



Technology and Territory

Data Sovereignty & Governance Review

Where your community's data lives, who controls it, and how to take it back

Prepared for: [Client organization] · Prepared by: Onake Systems Inc.

Representative excerpts from a full engagement report.

Inside this sample

- Data inventory and residency
- Access and control
- Agreements and exposure
- OCAP®-aligned governance framework
- Prioritized roadmap

SECTION 1

How to read this report

This review establishes where your organization's data actually lives, who can reach it, and what it would take to bring it under your own governance. It is written to be used: the data inventory becomes the working record your team maintains, and the findings support the agreements you negotiate with funders, cloud providers and vendors from a position of control.

The review is grounded in the First Nations principles of Ownership, Control, Access and Possession (OCAP®). The question throughout is not only where data sits technically, but who holds authority over it, and whether that authority rests with the community or has quietly passed to a vendor or a funding body.

- Findings are stated against evidence, not impression.
- Every holding is traced to where it physically resides and who controls access.
- Where information was unavailable, the report says so rather than estimating.

Scope of this sample

This document contains representative excerpts. A full engagement report runs approximately 40 to 60 pages, depending on the number of systems and agreements reviewed.

SECTION 2

Data inventory and residency

Every significant holding of community and member data, what it contains, where it physically resides, and who controls access. Most organizations have never mapped this, and the exercise routinely finds member data held in systems and jurisdictions no one chose deliberately.

Data holding	Contains	Resides	Controlled by
Membership system	Member records	Cloud (US)	Vendor
Health records	Clinical data	Provincial system	Health authority
Land / GIS	Territory data	On-site + cloud	Shared
Financial	Accounts, payroll	Cloud (CA)	Vendor
Research data	Survey results	University server	Researcher
Email / files	Correspondence	Cloud (US)	Vendor

In the example above, two findings come from the inventory alone: member records sit on US-based infrastructure under a vendor's control, and research data about the community resides on a university server held by an external researcher. Neither arrangement was a deliberate community decision; both accumulated by default.

SECTION 3

Access and control

Residency is where data sits. Control is who can decide what happens to it. This section separates the two, because data can rest on community premises and still be controlled by an outside party through an agreement, or sit offshore and still be under genuine community authority if the agreement is written correctly.

Holding	Community can access	Community can delete	Third-party access	Control
Membership	Yes	No	Vendor	Weak
Health records	Limited	No	Province	External
Land / GIS	Yes	Yes	None	Strong
Financial	Yes	No	Vendor	Partial
Research	No	No	Researcher	None

The pattern that matters: the community can see much of its data but cannot delete or move most of it, and in the case of research data cannot even access it. Under OCAP®, possession without control is the gap this review is built to close.

Agreements and exposure

Data control is set less by technology than by the agreements signed around it. This section reviews the funding, cloud, research and vendor agreements that touch community data, and flags the clauses that quietly hand away authority.

- A funding agreement that grants the funder a perpetual license to data collected under it.
- A cloud contract with no clause requiring return and deletion of data when the contract ends.
- A research agreement with no community ownership of results, and no obligation to share them back.
- A vendor agreement silent on where data may be stored, allowing it to move offshore without notice.

How to use this section

Each flagged clause is matched to a plain-language replacement in the full toolkit, so the next agreement can be negotiated from language the community controls.

SECTION 5

Governance framework

This section sets out, in plain language, how the community can hold authority over its data going forward. It is the OCAP®-aligned framework the toolkit provides for your team to adopt and run.

- Name who holds decision authority over each category of community data.
- Require that every new agreement touching member data pass a data-governance review before signing.
- Set a residency standard: where community data may and may not be stored, and under what conditions.
- Keep a living inventory, so control is monitored continuously rather than rediscovered in a crisis.

Grounding

This framework implements OCAP® (Ownership, Control, Access and Possession) as maintained by the First Nations Information Governance Centre, adapted to your community's own protocols.

SECTION 6

Roadmap

Findings are ordered by exposure. Holdings where the community has the least control over the most sensitive data are addressed first, and the agreements coming up for renewal are flagged so the window to renegotiate is not missed.

Priority	Action	Horizon	Indicative cost
1	Renegotiate membership data residency and deletion	0-3 months	\$4k-10k
2	Data-governance clause for all new agreements	0-2 months	\$3k-7k
3	Recover control of community research data	3-9 months	varies
4	Adopt OCAP®-aligned governance framework	3-6 months	\$8k-18k
5	Community data residency standard	6-12 months	\$6k-15k

- Costs are indicative ranges for planning only and are not quotations.
- Items 1 and 2 address active exposure and should proceed regardless of funding outcomes.
- Items 4 and 5 are the governance foundation a larger engagement or funding application would build on.