Understanding the Basics of OCAP®[1]

Description:

This tool provides an overview of OCAP® and offers some suggestions on how this can be integrated into data collection and research. *(This tool is respectfully adapted from information on the First Nations Information Governance Centre website*.)

How it can be used:

OCAP® is the recognized standard for data collection and conducting research on First Nations and has grown to include the governance of all First Nations' information. Review the definitions and examples to help guide any data collection or research initiatives in your community.

OCAP stands for **Ownership, Control, Access, and Possession.**

The interpretation of OCAP® is unique to each First Nation community or region. OCAP® is not a doctrine or a prescription but is a set of principles that reflect First Nation commitments to use and share information in a way that brings benefit to the community while minimizing harm.

Ownership:

The notion of ownership refers to the relationship of a First Nations community to its cultural knowledge/data/information. The principle states that a community or group owns information collectively in the same way that an individual owns their personal information. Ownership is distinct from stewardship. The stewardship or custodianship of data or information by an institution that is accountable to the group is a mechanism through which ownership may be maintained.

Some questions to consider[2]:

- How are First Nations identified in data?
- Who owns the data? Is there any licensing of data?
- How is ownership established?
- How is consent managed?
- Are First Nation(s) attributed as author/contributor?

---

[1] OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC) (www.FNIGC.ca/OCAP*)*

[2]The questions and considerations were presented at the FNIGC National Workshop in March 2013 and are a starting point for more extensive considerations and questions. They present a starting point and are not intended to be complete considerations for OCAP® compliance.

Control:

The aspirations and inherent rights of First Nations to maintain and regain control of all aspects of their lives and institutions extend to information and data. The principle of "control" asserts that First Nations people, their communities and representative bodies must control how information about them is collected, used and disclosed. The element of control extends to all aspects of information management, from collection of data to the use, disclosure, and ultimate destruction of data.

Some questions to consider:

- How will First Nations exercise control over data?
- Are any agreements proposed or in place?
- What is the decision-making process for use of data?
- What is the data flow?
- What happens to data and results upon completion?

Access:

First Nations must have access to information and data about themselves and their communities, regardless of where it is held. The principle also refers to the right of First Nations communities and organizations to manage and make decisions regarding who can access their collective information.

Some questions to consider:

- How can First Nations access their data?
- If personal information is being collected/held, how can First Nation individuals access their data?
- Who will be accessing data?
- Will everyone that has access to data receive training/education?
- What security/privacy policies and procedures are in place?

Possession:

While "ownership" identifies the relationship between a people and their data, possession reflects the state of stewardship of data. First Nation possession puts data within First Nation jurisdiction and therefore, within First Nation control. Possession is the mechanism to assert and protect ownership and control.

Some questions to consider:

- Will data be held by a First Nation or a First Nation-controlled entity? If not, why not?

General questions:

- How does the project benefit First Nations?
- Is there any potential harm to First Nations or First Nations people? If so, how will that be mitigated?
- Is there a communication strategy for ongoing communication?
- Does the project include any opportunities for First Nation capacity building?
- If the project includes the collection of personal information, has a Privacy Impact Assessment been conducted?
- Will the data and/or results of research be returned to the community?
- Has the project been reviewed by an Ethics Review Board?

Tools to help implement OCAP® principles

Education:

First Nations and First Nation organizations must reach out to their own communities, to government partners, to universities, and to anyone else that may wish to collaborate with First Nations in research or to assist with information governance. Information should be made available on-line and through other media. One component could be The First Nations Information Governance Centre's OCAP® certification process. Some specific activities could include:

- Share knowledge about OCAP® with academics and government;
- Educate government and university legal/contract staff regarding OCAP® requirements and how contracts may be changed (proactively) to meet the needs and values of First Nations;
- Create partnerships with universities;
- Make OCAP® -ready tools available for use by communities:
    - OCAP® "standards" (e.g., how to preserve intellectual property rights, etc.);
    - Data sharing agreements templates;
    - First Nation privacy laws;
    - Privacy and security policies and procedures for First Nations.
- Share OCAP® knowledge with communities and leadership;
- Promote the development of First Nation entities as First Nations data stewards.

Legislation:

First Nation laws are a tool that can help address some of the barriers associated with jurisdiction and capacity. A privacy law, with accompanying policies and procedures, would support a First Nation in holding its own data. A First Nation's exercise of jurisdiction in the area of privacy protection also builds capacity within a community for privacy protection. Such a law can deal with both personal privacy and community privacy, incorporating universal standards of personal privacy together with OCAP® principles.

Change the Data Steward:

The best and only reliable method of preventing application of the federal *Access to Information Act* or other similar provincial/territorial law that does not recognize all First Nations as government, or that fails to protect First Nation collective information, is to prevent First Nations data from being within the control of a federal institution. This can be done through:

- Transferring data to the stewardship of a First Nations or First Nation controlled organization;
- Retaining a third-party data steward that is not subject to access to information/freedom of information legislation. The third party could be a university, or a private entity, and in some cases provincial partners may be appropriate. A legislative review would have to be conducted to ensure that there are no other barriers in relation to the alternative data steward.

Data Sharing Agreements:

Agreements are a very important part of OCAP®. Because OCAP® principles, particularly First Nation values of collective privacy, are not recognized in Canadian law, the only way that First Nations can regulate the use of their information is through agreement. In all cases where First Nations information is being held by an entity other than the First Nation, there should be a legally binding agreement that governs the collection, use and disclosure of the data. First Nations can exert effective governance over their information through appropriately-drafted agreements.

Some important questions to ask or elements that should be considered in every agreement:

- Are the proper parties represented in the agreements? For example, the agreement should be between the First Nation itself, acting through Chief and Council.
- Is First Nation ownership of data acknowledged?
- How are intellectual property rights in research results addressed?
- How can First Nations access their own data?
- Controlling all possible use, access, and disclosure – listing uses that are acceptable to First Nation and requiring First Nation consent prior to any use not listed. No secondary use without consent.
- How will decisions be made about the use of First Nations' data for data linkages?
- Regular reporting requirements by the data steward regarding all access
- Personal privacy protection and community privacy.
- Legislative review to determine vulnerability under access laws, and to determine applicable privacy legislation.
- Can the First Nation terminate the agreement for any reason?
- What happens to the data upon termination or expiry of the agreement?
- Is there a breach protocol that requires First Nation notification?

- Are there specifications for publishing to ensure that First Nations are properly attributed for their contributions, given an opportunity to comment upon works prior to publishing?
- Are there requirements to present research results to the community before publication?
- Can the partnership/project be used to build First Nation capacity in the area of information management, analysis, etc.?
- Are there requirements for continued consultation and communication between the data steward and the First Nation?
- Does the agreement contemplate or accommodate the future transfer of data to a First Nation data steward?