CIO STRATEGY COUNCIL

National Standard of Canada
Standards Proposal

Proposed Standard Title:

Data governance for the delivery of community and social services

Plain Language Summary of Standards Proposal (200 words max):

A data governance framework for organizations that provide community and social services to safeguard the privacy of their client and donor data.

Proposed Scope:

This proposed standard aims to specify minimum requirements for the responsible and privacy-preserving collection, storage, use, and sharing of personal information by organizations delivering community and social services.

Considerations are given to:

- client/beneficiary and donor data;
- data governance and management practices;
- privacy regulations and other applicable legislation;
- relevant ethical guidelines and practices;
- requirements for service providers, funders, and technology vendors.

Strategic Need:

Identify the strategic need of key stakeholders and confirmation expressing the need.

This includes consideration for:

a. The strategic need of key stakeholder (e.g. legislator, industry, government, consumers);
b. The type of standard (international, regional, domestic standards and harmonization need);
c. Addressing up-to-date vs outdated standard to ensure latest innovative/technology/safety features available for businesses;
d. If the standard is intended to support national/regional/international certification programs;
e. If there is stakeholder intention to transition to different standard;
f. The type of maintenance (periodic, continuous, stabilized, best before date); and
g. The use of "CAN" descriptor.

Data Collection by Community and Social Service Providers

Canada's community and social service providers deliver services and support to vulnerable and at-risk individuals. The vast majority of these organizations collect and use some amount of client data. Some of this data is sensitive – such as participation in addiction treatment, a health diagnosis, or experience of violence.

Beyond client information, many also collect financial donations by individuals. This financial support can be critical to their success.

Risks Faced by Community and Social Service Providers

As community and social service providers adopt new technologies for client and donor management, this can multiply the amount of data under control of organizations and their vendors. This can pose serious new risks to privacy and security which may not be well understood:

1. Unauthorized use of client data can cause irreparable harm to clients, including reputational damage, trauma, exposure to identity theft and fraud.
2. If donor data is compromised, it can also result in a loss of donor confidence.
3. The reputation of the organization and the community and social service sector as a whole can be undermined as data breaches and other harms accumulate.

Vulnerability to Risks

Community and social service providers are uniquely vulnerable to these risks materializing.

First, the **multitude of privacy and regulatory requirements imposed on the social secto**r can cause uncertainty about what is required for compliance. Community and social service providers sit at the intersection of multiple privacy regulations and are not subject to a single regulatory regime as other industries are (e.g. financial services). The applicability of a specific regulatory regime largely depends on who is working with a client or their information (e.g. whether the work involves certain roles regulated under provincial health information acts) and who is funding the work. At different points in their interactions, the same entity might be subject to provincial or federal legislation, legislation dealing with personal information generally or health information specifically, and legislation that applies specifically to the nonprofit sector, to the private sector, or to the public sector. Funding requirements of various grant-making entities, including government, can bring certain legislation into play, but this does not evenly apply to all clients or all programs, resulting in uneven privacy management within the same organization.

Second, the **lack of consensus on tools and processes for managing client data** compounds the vulnerability. In Canada, billions of dollars were spent on digitization in the health sector, with a few central proven systems for data management. By contrast, many community and social service providers rely on paper, spreadsheets, and/or a subset of solutions that do not provide uniformity in privacy protection. Many rely on password protected Excel files (with shared passwords) or unlocked storage cabinets for data storage. Even if privacy regulations were clear, the service providers may not have the tools required to protect client information.

Third, **scarce core operating funding can result in insufficient internal capacity**. For example, many community and social service providers lack the internal capacity to:

1. fully understand and meet legal and regulatory requirements for data management and governance;
2. appropriately vet technology vendors (e.g. CRM/DMS software);
3. build and maintain IT infrastructure or processes, including cybersecurity systems to manage the cyber threats common in the digital age; or
4. train and retain staff who can provide consistent oversight.

Finally, community and social service providers may be vulnerable to ransomware attacks because the lumpiness of grant funding means they often hold significant sums in bank accounts.

Benefits of Strong Data Governance

The importance of the responsible collection, storage, use, and sharing of client, donor and donation data is therefore increasing to manage the risks and vulnerabilities.

Strong data governance practices can also improve the client experience, which is important from a trauma-informed perspective. This contrasts with a runaround of endless referrals, forms and consent processes. It can also contribute to staff retention and engagement.

In addition, with the appropriate guardrails in place, community and social service providers can better use the data available to them to serve their mission. Vendors do not provide uniform access to data, for example, and organizations would benefit from guidance on vendor management. Some early adopters are exploring AI solutions to enhance their operations. AI is not well-understood sector-wide and introduces additional risks of bias, lack of transparency, and lack of accountability. To unlock the efficiencies offered by AI, community and social service providers must first have strong data governance practices in place.

Insufficiency of Existing Standards

There are currently no recognized standards (e.g. ISO, CEN, BSI, SA) specifically focused on social sector data. More general data governance standards are not fit for purpose because:

1. Non-profit community and social service providers operate in a unique regulatory environment, and registered charities are managing tax-receipted donations, which implicates the public interest;
2. Community and social service providers are distinct from public entities and are not bound by laws regulating government use of data. At the same time, their stakeholders and beneficiaries hold them to higher ethical standards than other organizations. To maintain stakeholders’ trust, they require a specific standard that may surpass minimum legal requirements; and

3. This sector tends to use a common suite of software applications that are unique and not used in other industries.
4. Components within case management accreditation standards (CARF, CARAF, CAC) that address some aspects of privacy are often minor components of client service, not comprehensive standalone pieces that can be updated quickly to meet evolving challenges.
5. With respect to donor data, there are strong ethical guidelines for professional fundraisers, such as the Donor Bill of Rights, created by the Association of Fundraising Professionals (AFP), the Association for Healthcare Philanthropy (AHP), the Council for Advancement and Support of Education (CASE), and the Giving Institute: Leading Consultants to Non-profits. These guidelines set out high-level principles, such as the right "[t]o be assured that information about their donation is handled with respect and with confidentiality to the extent provided by law." These guidelines can be built on by (1) focusing more specifically on the technology and data risks and enablers and (2) providing more detailed technical guidance on how to meet the requirements of these ethical frameworks.

As a result, there is a need for a standard setting out the minimum requirements for the governance of data.

Key Stakeholders

Key stakeholders include:

- Non-profits and their associations and federations (e.g. CanadaHelps, Imagine Canada, United Way Centreaide Canada, Volunteer Canada, Ontario Non-profit Network, 211)
- For-profit social service delivery agencies
- Fundraisers and their associations (e.g. Association of Fundraising Professionals (AFP), CFREs, Council for Advancement and Support of Education (CASE))
- Foundations/philanthropists and their associations (e.g. Community Foundations of Canada, Philanthropic Foundations of Canada)
- Technology vendors for charities/foundations (e.g. FundMetric, FundraiseUp, Blackbaud, HelpSeeker, Salesforce, Benevity)
- Technology consultants for charities (e.g. Technology Helps, Ajah)
- Charity lawyers (e.g. Miller Thomson, Carters)
- Canada Revenue Agency
- CPA Canada

This proposed National Standard of Canada will:

- Support future certification programs developed at national, regional and international levels to support charitable/fundraising sectors;
- Be maintained on a periodic basis as determined by the technical committee responsible for developing the standard; and
- Use the CAN descriptor.

Need for Availability in Both of Canada’s Official Languages: *Do stakeholders need the standard published in both official languages?* *Do users of the standard need the standard published in both official languages?* *Do authorities having jurisdiction need the standard published in both official languages?* *Are there health and safety related needs for the standard to be published in both official languages?* *For adoptions, is there availability of the regional/international standard or other deliverable from the source?* *For adoptions, is there an agreement with the source committee to facilitate official translation?*	Yes

Geographical Representation Considerations:

Identify the Canadian geographical representation appropriate to the subject area covered by the standard.

Geographic representation may consider factors such as:

a. *Industry (e.g. petroleum in petroleum producing provinces);*
b. *Reference in regulation (if a regulation exists in a province); or*
c. *Commodity characteristics and social impact (e.g. heating oil for northern climates).*

All sectors of the economy.

Trade:

Identify how the standard meets the needs of the marketplace and contributes to advancing trade in the broadest possible geographical and economic contexts.

For example:

a. *Facilitate Canadian innovation to lead internationally;*
b. *Support the objectives of “One standard, one test, accepted everywhere”;*
c. *Support the objectives of “First to Market”; or*
d. *Foster international/ regional/ national alignment of requirements.*

A made-in-Canada standard will facilitate Canadian innovation to lead internationally, especially for Canadian vendors focused on data management and AI tools for social sector operations. The standard would enable confidence in Canadian technologies, resulting in advancing trade prospects of the technologies. The standard will take into consideration and align with any global standards, such as the global Association of Professional Fundraisers’ Code of Ethical Standards.

Relevant existing documents at the international, regional and national level:

ISO/IEC 38500, Information technology -- Governance of IT for the organization

ISO/IEC 38505-1, Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data

ISO/IEC TR 38505-2, Information technology -- Governance of IT -- Governance of data -- Part 2: Implications of ISO/IEC 38505-1 for data management

ISO 8000 series, Data quality

ISO 27001, Information Security

Association of Fundraising Professionals Code of Ethical Standards

CASE Global Reporting Standards

Donor Bill of Rights

Imagine Canada Standards Program