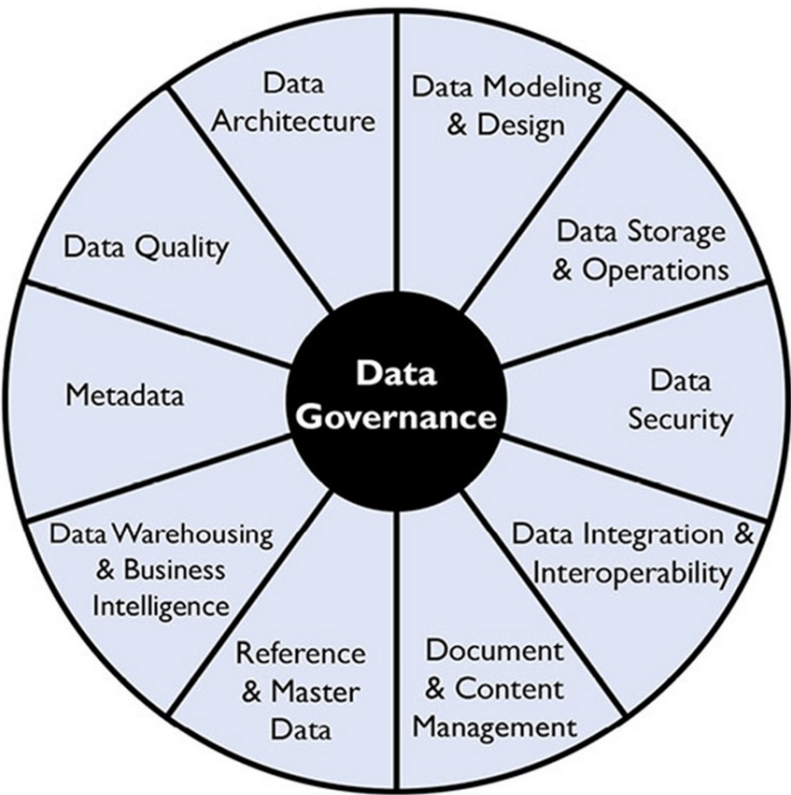


FIGURE 4. DAMA International Data Governance Framework (Earley et al., 2017)

As for the DAMA framework presented above, it remains a benchmark in Canada and, in particular, in Quebec. It is the framework used by **Quebec’s Ministère de la Cybersécurité et du Numérique** to guide analysis and decision making on data governance priorities. This framework is broken down into several technical, legal, ethical, managerial, and process-related components that remain central to data governance. Its originality lies in the emphasis it places on documenting, describing, and archiving data (in particular through the establishment of structured metadata) to make information more easily accessible and reusable by an organization’s members and stakeholders.

As far as information governance is concerned, we have identified two frameworks that we feel are particularly comprehensive, precise, and usable. These are from the international organization **ARMA** (Figure 5) and the law firm **Sibenco** (Figure 6).



FIGURE 5. ARMA Information Governance Model (2022)

These two frameworks present the central elements of information governance, as summarized in the literature (Smallwood, 2019; Tallon et al., 2014). These elements cover the many aspects of putting an information governance strategy into action, namely:

- Establishing **principles, rules, policies, and standards**, in line with the legal and regulatory context in which the organization operates.
- Implementing a **technological infrastructure** guaranteeing data security and integrity, and enabling information to be leveraged.
- Organizing **specific units and functions** to ensure that roles and responsibilities are properly assigned, thus enabling information to be managed throughout its lifecycle.
- Establishing **procedures and processes to manage risks** and control the quality and effects of information use.



FIGURE 6. Sibenco Information Governance Model (2023)

2.4 STEPS

Implementing an information governance framework within an organization, or designing an ad hoc data management structure, takes time, and a **stepwise approach** must therefore be used. In this context, organizations specializing in data governance propose a series of phases for implementing such planning. This is the case, for example, of the Data Governance Institute (Figure 7).



FIGURE 7. Seven Phases of the Data Governance Lifecycle (Data Governance Institute, 2020)

This quote from the Institute's report (Data Governance Institute, 2020, p. 11) sets out the philosophy behind data governance planning:

"Note that Data Governance does not begin with the design of the program!"

- *Before you start deciding who goes on what committee, you should be clear about your program's value statement.*
- *You should have developed a roadmap to share with stakeholders.*
- *Those stakeholders will want to know the WHO/WHAT/WHEN/WHERE/WHY/HOW of your program before they decide to support it, so you need to anticipate their questions. You'll need preliminary answers, even if they're only assumptions until you do your actual program design."*

Of course, these main steps are only guidelines, and can be adapted to suit the needs and realities of an organization or community. However, they do demonstrate the importance of consulting and involving relevant stakeholders from the earliest steps of planning an information governance model.

Furthermore, according to the literature (Deloitte, 2015; KPMG, 2017; Meehan, 2014; Tallon et al., 2014), data governance **must first and foremost be anchored in an organization's objectives and its value creation proposition.** This means knowing what problems or issues data governance should address, and what benefits or opportunities it can bring. This is the best way to justify the effort and investment required to establish effective, sustainable, and socially acceptable data governance.

For a more detailed look at planning, Fuller's (2018) proposed strategy for phasing in the implementation of information and data governance includes the following steps.

1 – Governance organizational model

- a. Develop a business case to staff the data governance office (DGO)
- b. Establish an operating rhythm for the information governance council(s).
- c. Develop operational training for data governance.

2 – Governance strategic plan

- a. Design and implement domain model.
- b. Current/future state data architecture analysis.
- c. Develop a data governance operating model to support major initiatives.
- d. Develop a data quality program.
- e. Implement a data security control plan.

3 – Governance tactical plan

- a. Implement a business glossary.
- b. Select a master data management or reference data management tool and/or methodology.
- c. Define a metadata strategy including data lineage.
- d. Develop standard operating procedures for project prioritization.

4 – Promote a governance culture

- a. Create a governance roadshow to increase awareness and the implications of implementing a governance program.
- b. Participate in industry forums, conferences, and groups.
- c. Build a process for evaluate and align governance initiatives.
- d. Form an education committee to drive governance training and communications.

As such, during this planning process, the organization can **measure its data governance maturity**. The literature provides relatively comprehensive measurement frameworks to guide stakeholders along the way (Carvalho et al., 2019). In particular, the guide from consulting firm KPMG, designed for the healthcare sector, is relatively useful and accessible for an organization (KPMG, 2018). In a more detailed approach, the CIHI (Canadian Institute for Health Information) model provides a relatively comprehensive toolkit for assessing an organization's information management maturity (CIHI, 2020).

2.5 ROLES AND RESPONSIBILITIES

In terms of human resources, the literature identifies a number of key roles in the governance of an organization's information and data (Mikalef et al., 2020). From data engineers to data scientists, information managers to compliance experts, the number of functions required to implement an information governance strategy seems considerable. However, of all these roles, two seem very specific to information and data governance.

These are **Chief Information Governance Officer (CIGO)** and **Chief Data Officer (CDO)**.

According to Meehan (2016, p. 41):

"The emerging leader in information governance (IG) is the **chief information governance officer (CIGO)**. [...] This individual is the face of IG across the organization. The CIGO leads the IG committee; ensures that IG-related activities and projects are moving forward; communicates wins to the committee, to the C-suite, and to the governing board; and ensures that the enterprise workforce is informed. The CIGO is also responsible for communicating and securing budgetary and human resources needs. The key is to ensure that the CIGO can focus time and attention on the activities of IG and can differentiate IG from the many areas of focus falling under IG oversight."

The **Chief Data Officer** can be seen as the Chief Information Governance Officer's counterpart when it comes to data and maintaining its quality, security, and long-term value.

According to AHIMA (2022, p. 9), in the healthcare sector:

“The Chief Data Officer (CDO) provides vision and strategy for all data management activities, including healthcare data system lifecycles. The CDO takes the lead in global data management, governance, quality, and vendor relationships across the enterprises.”

The CDO is responsible for a range of functions relating to data collection, curation, analysis, storage, and valorization (Figure 8). These roles can be briefly described as follows:

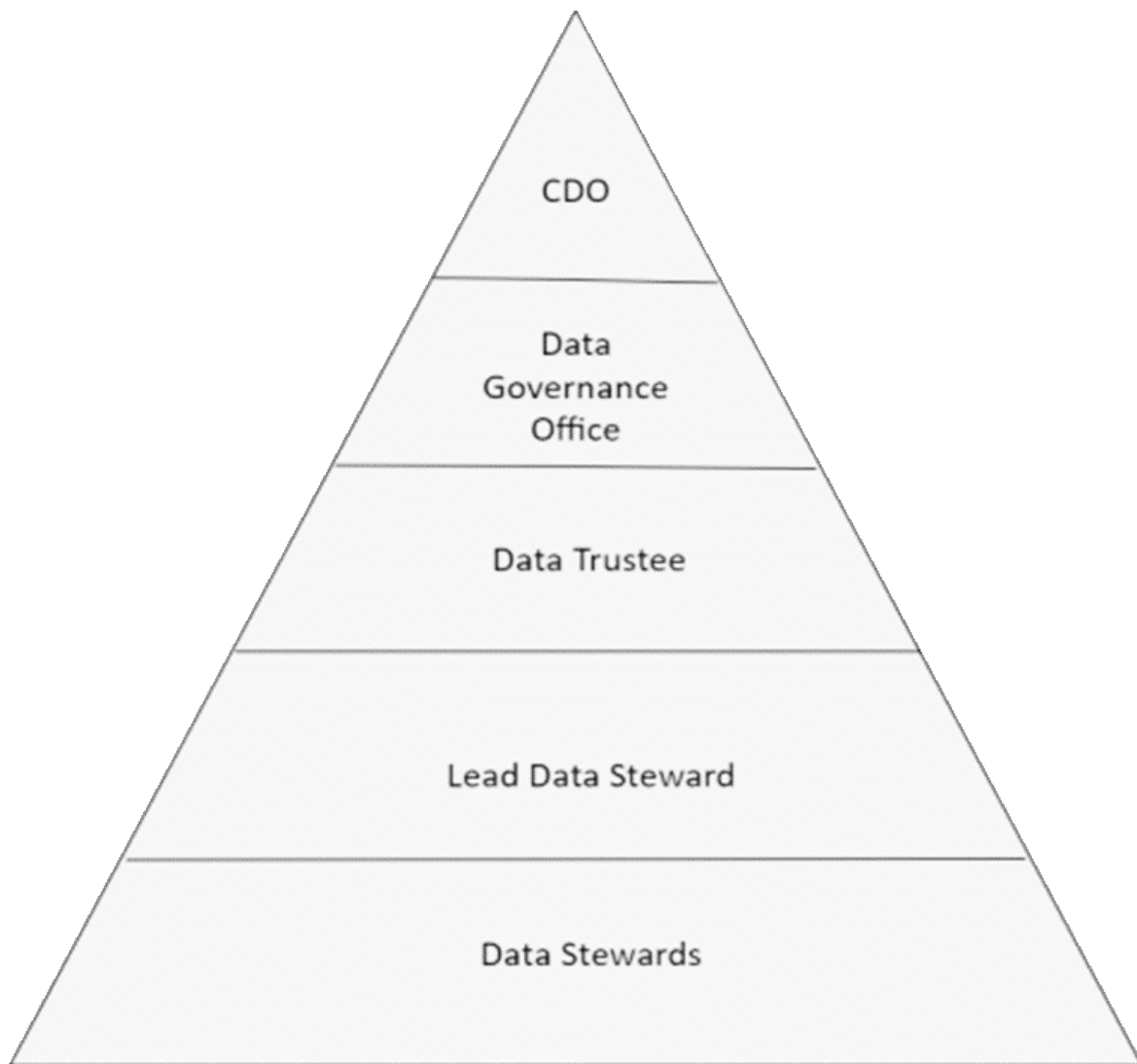


FIGURE 8. Hierarchy of Data Governance Roles (AHIMA, 2022)

Data Stewards are in charge of accessing and analyzing data to produce information for the organization. This role requires a focus on the data management strategy, executing and supporting the resulting projects and programs, and implementing continuous improvements to applications and service/product delivery. Data Stewards also define standards and best practices for data queries, analysis, modelling, and work with data producers to help them document their processes and ensure accurate, timely, and complete data collection.

The **Lead Data Steward** manages the team of Data Stewards and has in-depth expertise in a particular domain or subdomain of data valorization within the organization.

Like the Lead Data Steward, the **Data Trustee** has in-depth knowledge of a domain or subdomain and is responsible for how data is defined and used within the organization.

Of course, this is only a description of functions. Depending on the size of the organization and the number of data-related activities it creates, several people may hold these titles.

2.6 POLICIES AND PROCEDURES

In addition to establishing new roles and responsibilities, information and data governance involves establishing **specific policies and procedures** (Abraham et al., 2019; Alhassan et al., 2016). These are part of the legal and ethical framework within which the organization sets up its governance structure.

Here are a few examples of these policies:

- Data quality and integrity policy
- Data access policy
- Privacy and data protection policy
- Policy for sharing data internally and with members outside the organization
- Data retention policy

These policies can be annexed to an organization's management manual or framework, which brings together all the principles, norms, rules, and standards governing the management and valorization of data and information.

Moreover, these policies can be tied in with a specific information management framework, to guide and standardize decision-making processes. For example, when it comes to managing data access and information usage, the **Five Safes framework**, developed in Great Britain (UK Data Service, 2023), is widely used across the country, notably by Statistics Canada (Figure 9).



FIGURE 9. The Five Safes Framework (Source: UK Data Service)

2.7 CONDITIONS FOR SUCCESS

Lastly, the literature puts forward several conditions to ensure the success of an information and data governance strategy. Here is a summary of these conditions.

GENERAL CONDITIONS

According to AHIMA (2022):

- Prioritize business-critical data to focus efforts and achieve results.
- Assign clear functions across the governance structure with precisely defined roles and responsibilities to ensure a response to any questions or issues that arise.
- Demonstrate the value of governance through key indicators linked to the goals of the programs and projects implemented.
- Support collaboration between governance stakeholders.

According to KPMG (2017):

Have a clear strategy and an achievable plan that includes:

- An honest understanding of the questions the organization is trying to answer in using the data.
- A review of the most appropriate techniques, capabilities, and tools to answer these questions.

According to Oracle (2011):

- Opt for a comprehensive (holistic) approach, but start small.
- Gain executive support.
- Establish roles and responsibilities early in the process.
- List quantifiable benefits in a business case.
- Establish, apply, and report on measures of progress.
- Offer incentives to recognize and encourage stakeholder participation.

Key short-term conditions (KPMG, 2018)

- Be aware that data governance means different things to different people. For some, it could be seen as a control mechanism, rather than a value-generating one.
- Business priorities should drive data governance.
- Start where the need is greatest.
- List the quick wins and show progress early and often to demonstrate the benefits of data governance and create momentum.
- Consider legislative requirements and improve data management processes and analytical reporting.

Key medium-term conditions: Changing the culture

- Align information systems governance and data governance. This can speed up the deployment of a new system, and reduce the risk of failure or cost overruns, particularly when data governance considerations are integrated from the earliest stages of an information system's design and implementation.

Key long-term conditions: Seeing data as wealth

- Help senior leadership talk about data as an organizational asset and encourage a culture of change. The most difficult part, of course, is to go step by step, without rushing the learning process.

All these conditions reflect important actions to be taken by those responsible for developing and implementing an information governance strategy. They are not necessarily a guarantee that all the challenges involved in this arduous task can be met, but they certainly help optimize the financial, material, and human resources invested in operationalizing a governance model.

3. DATA GOVERNANCE MODELS

Having established the main definitions, characteristics, and conditions for the success of information and data governance, we now present the different organizational forms such governance may take. According to the literature, there are several governance models that individuals and organizations can choose to deploy to organize data and information management (Abraham et al., 2019; Gagnon-Turcotte et al., 2021; Health Data Hub, 2021). Not all of these models have been implemented, nor have they yet proved their success or sustainability. However, it is still interesting to draw up a typology of these models, to clarify and illustrate their particular features, while also examining their operating and financing mechanisms.

3.1 TYPOLOGY OF DATA GOVERNANCE MODELS

Literature reviews on governance models highlight the wide array of organizational and management structures for information and data (Al-Badi et al., 2018; McCraig and Rezania, 2021; Tallon et al., 2013). However, several authors, such as Lis and Otto (2021), have proposed clear, structured typologies in order to establish the main dimensions and characteristics of these governance models.

Layer	Dimension	Characteristics			
Interaction	Purpose	Control	Collaboration	Value Creation	Conflict Resolution
	Scope	Intra-organizational		Inter-organizational	
	Phase	Pre-partnership collaboration	Partnership creation	Partnership program delivery	Partnership termination/succession
Governance	Configuration	Centralized		Decentral	Self-organizing
	Structure	Market	Hierarchy	Network	Bazaar
	Mechanism	Formal		Relational	
Data	Data Ownership	Individual		Organizational	Shared
	Decision Rights	Monocentric		Polycentric	

FIGURE 10. Typology of the Data Governance Ecosystem (Lis and Otto, 2021)

A detailed description of the dimensions and characteristics of these governance models can be found in the article (pp. 6070–6072). Given the objective of our research, we have chosen to elaborate on the three dimensions of the governance component, along with the corresponding characteristics.

A. CONFIGURATION: This dimension refers to the positioning of the data management organization within the ecosystem. The configuration therefore determines how decision making and authority over data access and use can be achieved.

Possible characteristics

- **Centralized:** A single platform or organization is responsible for all control and decision-making authority.
- **Decentralized:** Decision-making mechanisms are shared between various actors or structures that operate along common or harmonized operating principles.
- **Self-organizing:** Governance is shared among multiple stakeholders who are organized according to community-based management principles (similar to the open-data movement).

B) STRUCTURE: This dimension describes the governance arrangements in place for the control and implementation of incentives.

Possible characteristics

- **Market:** Governance is governed by strict compliance with contractual clauses. Central coordination is ensured by the price.
- **Hierarchy:** This model is the opposite of the market structure. It is characterized by the exercise of control by one or more dominant authorities.
- **Network:** This model stems from a number of organizations or entities pursuing common objectives and whose capabilities are interdependent. Collaboration along the network is primarily based on reciprocity, shared benefits, and trust.
- **Bazaar:** This alternative governance structure originates from the open source movement. Unlike other models, the bazaar does not require formal contracts or a prior relationship of trust. Contributing members are motivated by the desire to distribute information assets for intrinsic reasons, or to build a reputation within a community.

C) MECHANISM: This dimension refers to the type of control mechanisms that influence behaviour and collaboration dynamics, for example incentives, rewards, and penalties.

Possible characteristics

- **Formal:** These are rules of conduct that are spelled out in the governance structure in such a way as to encourage desirable behaviour and minimize the risk of deviating from the rules.
- **Informal:** These are social norms that can be used in addition to formal regulations, and can be based on the communication of visions and values (such as trust and collaboration) that reinforce stakeholder commitment and respect.

At the heart of this typology, we see the emergence of collaborative governance models, organized in a decentralized or networked manner, in pursuit of a collective or general interest objective. These governance models are sometimes referred to as “**alternative data governance models,**” or “data partnerships” (Gagnon-Turcotte et al., 2021).

According to Gagnon-Turcotte et al. (2021, p. 17), whose report on collaborative data governance models has become a benchmark in Quebec, the term **digital data partnerships** refers to “any initiative in which two or more organizations unite around a common goal, which requires the sharing and leveraging of data.” There are several types of data partnerships, as described in Figure 11 below, taken from the report.

These models are built on collaborative principles and pursue a common interest. They are promising models for non-hierarchical data governance that allow the stakeholders involved to exercise decision-making power and control over data. We will illustrate several of these data partnerships in section 3.4. of this document, to clarify their characteristics.

BOX 3: ALTERNATIVE DATA GOVERNANCE MODELS

DATA COLLABORATIVES

The GovLab defines data collaboratives as forms of partnerships that bring together private companies, research institutions, and government agencies that are designed to combine data and generate public value (Verhulst and Sangokoya, 2015).

DATA COOPERATIVES

Data cooperatives are similar to traditional cooperatives. In that sense, they are a group of people who come together to achieve common goals in a joint organization. Data cooperatives can be defined as mutual “organisation[s] owned and democratically controlled by members, who delegate control over data about them” (Hardinges et al., 2019, p. 9).

DIGITAL COMMONS

Digital commons, on the other hand, are initiatives where individuals or organizations share data as a common resource and collectively set the rules governing access (Bass and Old, 2020).

DATA TRUSTS

Data trusts are defined as legal structures mandated to provide independent stewardship of data for the benefit of their trustees (Hardinges et al., 2019). This model has received a lot of attention in recent years. For example, the Open Data Institute began exploring data trusts with the British government in 2018. What distinguishes data trusts from other models is that the trust is an intermediary distinct from the members of the data sharing initiative.

PERSONAL DATA SOVEREIGNTY

The main feature of personal data sovereignty is that individuals have direct control over their personal information. New digital platforms and initiatives now provide individuals “the means [...] to control, use and share their data – and re-users with whom data subjects decide to share their data” (Micheli et al., 2020, p. 9). In particular, the personal data sovereignty movement has been strengthened by the right to data portability under Article 2, Directive 20, of the General Data Protection Regulation (GDPR) adopted by the European Union.

FIGURE 11. Alternative Data Governance Models (Gagnon-Turcotte et al., 2021)⁵

⁵ The figure in its original size can be found via this link: opennorth.ca/wp-content/uploads/legacy/Digital_Data_Partnerships_Report-EN.pdf (p. 21).

3.2 DATA AND INFORMATION ACCESS LEVELS

A typology of data governance would not be complete without considering the issue of data access levels. In fact, some governance models include **free and open access** to all pooled data or information, particularly when it comes to data collected by public administrations (Brown and Toze, 2017). This is the principle that has underpinned the open data model since its origins (Murray-Rust, 2008).

However, this model can often be difficult to implement for several reasons (Yang and Maxwell, 2011), including:

- Organizations that pool data share sensitive information about their activities, and sometimes want **to protect their intellectual property or competitive position**.
- Organizations or individuals share **personal information about themselves that can be re-identified** and lead to harmful consequences if misused or used without consent. This is the case, for example, with health data.

Consequently, different access levels can be considered when implementing a data and information governance model (Figure 12).

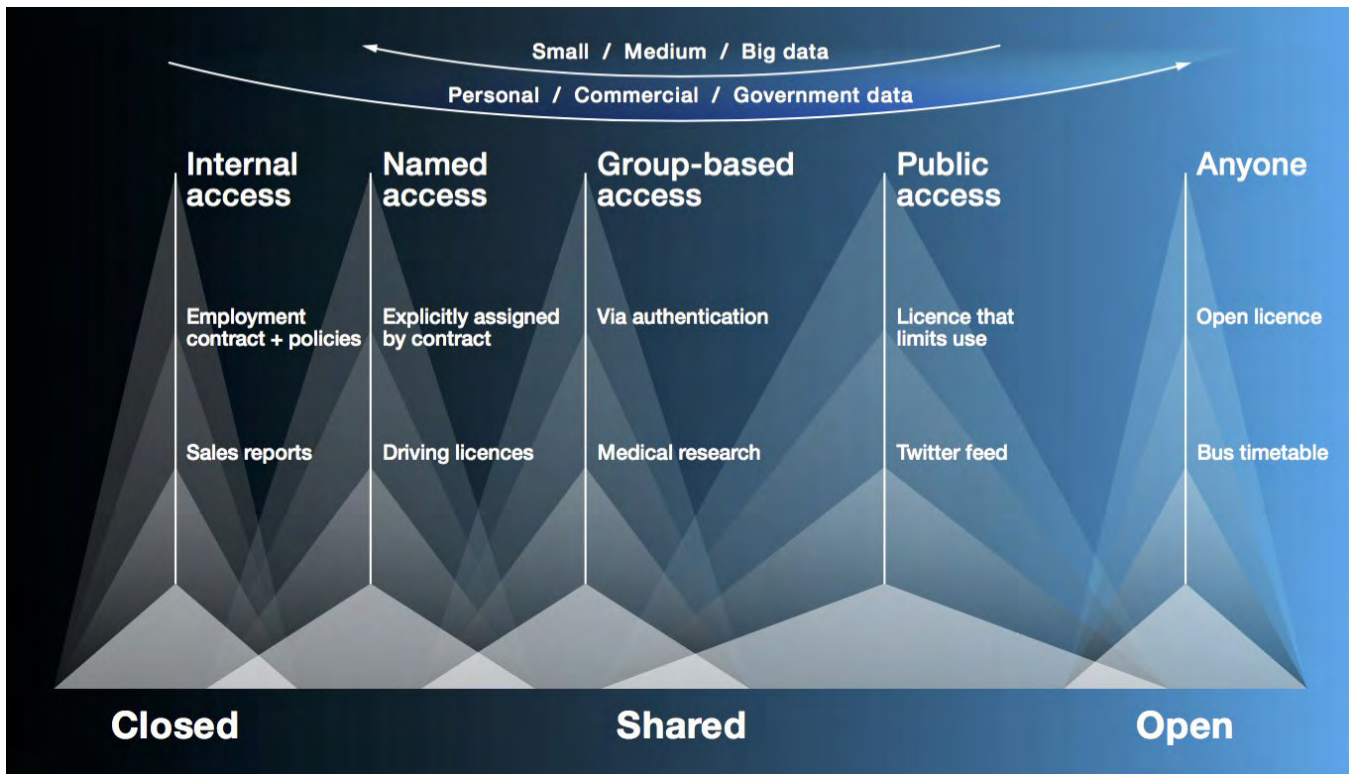


FIGURE 12. The Data Spectrum (Open Data Institute, 2023)⁶

3.3 DATA AND INFORMATION VALORIZATION OPTIONS

Lastly, before illustrating governance models with concrete examples, it is important to discuss how these models can provide **various means for financing their implementation and operation** over the long term. This involves the options chosen to bring value to the data or information of an organization or network of organizations.

Focusing on for-profit organizations, Wixom and Ross (2017) highlight three ways in which businesses can produce value from their data or the data entrusted to them:

- Businesses can use data and analytics to improve their internal processes.
- Businesses can use data to expand their products, services and customer experience.
- Businesses can monetize their data by selling it to third parties.

⁶ The figure in its original size can be found via this link: theodi.org/insights/tools/the-data-spectrum/

These are all **business strategies whose primary aim is to generate profit**. In fact, they are ways of monetizing data or information to generate revenue that exceeds the costs involved in data valorization.

For **not-for-profit organizations**, there are other options for data valorization, with the aim of generating revenue to recover implementation and operating costs, and to ensure the organization's continued purpose in the long term.

The literature highlights several types of business models that can be adapted based on an organization's objectives (Ada Lovelace Institute, 2020; Spiekerman, 2019; Wiener et al., 2020). These are two main types:

- Individuals who share data with the organization may agree to pay a fee in return for services (securing their information, access to analyses and recommendations generated from the data, etc.).
- Individuals seeking access to data can agree to pay user licenses (monthly, yearly, per access, etc.) in return for receiving quality information from the organization.

As a result, the organization does not have to monetize its data or provide direct access to the raw data it holds. It can **market analyses derived from this data**, or "aggregate data," which can produce value for users and present no risk to the confidentiality or privacy of the people who share their data.

Lastly, the organization that manages the data can **offer services** based on data valorization. For example, it could offer:

- Hosting and secure storage services for third-party data.
- Data anonymization and protection services.
- Data management services for people who have neither the expertise nor the infrastructure.
- Consulting services (e.g., legal and ethical) and training in data valorization.

These strategies, far from being exhaustive, nevertheless represent interesting options for financing and sustaining a data and information governance model that adopts a not-for-profit approach and does not aim to commercialize data directly.

However, it is important to note that few organizations in the world have implemented such revenue-generation strategies to pursue a social or general interest objective. This is illustrated by the Ada Lovelace Institute's survey of data trusts in the UK.⁷ It reveals that most of these organizations depend on public and private subsidies to survive.

However, it is possible to identify collaborative data governance models in which successful, self-sufficient strategies have been described over the last few years.

⁷ The Ada Lovelace Institute uses the term data stewards to describe these data trusts.

3.4 EXAMPLES OF DATA AND INFORMATION GOVERNANCE MODELS

We will now explore several models of data and information governance. These models include concrete examples that clarify their scope, governance mechanisms, and data and information valorization models, but do not include models that are specific to Indigenous information governance. They will be presented in the next section of this study.

DATA COMMONS

Definition: A data commons is a pool of data from multiple sources that is stored on a cloud platform to support large-scale data management, analysis, harmonization, and sharing. In addition to making data available, a data commons can focus on providing resources and services (analysis, visualization, etc.) for one or more communities.

Characteristics: In light of the governance model typologies presented above, here are the characteristics of the data commons model.

Model's characteristics	Associated features
Model's objective	Speed up access to and sharing of as much data as possible to encourage collective and collaborative projects
Governance (several options are possible)	Decentralized or self-organizing configuration
	Network or bazaar structure
	Formal and relational regulation mechanisms
Data access	Open or lightly controlled data
Financing strategies (most common options)	Subsidies, fundraising, crowdfunding

Examples:

- NCI Genomic Data Commons: a data commons for cancer genomics data
- European Open Science Cloud: a European partnership supporting open science
- Australian BioCommons: a data commons supporting Australian bioscience
- datacommons.org: a data commons operated by Google

Additional references:

- data.org/guides/3-key-steps-to-a-successful-data-commons/
- opendatacommons.org/
- commonfund.nih.gov/commons

DATA BANK (ALSO KNOWN AS A DATA REPOSITORY)

Definition: A data bank is a collection of databases that are generally structured and organized in such a way as to facilitate information searching and retrieval in order to answer data queries and promote their reuse. A data bank can be centralized or decentralized, in the sense that storage can be in a single location or via a network of servers housed in several organizations.

Characteristics: As the term “data bank” is very common and generic, it can refer to several types of organization. What they all have in common, however, is the use of a structured architecture model and data access mechanisms, ensuring that the bank’s information is protected and controlled. Furthermore, some data banks are built based on the informed consent of individuals to the storage and sharing of their data (e.g., in the healthcare sector).

Model’s characteristics	Associated features
Model’s objective	Promote the structuring and organization of data so as to respond quickly to queries and facilitate data reuse
Governance	Centralized or decentralized configuration
	Hierarchical structure
	Primarily formal regulation mechanisms
Data access	Highly controlled data
Financing strategies (most common options)	Public subsidies and payment of licenses for data access (per use or monthly)

Examples:

- UK Biobank: Great Britain’s genomic data bank
- Sail Data Bank: health data bank in Scotland
- Digital Repository of Ireland: Ireland’s social and cultural data bank
- StatBank Greenland: data bank containing all kinds of information on the population of Greenland

Additional references on data banks:

General articles:

- altametrics.com/blog/data-banks-behind-the-scenes-of-a-data-bank-what-they-can-do.html
- en.wikipedia.org/wiki/Data_bank

DATA TRUST

Definition: In Quebec law, a data trust, known as a “fiducie de données”, is a legal vehicle for holding and administering the information assets of individuals according to the purpose they choose (this is the “affectation” of the “fiducie”). The administration of a trust is assumed by a trustee. When a trust pursues an objective of general interest, it is referred to as a social utility trust, a legal concept found in the Civil Code of Quebec under the name “fiducie d’utilité sociale”. In the anglosaxon realm, the concept of data trust covers a large number of organizations that do not always have the same legal status: cooperatives, not-for-profit organizations, collective enterprises, and so on.

Characteristics: Data trusts can have a wide range of characteristics. They do, however, have a central mechanism and objective at their core: to ensure trust between the people who share their data and the trustee who manages it, in pursuit of a collective or societal goal.

Model's characteristic	Associated features
Model's objective	Promote confidence in the use and protection of data entrusted to the trustee by the people who produce the data
Governance (several options are possible)	Centralized or decentralized configuration
	Hierarchical or network structure
	Formal (trust agreements) and relational (shared visions and values) regulation mechanisms
Data access	Data controlled according to strict rules
Financing strategies	They can be many and varied: subsidies, fundraising, crowdfunding, sale of services associated with data, etc.

Examples:

- Pilot by the Open Data Institute at the Greater London Authority (GLA) and the Royal Borough of Greenwich (RBG), managing energy and mobility data for several public and private organizations
- Place in the United States and the United Kingdom: a data trust for geospatial and geographic data
- UK Cystic Fibrosis Registry: a secure, centralized database sponsored and managed by the Cystic Fibrosis Trust. Non-identifiable data from the registry is used to improve the health of people with cystic fibrosis through research.

Additional references:

TIESS (Territoires innovants de l'économie sociale et solidaire) resources:

- tiess.ca/les-fiducies-dutilite-sociale-synthese-de-connaissances/
- tiess.ca/gouvernance-des-donnees-la-fiducie-dutilite-sociale-un-outil-a-fort-potentiel/

Database developed by the Ada Lovelace Institute:

- docs.google.com/spreadsheets/d/1hAN8xMJuxobjARAWprZjtcZgq1lwOiFT7hf2UsiR-BYU/edit#gid=432908716

DATA INTERMEDIARY

Definition: A data intermediary is a platform that offers individuals or organizations a range of services for storing, protecting, managing and adding value to their data. While providing these services, the intermediary ensures that individuals or organizations have control over how their data is used. Platforms performing this role are commonly referred to as personal data stores, data hubs, or data platforms. Individuals or organizations are invited to provide their data to the intermediary, and to choose with whom and for what purposes they wish to share it.

Characteristics: Data intermediaries can be run by companies or non-profit organizations. In all cases, they generally adopt an autonomous funding model based on user payment for data access and the implementation of a reward system for data providers.

Model's characteristic	Associated features
Model's objective	Increase people's control over their data and enable them to obtain services (storage, protection, etc.) and rewards for their data (money, services, etc.).
Governance (several options are possible)	Self-organizing configuration, even though the platform is centralized
	Market (profit model) or network structure (non-profit model)
	Formal regulation mechanisms (platform rules)
Data access	Individually controlled data
Financing strategies	Payment of licenses for data access (per use or monthly), with prices varying based on user type

Examples:

- Geens: a Belgian non-profit platform that allows individuals and organizations to entrust the platform with their sensitive data and choose with whom they wish to share it
- Cozy.io: a French website that lets users store their data securely for a fee, and to use it easily
- CityVerve Manchester: a platform for connecting data from the connected applications of individuals and organizations (Internet of Things and Smart City vision)

DATA COOPERATIVE

Definition: A data cooperative refers to the voluntary and collaborative pooling of personal data by individuals for the benefit of their group members or society as a whole. Individuals are motivated to come together and pool their data for a number of reasons, including the desire and need to share common information that would otherwise be siloed or inaccessible. This information provides cooperative members with a better understanding of their living conditions, habits, preferences, and activities, while at the same time guaranteeing control over the data, particularly with regard to the uses to which it is put.

Characteristic: Data cooperatives are essentially owned and managed by the members who contribute to the sharing of data. In principle, all members have decision-making power, which may be proportional to their personal investment in the activities of the cooperative and the responsibilities they come to assume. The benefits of a cooperative are passed on to its members and contributors.

Model's characteristic	Associated features
Model's objective	Increase people's control over their data and guarantee benefits for themselves and, more broadly, for society
Governance	Centralized configuration
	Hierarchical or network structure
	Formal (articles of incorporation and rules) and relational (shared visions and values) regulation mechanisms
Data access	Data controlled according to strict rules
Financing strategies	They can be many and varied: subsidies, fund-raising, participatory financing, sale of services associated with data, etc.

Examples:

- Health Bank: A platform for the exchange of health data “belonging to individuals.” It allows people to share data with “doctors, care teams, relatives, and anyone else with an Internet connection.”
- Holland Health Data Coöperatie: This Dutch cooperative offers people the opportunity to manage their own data and make it available to third parties for research purposes and in the service of personalized health, giving citizens control over their data.
- Midata Switzerland: The cooperative enables citizens to collect their health data and freely decide how the data will be used in research projects. In this way, they can actively contribute to medical research as “citizen scientists”.
- Salus Coop in Catalonia: This cooperative aims to legitimize the right of citizens to control their own medical records, while facilitating data sharing to accelerate innovation in healthcare research.

Additional references:

- Article on the Data Lama website
datalama.ca/cooperative-de-donnees/
- Chapter from the book by Alex Pentland and Thomas Hardjono (MIT)
wip.mitpress.mit.edu/pub/pnxgvubq/release/2
- Blog article by Sameer Mehta, Milind Dawande, and Vijay Mookerjee (LSE)
blogs.lse.ac.uk/businessreview/2021/08/02/can-data-cooperatives-sustain-themselves/

DATA PLATFORM

Definition: This governance model ensures collaboration between several data-holding organizations, and aims to promote unified, coordinated management of data access and use by its stakeholders. A data platform can have various levels of complexity and characteristics.

Characteristics:

- Level 1 – Data directory: This platform simply lists the types of data held by data-holding organizations, in order to facilitate their discoverability.
- Level 2 – Access gatekeeper: This platform is responsible for receiving and administering data access and service requests from external users. These users then have to contact the organizations holding the data to have their request met.
- Level 3 – Access gateway: This platform not only receives data access requests, but also administers data access for authorized users. Connected to data-holding organizations, this platform features a state-of-the-art data storage, preparation, and delivery infrastructure to ensure confidentiality protection and access management.
- Level 4 – Service offer: In addition to or as a substitute for data access, the platform can offer a range of services to its members or users, such as data hosting services, complex analyses, training, and advice on data protection and valorization, organization of networking activities, etc.

Examples for each level of platform complexity:

- Data directory: [UK Health Data Gateway](#)
- Access gatekeeper: [CESREES](#) (Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé), in France, or any other ethics committee with authority over the decision to access data, without providing technical access to the data.
- Access gateway: [FinData](#), in Finland, is a platform for accessing data from the country's public bodies.
- Service offer: The [Amsterdam Smart City](#) platform acts as a connector between individuals and organizations working in the field of data valorization and open innovation in the urban environment. In France, Ekitia offers a complete range of services around data usage; from legal advice to the certification of a socially responsible organization through an audit of its data-related activities.

4. RECONCILING THE MODELS AND PRINCIPLES OF INDIGENOUS INFORMATION GOVERNANCE

Having outlined and described several data governance models, we now turn our attention to how these can be reconciled with the principles and objectives of the First Nations information governance strategy. The challenge is not only to analyze the strengths and weaknesses of each model in terms of First Nations values and interests, but also to present examples of Indigenous information governance structures. This will enable us to contemplate new avenues for structuring a network of Indigenous information governance centres across Canada's various communities.

4.1 STRENGTHS AND WEAKNESSES OF DATA GOVERNANCE MODELS

The First Nations Data Governance Strategy (2020) action plan calls for the implementation of a **national network of regional information governance centres**. As part of this strategy, several governance model options could be adopted, depending on regional realities and the types of data considered. It is therefore important to understand the potential offered by each of these models, as well as their main limitations, so as to respect and promote the principles of Indigenous information governance.

The OCAP® principles can serve as a starting point for us to grasp the foundations of First Nations information governance (FNQLHSSC, 2016). The principles of **ownership, control, access, and possession** assert that First Nations have control over data collection processes, and that they own and control the way in which this information can be used.

In addition to the OCAP® principles, the CARE Principles for Indigenous Data Governance were developed by the Global Indigenous Data Alliance (GIDA) in 2019, complementing the FAIR Principles and advances in open science (Carroll et al., 2021). The CARE Principles highlight the following considerations:

- **Collective benefit:** Indigenous communities must be able to benefit from data concerning them.
- **Authority to control:** The interests and rights of Indigenous communities with regard to their data must be recognized, and they must be able to exercise control over its use and the benefits derived from it.
- **Responsibility:** Individuals working with Indigenous data must ensure transparency in data use and promote the self-determination, control, and collective benefits of Indigenous communities.
- **Ethics:** Respect for the rights of Indigenous communities and the pursuit of their well-being must be central to the concerns of those using Indigenous data, throughout the data lifecycle and its entire ecosystem.

With these principles in mind, it is possible to assess how the governance models presented in the previous section are more or less conducive to the achievement of First Nation governance aspirations and projects concerning the use and valorization of their data.

DATA COMMONS MODEL

Strength: Based on the principles of Indigenous information governance, the data commons model increases the availability of data, makes it accessible to a large number of people, and potentially increases the collective benefit to people from the use of this information.

Weakness: This model is not suitable, however, for sensitive or confidential data, nor does it allow strict control over the use of data by those who have access to it.

Example of this model in the context of Indigenous governance

Kipuka Database in Native Hawaiian Territory

The Kipuka Database created by the Office of Hawaiian Affairs (OHA) is an information system featuring mapping technology to provide a window on the land, culture, and history of Hawaii. Kipuka visually combines historical, demographic, and cultural data with geographic locations to highlight the richness and diversity of Hawaii's indigenous heritage. The aim of this platform is to catalogue the cultural and geographical data that will help forge new relationships between First Nations and their territories.

References:

- For more information: kipukadatabase.com/
- To see an example of a virtual map: kipukadatabase.com/Apps/NHData/

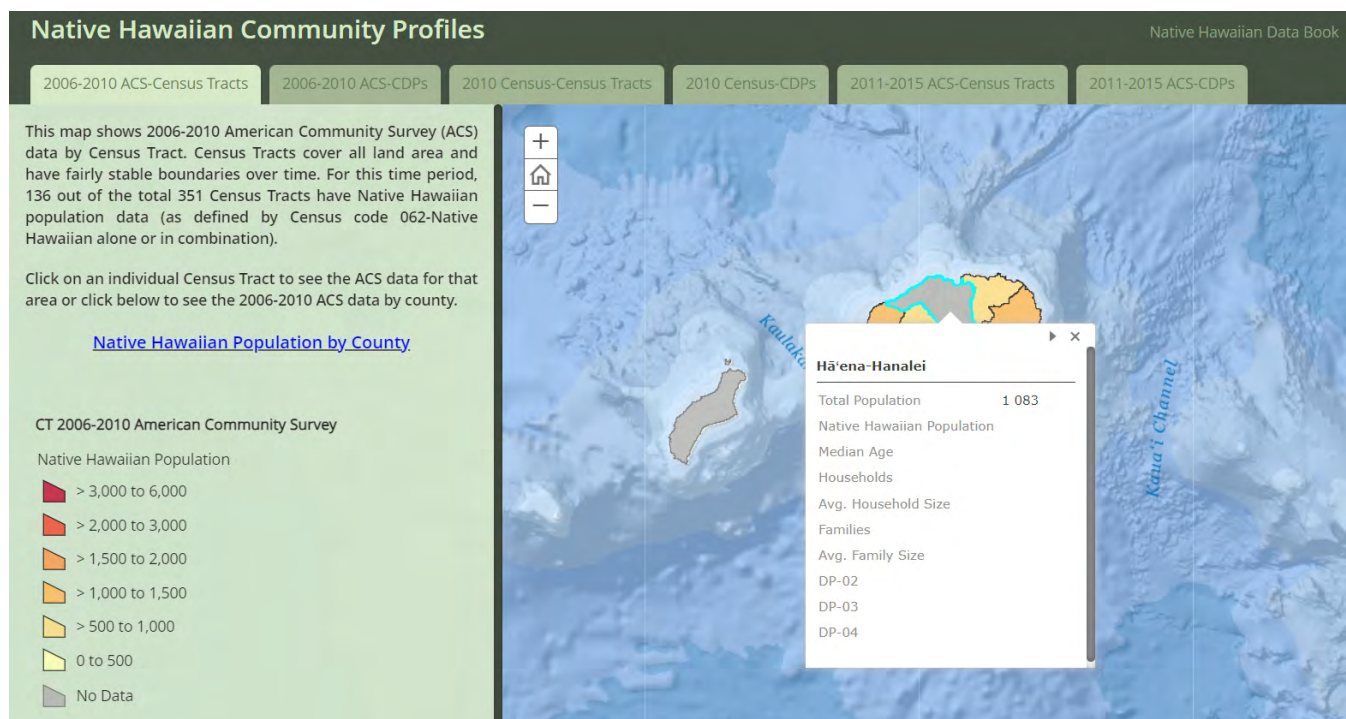


FIGURE 13. Extract of a Dynamic Map on the Sociodemographic Profile of Hawaiian Communities⁸

⁸ The figure in its original size can be found via this link: kipukadatabase.com/Apps/NHData/.

DATA BANK MODEL

Strength: The data bank model is well suited to exercising collective ownership and possession over data, insofar as access to data can be fully controlled. It thus makes it possible to protect sensitive or confidential information such as health or financial data.

Weakness: This model, however, requires that a relatively complex and expensive infrastructure be put in place, especially as the number of databases and data users grow. In addition, it does not allow individual control over data use.

Example of this model in the context of Indigenous governance

Information Governance Based on the Tui'kn Partnership (Nova Scotia)

The Tui'kn Partnership (an initiative of the Eskasoni, Membertou, Potlotek, Wagmatcook, and Waycobah Nations) established a roadmap in 2015 for the implementation of a **centre of excellence for First Nations information management**, with the support of the Government of Nova Scotia. The centre of excellence has set itself the mission of:

- supporting the analysis of health information and community health applications for planning and decision making;
- providing training and education initiatives to build First Nations capacity in health information management, community health planning, and evaluation;
- creating and introducing applications, such as telemedicine and other digital applications; and
- enabling more effective management of financial information and evaluation results and reports for accountability purposes.

The centre of excellence also aims to create and administer a data repository to gather information collected by First Nations and provincial and federal governments. Lastly, the centre would like to be able to offer assistance services to local populations and staff for health information management.

References:

- www.tuikn.ca/
- www.tuikn.ca/wp-content/uploads/2014/02/tuikn_health_information_banner.pdf
- www.tuikn.ca/wp-content/uploads/2014/02/tuikn_health_information_brochure.pdf

Building a First Nations Health Information Management System

While we secure long term funding to unlock the full potential of our work, we have established proof of concept with our partners through a number of project-based innovations. All of this work represents the building blocks of a comprehensive and sustained model of First Nations health information management.

Data Sharing Agreement

A multi-lateral Data Sharing Agreement was signed by the five First Nations and the Nova Scotia Minister of Health.

The complexity of the relationships and inherent data hand-offs between jurisdictions required close attention to the legal and contractual obligations of the parties involved in the data sharing agreement.

A “Privacy Sensitive” Culture

We are fostering a “privacy sensitive” culture within our organizations through regular privacy reviews, privacy training and the development of a comprehensive privacy policy framework and procedures.

As part of our strategy, we have completed privacy impact assessments that identify potential privacy and data protection risks and mitigation strategies, and have created strong legal and service agreements that protect personal and community information.

Chronic Disease Surveillance

Our communities are working with the Population Health Research Unit at Dalhousie University to develop a surveillance monitoring system that encompasses all of the current chronic disease categories currently being evaluated by the Public Health Agency of Canada (Arthritis, Asthma and COPD, Diabetes, Cardiovascular disease, Cancer, and Mental Illness). This two-year project is funded by the Public Health Agency of Canada's Enhanced Surveillance for Chronic Disease Program.

Given the significant impact of diabetes on the First Nations population, we are giving specific attention to this issue in its own project.

Data Linkage Model

Our data linkage model enables First Nations' health information to be pulled from administrative data. This model involves:

- The five First Nations in Cape Breton;
- Medavie (Nova Scotia's administrator of the Medical Services Insurance system);
- Nova Scotia Department of Health and three participating provincial programs:
 - » Reproductive Care Program of Nova Scotia,
 - » Cardiovascular Care Nova Scotia, and
 - » Cancer Care Nova Scotia;
- Cape Breton District Health Authority
- Guysborough Antigonish Strait Health Authority
- The Population Health Research Unit at Dalhousie University
- Indian and Northern Affairs Canada
- Dymaxion (our software supplier)

Epidemiological Training

In order to be custodians of our own health information, it is necessary for local staff to be skilled in all aspects of data collection and interpretation. This capacity building is central to our comprehensive strategy to improve the quality of health planning, management and evaluation.

Data Access Process and Protocols

We have created a data access process and the Unama'ki Data Access Committee, which reviews all requests for access to the registry's data holdings. This process is respectful of both OCAP principles surrounding First Nations data and the Department of Health's legal and policy requirements surrounding the Nova Scotia Health Card Registry.

A Web-based Reporting Tool

The creation and implementation of a web-based reporting tool will provide trained Unama'ki health centre staff with real-time access to aggregate and de-identified Unama'ki health information for routine planning, reporting and evaluation purposes. It will also allow the health centres to respond in a timely way to requests for information at the local level and from partners at the District, Provincial and Federal levels.

FIGURE 14. Building a First Nations Health Information Management System⁹

DATA TRUST MODEL

Strength: The trust model makes it possible to delegate control over data to a trusted third party to promote collective information governance. This type of delegated management is likely to bring efficiency and fluidity to information governance, by allowing the application of standardized procedures and processes for managing access to data.

Weakness: This model does not provide for individual control over data usage. In fact, individuals and communities agree to entrust the management of their information to the trust through a system of delegation of consent and decision making. The trust, for its part, undertakes in a constitution to respect the wishes and preferences of the people and communities

⁹ The figure in its original size can be found via this link: www.tuikn.ca/wp-content/uploads/2014/02/tuikn_health_information_brochure.pdf.

sharing their data. Therefore, a robust mechanism for transparency and accountability to stakeholders must be put in place.

Example of this model in the context of Indigenous governance

Te Kāhui Rongoā Trust and Data Governance in Māori Territories

Established in New Zealand in 2009 at the instigation of indigenous communities and the Ministry of Health, the Te Kāhui Rongoā Trust (TKR) is the collective of Māori healers. This Trust is specifically responsible for the governance of information relating to the health and well-being of communities and their historical and cultural heritage. As such, TKR is responsible for the analysis and approval of research projects conducted in and with Maori communities, and can decide on the terms of use and sharing of the resulting research data. In this respect, the TKR acts as a data trust, although the Trust seems to lack the resources to carry out all of these mandates (Boulton et al., 2014).

References:

- For more information: www.rongoamaori.org.nz/
- Research article in collaboration with TKR: [Boulton et al. \(2014\)](#)

DATA INTERMEDIARY MODEL

Strength: This model has the advantage of promoting individual control over data use by allowing each person or community to decide on the types of data shared, the authorized uses, and the time of data sharing.

Weakness: This model, however, involves significant installation and implementation costs, as a robust, agile, and highly-secure platform must be put in place to ensure individual possession, ownership, and control over access to information.

We were unable to find an example of an Indigenous information governance structure that fits this model.

DATA COOPERATIVE MODEL

Strength: The cooperative model reflects the Indigenous approach to collective and participatory governance in the management of its information assets. This model gives equal voice to each member of the cooperative, while establishing joint and shared governance principles to ensure respect for ethics and responsibility.

Weakness: This model relies on the active participation of cooperative members in activities relating to data management and use. To ensure compliance with the principle of participative governance, it is therefore difficult for a cooperative to include a large number of members, unless it is organized as committees and subcommittees, thereby ensuring horizontal governance and a fair redistribution of benefits among cooperative members.

Example

Indigenous Cooperatives in Canada

Given the small number of data cooperatives in the world, we were unable to identify such a model within an Indigenous community. Nevertheless, the cooperative approach (based on self-management of the means of production) has been quite successful in the First Nations, Inuit, and Métis territories of North America. In Canada, in 2012, there were 123 cooperatives with several thousand members. Arctic Cooperatives Limited, which includes cooperatives in Nunavut and the Northwest Territories, has some 22,000 participating members.

References:

- Article on Indigenous cooperatives in Canada: [Cooperatives-First \(2018\)](#)
 - Report on Indigenous Cooperatives in Canada: [Canadian Co-operative Association \(2012\)](#)
 - Arctic Co-operatives Limited website: arctic-coop.com/
 - Indigenizing the Co-operative Model: [Article by Thunder and Intertas \(2020\)](#)
-

DATA PLATFORM MODEL

Strength: This model offers a high degree of flexibility for the governance of Indigenous community information, insofar as it offers the choice of a variety of data management and sharing modalities: from the provision of data-related services (ethics, law, management, etc.) to the connection of databases to promote access through a single gateway. A platform model enables a variety of governance modes to be established, providing individual and/or collective control over data access decisions, depending on the management frameworks and procedures chosen by the community.

Weakness: The platform model has various limitations, depending on the community's choice of platform. If the community opts for a platform that provides access to data, implementation and operationalization costs can be high, as with a data bank. If, on the other hand, the community chooses a platform that only provides consulting services or a directory of available databases, costs can be considerably reduced, as can the risks associated with data use (confidentiality, cybersecurity, etc.).

Example of this model in the context of Indigenous governance

Papakilo: Hawaiian Database Platform

Administered by the Office of Hawaiian Affairs (OHA) since 2009, Papakilo is described as the “database of databases”. It contains a diverse collection of data on places, events, and documents of historical and cultural significance in Native Hawaiian history. This online data repository serves to enhance OHA's ability to preserve and perpetuate First Nations cultural and historical information and practices.

Papakilo is also based on a number of principles and objectives aimed at preserving and enriching the informational and cultural heritage of Native Hawaiian communities.

“**Aina:** To maintain the connection to the past and a viable land base, Native Hawaiians will participate in and benefit from responsible stewardship of Ka Pae 'Aina O Hawai'i (manifesto of self-determination and independence).

Mo'omeheu: To strengthen identity, Native Hawaiians will preserve, practice and perpetuate their culture.

Ho'ona'auao: To maximize choices of life and work, Native Hawaiians will gain knowledge and excel in educational opportunities at all levels.”¹⁰

¹⁰ Excerpted and adapted from: www.papakilodatabase.com/main/about.php.

References:

- Papakilo website: www.papakilodatabase.com/main/about.php
- List of reviewed and accessible databases: www.papakilodatabase.com/main/tutorial.php



FIGURE 15. Objectives Underlying the Creation of the Papakilo Database¹¹

¹¹ This figure in its original size can be found via this link: www.papakilodatabase.com/main/about.php.

4.2 CHOOSING ONE OR MORE GOVERNANCE MODELS

Finally, which governance model should be chosen for data and information management that respects the principles and objectives of Indigenous communities? Such a question cannot be answered, as there is no single model that is compatible with an Indigenous information governance strategy. Rather, a trade-off must be made between several models, in order to choose information governance structures that are best suited to the priorities established for the collection, use, storage, and sharing of data.

To illustrate how such a trade-off can take place, we have divided the guiding principles of Indigenous data governance into two groups.

- On the one hand, there are principles that demonstrate the importance of maintaining control over information and its use: ownership, control, possession, authority. These principles are grouped under the term **CONTROL**.
- On the other hand, there are principles that underscore the importance of guaranteeing the creation of benefits for all community members: access, collective benefit, ethics, responsibility. These principles are grouped under the term **BENEFIT**.

Based on these two groupings of principles—control over data and the benefits it can provide—we can build a simplified diagram that positions the six governance models studied above in relation to these two components (Figure 16).

Figure 16 clearly shows that **a compromise has to be made** between, on the one hand, the degree of control and protection wanted for data, for example, through barriers to access, and, on the other hand, the desire to allow a greater number of individuals to use data to generate benefits for communities. In fact, overly protected data can certainly be well controlled, but can quickly become difficult to access. Conversely, open data severely limits the control that individuals can exercise over its use, but ensures that as many people as possible can access and use it for research, analysis, and studies leading to improvements for communities.

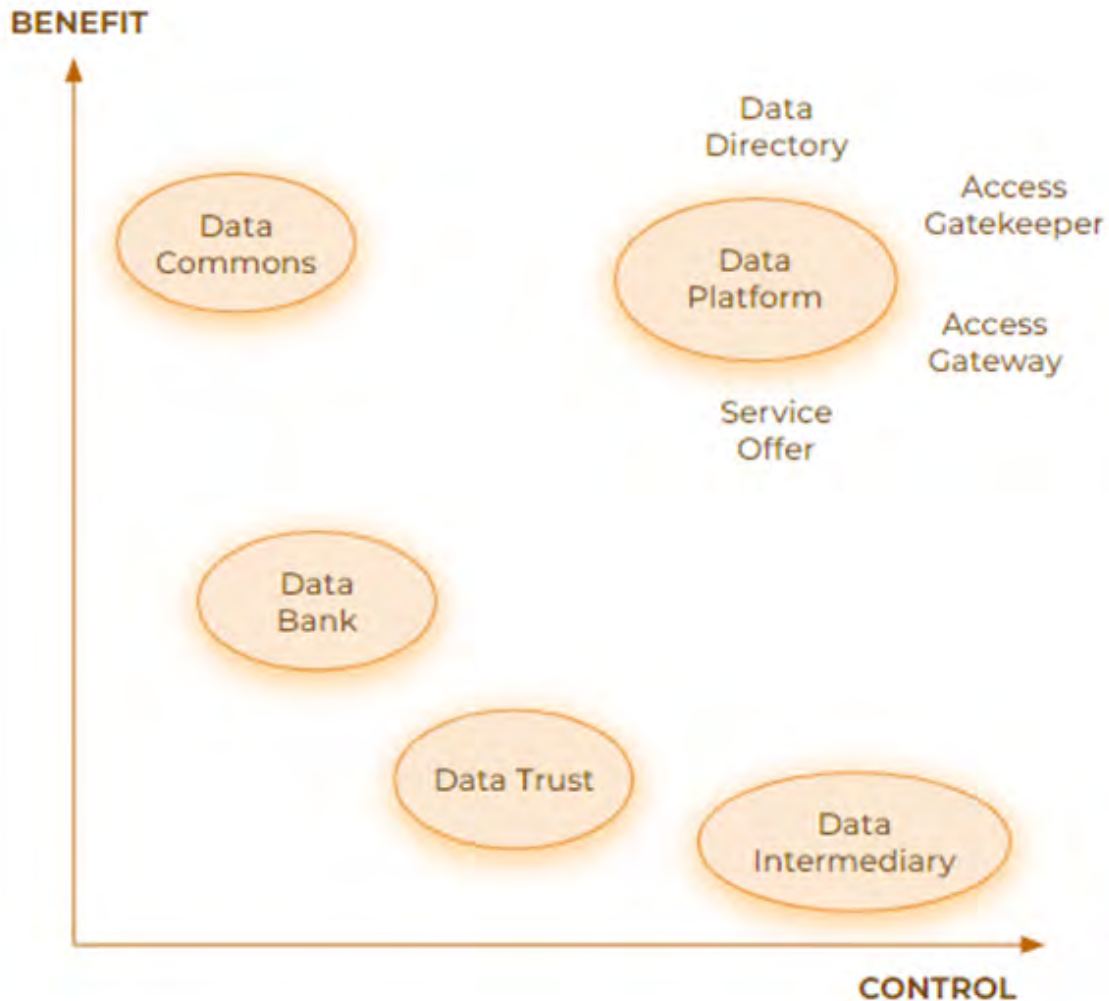


FIGURE 16. Trade-off Between Control Over Data and the Benefits of Opening It Up to a Wider Range of Users (developed by the author)

4.3 NETWORK OF MODELS AND ORGANIZATIONS

Lastly, the information governance of Indigenous communities could well be based on a set of models chosen according to their features and strengths. For example, some organizations might decide to establish a **data commons** to share geographic and sociodemographic data without risk to privacy, while others might lean towards a protected **data bank** to manage access to sensitive information, such as population genetic data.

The challenge remains that of harmonizing the various models chosen, so as to ensure that **unified governance** can be implemented to promote the sovereignty of Indigenous communities and enhance their ability to use data for the benefit of their people. Such unified governance can be structured by setting up a network dedicated to fostering connections between data stakeholders and the harmonization of Indigenous information management practices.

To this end, a number of networks around the world focus on the sovereignty of Indigenous information (Caroll et al. 2019). Here are a few examples:

- Mana Raraunga, Maori network based in Aotearoa, New Zealand, founded in 2015.
- United States Indigenous Data Sovereignty Network (USIDSN) launched in 2016 (website no longer active).
- Maiaṃ nayri Wingara Aboriginal and Torres Strait Islander Data Sovereignty Collective created in Australia in 2017.
- Global Indigenous Data Alliance grew out of the three previous networks and was founded in 2019, at the same time as the publication of the CARE Principles.
- Data Alliance's International Indigenous Data Sovereignty Working Group launched in 2021.
- First Nations Information Governance Centre (FNIGC), in Canada.

These networks can serve as pivotal actors for the sharing of information and expertise, as well as alignment between the management principles and practices of various structures responsible for Indigenous information governance.

Moreover, in the health data ecosystem, there are several bodies that could serve as sources of inspiration in considering the roles and responsibilities that a First Nations data governance network could assume. One such example is Health Data Research Network Canada. Incorporated as a non-profit corporation in 2020, the Network serves as a platform for exchanging information and expertise on access and use of health data across the country. In addition to facilitating the discoverability of health data and access to this data for research, the Network has a council of citizens and experts which focuses on the social acceptability of the use of data. Through its research and consultations, it is able to develop practice frameworks and recommendations for data management that are based on the expectations and needs of Canadian populations.

4.4 CONCLUSION AND RECOMMENDATIONS

In light of this analysis, we could finally draw up a set of recommendations concerning the form and functions that a Canadian network of regional information governance centres could take, as projected in the 2020 First Nations Data Governance Strategy.

Firstly, regional governance centres could be organized as **data platforms**. All the data for a region would not necessarily be stored in the centres themselves, but could be kept in the organizations holding the data (social service centres, dispensaries, schools, etc.), which would then be connected to the centre. The primary objective would be to identify existing data sources in a given territory, and to ensure that they are easily accessible in a predictable and reasonable manner and timeframe.

As a data platform, a **regional governance centre** would support the following roles and responsibilities:

- Building an up-to-date data directory listing databases, access procedures, and permitted uses.
- Establishing an access point to manage data requests from authorized users.
- Setting up a storage and analysis infrastructure capable of producing information from the data, analyzing it, and sending it to the various federal, provincial, and community authorities.
- Developing a range of services focused on data valorization: data structuring, ethical and legal advice, knowledge sharing, training, etc.

As a minimum, each regional information governance centre should have:

- A data governance and management framework, which could include different modalities for opening up data (from open data to closed data, via controlled access), depending on their level of sensitivity.
- Policies and procedures to ensure data security, confidentiality (for sensitive data), access management, data quality and integrity, among others.
- A technological infrastructure that is sufficiently advanced, up to date, and secure to ensure the quality, value, and management of information.
- Qualified staff in the fields of data preparation and analysis, and in the governance and management of data access and use.

Information governance centres would be organized **as a network** so that their policies, procedures, and practices could be harmonized. Moreover, without pooling all their data (at the very least, only the least sensitive ones), centres could bring together their **data repositories** to inform all communities of the data available across the centres, and how to access it. As we have seen, Indigenous and non-Indigenous models could serve as inspiration for building a network that would link **a constellation of connected platforms** in the field of First Nations information governance.

Lastly, to ensure that the network and the regional information governance centres are rooted in community life, and that their activities are continuously aligned with the principles and values of people, these organizations should certainly develop an **active program of consultation, information, and participation** involving the various stakeholders. In this respect, there are many inspiring models of citizen engagement concerning data. This could be the subject of an additional literature review to complement this document.

5. REFERENCES

- Abraham, René, Johannes Schneider, and Jan vom Brocke. 2019. "Data governance: A conceptual framework, structured review, and research agenda." *International Journal of Information Management* 49 (December): 424-438. <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>.
- Ada Lovelace Institute. 2020. *Exploring principles for data stewardship*. London: ALI. <https://www.adalovelaceinstitute.org/project/exploring-principles-for-data-stewardship/>.
- American Health Information Management Association. 2022. *Healthcare Data Governance*. Chicago: AHIMA. <https://www.ahima.org/media/pmcb0fr5/healthcare-data-governance-practice-brief-final.pdf>.
- Al-Badi, Ali, Ali Tarhini, and Asharul Islam Khan. 2018. "Exploring Big Data Governance Frameworks." *Procedia Computer Science* 141 (November): 271-277. <https://doi.org/10.1016/j.procs.2018.10.181>.
- Alhassan, Ibrahim, David Sammon, and Mary Daly. 2016. "Data governance activities: An analysis of the literature." *Journal of Decision Systems* 25, no. 1 (June): 64-75. <https://doi.org/10.1080/12460125.2016.1187397>.
- ARMA. 2022. "ARMA International Information Governance Implementation Model." Arma Resources. Accessed January 26, 2023. <https://www.arma.org/page/igim>.
- Bennett, Susan. 2017. "What is information governance and how does it differ from data governance?" *Governance Directions* 69, no. 8 (September): 462-467. https://www.sibenco.com/wp-content/uploads/2017/09/Information_governance_data_governance_September_2017.pdf.
- Boulton, Amohia, Maui Hudson, Annabel Ahuriri-Driscoll, and Albert Stewart. 2014. "Enacting Kaitiakitanga: Challenges and Complexities in the Governance and Ownership of Rongoā Research Information." *The International Indigenous Policy Journal* 5, no. 2 (April): 1. <https://doi.org/10.18584/iipj.2014.5.2.1>.
- Brown, David C. G., and Sandra Toze. 2017. "Information governance in digitized public administration." *Canadian Public Administration* 60, no. 4 (November): 581-604. <https://doi.org/10.1111/capa.12227>.
- Bruhn, Jodi. 2014. "Identifying Useful Approaches to the Governance of Indigenous Data." *International Indigenous Policy Journal* 5, no. 2 (April): 1-32. <https://doi.org/10.18584/iipj.2014.5.2.5>.
- Canadian Institute for Health Information. 2020. Health data and information governance and capability framework. Canada: CIHI. <https://www.cihi.ca/en/health-data-and-information-governance-and-capability-framework>.
- Carroll, Stephanie Russo, Edit Herczog, Maui Hudson, Keith Russell, and Shelley Stall. 2021. "Operationalizing the CARE and FAIR Principles for Indigenous data futures." *Scientific Data* 8, no. 1 (April): 108. <https://doi.org/10.1038/s41597-021-00892-0>.
- Carroll, Stephanie Russo, Desi Rodriguez-Lonebear, and Andrew Martinez. 2019. "Indigenous Data Governance: Strategies from United States Native Nations." *Data Science Journal* 18, no. 1 (September): 31. <https://doi.org/10.5334/dsj-2019-031>.
- Carvalho, João Vidal, Álvaro Rocha, José Vasconcelos, and António Abreu. 2019. "A health data analytics maturity model for hospitals information systems." *International Journal of Information Management* 46 (June): 278-285. <https://doi.org/10.1016/j.ijinfomgt.2018.07.001>.
- Data Governance Institute. 2020. "DGI Data Governance Framework." Accessed January 22, 2024. <https://datagovernance.com/the-dgi-data-governance-framework/>.
- Data Governance Institute. 2023. "Definitions of Data Governance." Accessed February 22, 2024. <https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/>.
- Data Trusts Initiative. 2020. "Selecting a data sharing structure: A value-based choice." Accessed February 22, 2024. <https://datatrusts.uk/blogs/selectingdatastructures>.

- DataGov Lab. 2021. *Data Governance – Tools & Solutions* (Version 1.0). Paris: ARISS. https://ariis.fr/wp-content/uploads/2021/09/2021-07_DataGov-Lab-BookV1.0-July2021.pdf.
- Deloitte. 2015. *NHS Briefing: Data Governance and Analytics Effectiveness*. London: Deloitte LLP. <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-nhs-briefings-data-governance-analytics-effectiveness.pdf>.
- Earley, Susan, Deborah Henderson, and Data Management Association. 2017. *DAMA-DMBOK: Data Management Body of Knowledge*, 2nd ed. Sedona: Technics Publications.
- First Nations Information Governance Centre. 2020. "First Nations Data Governance Strategy." Accessed February 22, 2024. <https://fnigc.ca/what-we-do/first-nations-data-governance-strategy/>
- First Nations of Quebec and Labrador Health and Social Services Commission. 2016. OCAP® *Reminder*. Wendake: FNQLHSSC. <https://cssspnql.com/en/produit/aide-memoire-pcap-ocap-reminder-2016/>
- Fuller, Shannon. 2018. "Examining the Importance of Data Governance in Healthcare." *Journal of AHIMA* 89, no. 10 (December): 42-44. <https://www.proquest.com/docview/2124682601?sourcetype=Trade%20Journals>
- Gagnon-Turcotte, Sarah, Miranda Sculthorp, and Steve Coutts. 2021. *Digital Data Partnerships*. Montreal: Open North. <https://opennorth.ca/resources/digital-data-partnerships/>
- Gartner Glossary. 2023. "Information Governance." Information Technology Glossary. Accessed February 22, 2024. <https://www.gartner.com/en/information-technology/glossary/information-governance>.
- Gentelet, Karine, and Alexandra Bahary-Dionne. 2021. "First Peoples' digital data strategies: decolonization and sovereignty." *tic&société* 15, no. 1 (May): 189-208. <https://journals.openedition.org/ticetsociete/6063?lang=en>
- Health Data Hub. 2021. *Health data access and data governance structures: International benchmark 2020*. Paris: HDH. https://www.health-data-hub.fr/sites/default/files/2021-07/EN_Pr%C3%A9sentation%20de%20restitution%20BK%202020%20-%2020210720_revu%20charte.pdf
- International Organization for Standardization. 2015. *Information technology—Governance of IT for the organization* (ISO/IEC 38500:2015). ISO. <https://www.iso.org/fr/standard/62816.html>.
- International Organization for Standardization. 2017. *Information technology—Governance of IT—Governance of Data* (ISO/IEC 38505-1:2017). ISO. <https://www.iso.org/standard/56639.html>.
- International Organization for Standardization. 2022. *Information and documentation—Information governance—Concept and principles* (ISO 24143:2022). ISO. <https://www.iso.org/standard/77915.html>.
- KPMG. 2017. *A blueprint for success in healthcare data and analytics (D&A)*. United Kingdom: KPMG. <https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/10/blueprint-for-success-in-healthcare-data-and-analytics.pdf>.
- KPMG. 2018. *Data governance: Driving value in healthcare*. United Kingdom: KPMG. <https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/06/data-governance-driving-value-in-health.pdf>.
- Lepenioti, Katerina, Alexandros Bousdekis, Dimitris Apostolou, and Gregoris Mentzas. 2020. "Prescriptive analytics: Literature review and research challenges." *International Journal of Information Management* 50 (February): 57-70. <https://doi.org/10.1016/j.ijinfomgt.2019.04.003>.
- Lis, Dominik, and Boris Otto. 2021. "Towards a Taxonomy of ecosystem Data Governance." *Hawaii International Conference on System Sciences 2021* (HISCC-54) (January). https://aisel.aisnet.org/hicss-54/os/it_governance/10.
- Mackenzie DataStream. 2020. "FAIR and CARE Data Principles." Accessed February 22, 2024. <https://mackenzie-datastream.ca/fr/article/fair-and-care-data-principles>.
- McCaig, Mélanie, and Davar Rezanian. 2021. "A Scoping Review on Data Governance." *Proceedings of the International Conference on IoT Based Control Networks & Intelligent Systems 2* (July). <https://dx.doi.org/10.2139/ssrn.3882450>.

- Meehan, Ann. 2016. "The Information Governance Roadmap: Mile Marker 1--Engaging IG Leadership and Celebrating Quick Wins." *Journal of AHIMA* 87, no. 5, 38-41. PMID: 27244946.
- Mikalef, Patrick, Maria Boura, Gero Lezakos, and John Krogstie. 2020. "The role of information governance in big data analytics driven innovation." *Information & Management* 57, no. 7 (November). <https://doi.org/10.1016/j.im.2020.103361>.
- Murray-Rust, Peter. 2008. "Open Data in Science." *Nature Precedings* (January). <https://doi.org/10.1038/npre.2008.1526.1>.
- Oachs, Pamela, and Amy Watters. 2020. *Health Information Management: Concepts, Principles, and Practice*, 6th ed. Chicago: AHIMA Press. EPUB. <https://my.ahima.org/store/#/productdetail/50320f8b-434e-ee11-be6e-6045bd095340>.
- Oracle. 2011. *Enterprise Information Management: Best Practices in Data Governance*. Redwood Shores: Oracle. <https://www.oracle.com/assets/oea-best-practices-data-gov-1357848.pdf>.
- Sibenco Legal & Advisory. 2023. "Information & Data Governance: Maximising data value, minimising risks and business costs." Accessed February 22, 2024. <https://www.sibenco.com/services/information-governance/>.
- Smallwood, Robert F. 2019. *Information Governance: Concepts, Strategies and Best Practices*. New York: John Wiley & Sons.
- Spiekermann, Markus. 2019. "Data Marketplaces: Trends and Monetisation of Data Goods." *Intereconomics* 54, no. 4 (October): 208-216. <https://doi.org/10.1007/s10272-019-0826-z>.
- Tallon, Paul P., Ronald V. Ramirez, and James E. Short. 2013. "The Information Artifact in IT Governance: Toward a Theory of Information Governance." *Journal of Management Information Systems* 30, no. 3 (December): 141-178. <https://doi.org/10.2753/MIS0742-1222300306>.
- Taylor, John, and Tahu Kukutai, eds. 2016. *Indigenous Data Sovereignty: Toward an Agenda* 38 (November). Canberra: ANU Press. <http://doi.org/10.22459/CAEPR38.11.2016>.
- Thunder, Jimmy, and Mark Intertas. 2020. *Indigenizing the Co-operative Model*. Manitoba: Canadian Centre for Policy Alternatives. <https://policyalternatives.ca/publications/reports/indigenizing-co-operative-model>.
- Trevethan, Shelley. 2019. Strengthening the Availability of First Nations Data. Ottawa: QMR Consulting. https://www.afn.ca/wp-content/uploads/2019/05/NCR-11176060-v1-STRENGTHENING_THE_AVAILABILITY_OF_FIRST_NATIONS_DATA-MAR_25_2019-FINAL_E.pdf
- UK Data Service. 2023. "What is the Five Safes framework?" Accessed February 22, 2024. <https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/>.
- Wiener, Martin, Carol Saunders, and Marco Marabelli. 2020. "Big-data business models: A critical literature review and multiperspective research framework." *Journal of Information Technology* 35, no. 1 (March): 66-91. <https://doi.org/10.1177/0268396219896811>.
- Wixom, Barbara H., and Jeanne W. Ross. 2017. "How to Monetize Your Data." *MITSloan Management Review* 58, no. 3 (January). <https://doi.org/10.7551/mitpress/11633.003.0009>.
- Yang, Tung-Mou, and Terrence A. Maxwell. 2011. "Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors." *Government Information Quarterly* 28, no. 2 (April): 164-175. <https://doi.org/10.1016/j.giq.2010.06.008>.

