Data Standards for the Identification and Monitoring of Systemic Racism

Government of Ontario

Ontario

INTRODUCTION

The *Data Standards for the Identification and Monitoring of Systemic Racism*, also known as Ontario's *Anti-Racism Data Standards* (Standards) were established to help identify and monitor systemic racism and racial disparities within the public sector.

The Standards establish consistent, effective practices for producing reliable information to support evidence-based decision-making and public accountability to help eliminate systemic racism and promote racial equity.

The Government of Ontario is committed to helping to create an inclusive and equitable society for all Ontarians. By identifying and monitoring systemic racial disparities, public sector organizations will be better able to close gaps, eliminate barriers, and advance the fair treatment of everyone.

Purpose

The purpose of the Standards is to set out requirements for the collection, use, disclosure, de-identification, management, publication and reporting of information, including personal information. They help enable public sector organizations (PSOs) to fulfil their obligations under the *Anti-Racism Act, 2017* (ARA) to identify and monitor racial disparities in order to eliminate systemic racism and advance racial equity.

Legal Authority

The Standards have been made by the Minister Responsible for Anti-Racism under the authority of s. 6(1) of the ARA and have been established by approval of the Lieutenant Governor in Council. The Information and Privacy Commissioner (IPC) and the Ontario Human Rights Commission (OHRC) were consulted in developing them.

The Standards should be read alongside the ARA and its associated regulations.

Application

The Standards apply to PSOs, as defined in the ARA, that are required or authorized by the regulations to collect personal information related to specific programs, services, and functions. This includes personal information related to Indigenous identity, race, religion, ethnic origin, and other personal information listed in the regulations.

PSOs listed in regulations must comply with the ARA, and all or part of the Standards. The particular standards each organization must follow are specified within the ARA itself, and in the regulations.

The Standards do not replace, limit or diminish any responsibilities or obligations owed to persons under the *Ontario Human Rights Code*, 1990 (the Code).

Organizations that are not authorized or required to collect personal information in regulations made under the ARA may also be authorized to collect, use and disclose personal information for the purpose of identifying and monitoring systemic racism and racial disparities under other Acts, including the Code.

In such cases, organizations must follow the requirements of relevant legislation, such as the *Freedom of Information and Protection of Privacy Act* (FIPPA) or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). Organizations may consider the Standards and the related guidance in developing and implementing any program to identify, monitor, and eliminate systemic racism and advance racial equity.

Scope

The Standards govern how organizations manage information, including personal information that is collected under the authority of the ARA. The purpose of collecting this information is to understand how systemic racism impacts Indigenous, Black, and racialized groups, and to identify potential racial inequalities.

The Standards set out requirements, rationale, and guidance at every stage from planning and preparation to analysis and reporting. This includes, collecting, using, disclosing, de-identifying, and managing information, including personal information.

The Standards do not provide guidance on how to mitigate, eliminate, or prevent adverse racial impacts and inequitable outcomes of policies and programs.

The IPC may review the information handling practices of any organization subject to the ARA to determine if the requirements under the ARA, the regulations and the Standards have been met. If the Commissioner determines that a practice contravenes the ARA or regulations, the Commissioner may order a PSO to stop the practice, destroy personal information collected or retained under the practice, change the practice, or implement a new practice.

How to Use This Document

In addition to specific Standards, this document offers rationales and guidance:

- **Standards** are requirements that apply to PSOs regulated under the ARA.
- **Rationales** provide reasons behind the Standards.
- **Guidance** describes exemplary practices and important considerations to take into account in complying with the Standards.

The Standards reflect consideration of the diverse functions, needs and operational realities of PSOs in Ontario.

Principles

These principles should be followed by organizations in interpreting and applying the Standards:

Principle 1: Privacy, Confidentiality, and Dignity

Protect the confidentiality of personal information, and respect the privacy and dignity of individuals, groups, and communities.

Principle 2: Commitment and Accountability

Be accountable for using the Standards to help eliminate systemic racism and advance racial equity.

Principle 3: Impartiality and Integrity

Apply the Standards impartially and promote public confidence in efforts to eliminate systemic racism and advance racial equity.

Principle 4: Quality Assurance

Make continuous efforts to ensure the quality of the personal information collected, to conduct analysis in a careful and thorough manner, and to verify the accuracy of reported findings.

Principle 5: Organizational Resources

Use resources in ways that fulfill the requirements of the Standards.

Principle 6: Transparency, Timeliness and Accessibility

Collect and report on information in a timely manner, making the information available to the public in a way that is clear, transparent, and accessible.

Overview of the Standards

1. **Assess, Plan and Prepare**

- Identify need and establish specific organizational objectives for personal information collection based on stakeholder and community input.
- Determine organizational priorities and resources and conduct a privacy impact assessment.
- Identify meaningful policy, program, or service delivery outcomes, and establish an analysis plan.
- Establish data governance processes and develop and plan collection policies and procedures, including measures related to quality assurance and security of personal information.
- Identify training needs and develop and deliver appropriate training and other resources to support compliance with the ARA, the regulations and the Standards, and relevant privacy legislation.

2. **Collect Personal Information**
- Communicate the purpose and manner of personal information collection to clients and communities.
- Implement the collection of personal information based on voluntary express consent.

3. **Manage and Protect Personal Information**
- Implement processes for quality assurance and the security of personal information.
- Maintain and promote secure systems and processes for retaining, storing, and disposing of personal information.
- Limit access to and use of personal information

4. **Analyse the Information Collected**
- Calculate and interpret racial disproportionality or disparity statistics.
- Apply thresholds and interpret whether notable differences exist that require further analysis and/or remedial action.

5. **Release of Data and Results of Analysis to the Public**
- De-identify data sets and results of analyses before making information public, consistent with Open Government principles.
- Include results of racial disproportionalities or disparities in the reports to the public, along with thresholds used.

6. **Support and Promote Anti-Racism Organizational Change**
- Use information to better understand racial inequities, and to inform evidence-based decisions to remove systemic barriers and advance racial equity.
- Continue to monitor and evaluate progress and outcomes.
- Promote public education and engagement about anti-racism.

7. **Participant Observer Information (POI)**
- Plan to collect, manage and use POI with input from affected communities and stakeholders.
- Implement the collection of POI according to requirements for indirect collection.
- Have measures in place to ensure the accuracy of POI before use.

Periodic Review

With involvement of affected communities, the Government of Ontario will review the Standards periodically to ensure that they continue to fulfill the purpose set out under s. 6(1) of the ARA.

The Minister Responsible for Anti-Racism will oversee the periodic review. The OHRC and IPC will be consulted before any amendments are made to the Standards.

Context

Understanding Racism

These Standards are designed to address racism at a systemic level, through the collection and analysis of personal information in connection with specific functions, programs and services of PSOs to identify and monitor potential racial inequities.

Racism consists of ideas, beliefs or practices that establish, maintain or perpetuate the superiority or dominance of one racial group over another. The OHRC notes that racism differs from prejudice in that it is tied to the social, political, economic, and institutional power that is held by the dominant group in society (OHRC, *Policy and guidelines of racism and racial discrimination*).

Systemic racism occurs when institutions or systems create or maintain racial inequity often as a result of hidden institutional biases in policies, practices, and procedures that privilege some groups and disadvantage others. In Ontario, systemic racism can take many forms, such as:

- Officials who single out members of Indigenous, Black, and racialized groups for greater scrutiny or different treatment;
- Opportunities shared through informal networks that exclude Indigenous, Black, and racialized individuals; and
- Lack of public attention and policy concern regarding social, health and economic problems that disproportionately affect Indigenous, Black, and racialized communities.

Throughout Canada's history including prior to Confederation, colonial practices, including the oppression of Indigenous peoples and the enslavement of people of African descent, have entrenched public attitudes, beliefs, and practices that continue to negatively impact Indigenous, Black, and racialized individuals and communities in social, economic, and political life. The exclusion and devaluing of different groups is also evident in Canada's history of discriminatory immigration and citizenship policies, including restricted admission for Jewish people at the height of the Holocaust; the Head Tax on Chinese immigrants; and the internment of Japanese Canadians during World War II, among many other examples.

The legacy of this history impacts Indigenous, Black, and racialized groups by perpetuating the advantages and institutional power of the historically dominant group (White individuals with higher socio-economic status). The negative consequences of this legacy are compounded over time and transmitted intergenerationally. Systemic racism continues to result in racially inequitable outcomes across public sectors such as education, child welfare and justice. Racist ideas and practices persist in a variety of forms, including anti-Black racism, anti-Indigenous racism, Islamophobia and antisemitism (see glossary for definitions of these terms).

Understanding Anti-Racism

Anti-racism is a proactive course of action to identify, remove, prevent, and mitigate the racially inequitable outcomes and power imbalances between dominant and disadvantaged groups and the structures that sustain these inequities. It recognizes the historic nature and cultural contexts of racism, and focuses critically on systemic racism.

Anti-racism aims to ensure the absence of unfair treatment, which includes exclusionary or discriminatory practices. The Standards set out requirements to collect, analyze and report information to help assess whether there is fair treatment and equitable access to public services and programs, such as:

- policing services;
- bail processes;
- high quality education and healthcare; and
- supports and services for the well-being of children and families.

Anti-racism for Indigenous peoples is distinct from anti-colonialism

Anti-racism for Indigenous people must be understood in light of the ongoing impact of assimilative policies and laws on Indigenous people, and the prevalence of anti-Indigenous racism in Ontario. However, it is important to recognize that anti-racism is a distinct component of the larger struggle of anti-colonialism for Indigenous peoples. One reason that anti-racism does not fully capture the experiences of many Indigenous communities is that it tells only one part of the story.

The other part of the story is based on the fact that Indigenous peoples were here long before the coming of Europeans. This reality grounds their claims for self-determination and for recognition of Indigenous sovereignty, laws, and governance structures. Indigenous peoples have a unique legal status recognized constitutionally.

Anti-colonialism, therefore, is broader than anti-racism because it includes recognition of Indigenous peoples' inherent rights and sovereignty, constitutionally protected Aboriginal and Treaty rights, and right to self-determination in accordance with the *United Nations Declaration on the Rights of Indigenous Peoples*.

Understanding Canada's colonial history and its ongoing impacts

Throughout Canada's history, successive governments have implemented laws and policies aimed at devaluing and destroying Indigenous identities and cultures within Canada. The federal Indian Act and the Indian Residential Schools[1] are just two examples. The result of this history of colonization and policies is that in many Indigenous communities within Canada, people experience extreme poverty, housing shortages, lack of access to clean drinking water, health issues, lower life expectancies, lower levels of

[1] For a detailed history of the Indian Residential Schools Legacy in Canada, see online: Truth and Reconciliation Commission of Canada <www.trc.ca>.

educational attainment, limited employment opportunities, racism, violence, over policing, under-policing, and over-victimization.

Without an understanding of the historical context and current realities facing Indigenous communities, there is a danger that these socioeconomic indicators could be misunderstood as a reflection of Indigenous peoples' own choices rather than as a direct consequence of assimilative policies and laws aimed at cultural genocide.

This means that in some cases there are different considerations that must be taken into account when decisions are being made about an Indigenous person's liberty (i.e. consideration of the Gladue principles*).*

The impact of research and data collection on Indigenous communities

Within this colonial history, Indigenous communities have had an extremely difficult history associated with research and data collection. Indigenous people have been the subject of non-consensual medical and social experiments without regard for their human rights. In addition, the government of Canada assigned names and identification numbers, and collected data to control the movement of Indigenous peoples, limit access to services, and monitor Indigenous populations.

Many Indigenous people and communities are understandably suspicious of government data-collection efforts. There may be an unwillingness to disclose Indigenous identity, especially in cases where particular groups of government or law enforcement workers have had a significant role in enforcing assimilation and other punitive laws and policies.

Care must be taken to ensure that Indigenous-related information is collected according to appropriate policies and protocols, and that the information is managed and used in ways that benefit Indigenous communities. Anyone responsible for collecting information must also be trained to understand the causes of the deep mistrust that Indigenous people and communities have of government systems, personnel, and information collection efforts.

Respecting Indigenous identity and self-identification

Customarily, Indigenous communities across what is currently known as Canada may not self-identify as belonging to one pan-Indigenous group. Instead, Indigenous identity may be tied to an individual's clan, community, nationhood, or language family.

This is an important consideration when collecting information about Indigenous identity. The Standards contain a specific question and allow for flexibility in the way Indigenous people choose to self-identify. This question is distinct from the question about race, which is designed to collect information about how Indigenous people may be racialized by society.

Applying research and data collection as anti-racism tools

For centuries, government-led data collection, analysis and measurement processes in Canada has been centred in Eurocentric perspectives. Properly applied, the Standards provide a way to use data for anti-racism purposes, grounded in an understanding of the historical context and the current realities facing Indigenous, Black, and racialized communities. Public accountability and community involvement are core aspects of the Standards and will help to ensure that the information gathered serves the racial equity intentions of the ARA.

Standards and Guidance

1. Assess, Plan and Prepare

Reasons to Collect Information

PSOs should collect information if there are observed unequal outcomes for Indigenous, Black, and racialized persons, persistent complaints of systemic racial barriers, and/or widespread public perception of systemic racial barriers or bias within the organization.

Guidance in the *OHRC policy and guidelines on racism and racial discrimination* states that “data collection and analysis should be undertaken where an organization or institution has or ought to have reason to believe that discrimination, systemic barriers or the perpetuation of historical disadvantage may potentially exist.”

Assess and Plan

Standard 1. Assess and Plan for Compliance with the ARA, the Regulations and the Standards

PSOs must assess their objectives and priorities for the collection and use of personal information for the purpose of conducting analyses to identify and monitor systemic racism and racial disparities.

PSOs must sufficiently plan and prepare for complying with, and implementing the ARA, the regulations and the Standards with input from affected communities, stakeholders, and partners.

Rationale

Planning and preparation is an integral part of understanding the requirements of and ensuring compliance with the ARA, the regulations and the Standards.

Guidance

Assess what personal information is required, for the purpose of the ARA, to identify and monitor racial inequalities in outcomes and help promote racial equity and fair treatment in programs, services, and functions.

Before collecting, using or disclosing any personal information, organizations should consider the following (generally in the order given):

Community input*:* Regularly engage with Indigenous, Black, and racialized communities, stakeholders, clients, and partners to understand their priorities, concerns, needs, and interests in collection, management, use and analysis of information.

Organizational objectives and priorities: Identify clear organizational objectives for the collection and use of personal information under the ARA. In relation to matters required or authorized in the regulations, PSOs should scan the specific policies, practices, services, and/or programs to prioritize how to track and monitor potential systemic racial inequalities. (See OHRC Count me in! Guide).

The race-based personal information will always need to be combined with other information in order to determine the impact of race on outcomes. Organizations should consider the personal information they need to collect, or already lawfully collect for program purposes, that may also be used for the purpose of identifying and monitoring systemic racial inequalities.

Identifying organizational objectives should also include determining which performance measures should be tracked for the purposes of identifying and monitoring systemic racism and racial disparities, and/or measuring progress in advancing racial equity. PSOs should consider monitoring the outcomes of key decisions in a client's interaction with a service or system (see Appendix A for an example).

Privacy Impact Assessment (PIA)*:* Conduct a PIA to identify privacy implications, risks and mitigation strategies. A useful resource is *Planning for Success: Privacy Impact Assessment Guide*, developed by the IPC.

Resources and Training*:* Assess and review organizational resources, capacities, and competencies needed to collect, use, manage, de-identify, analyze, publish, and report information. This includes reviewing existing processes, information technology, and software capabilities, as well as assessing the expertise and skills needed to comply with the Standards. In most cases, training the employees, officers, consultants, and agents of the organization will be necessary to ensure the proper implementation of the Standards (see Standard 4).

Public Communication and Outreach*:* Communicate the organization's information-related objectives and plans to the public, affected communities, and clients. This includes external communications and processes for informing individuals of their privacy rights and the PSO's policies and protocols.

Indigenous Interests in Data Governance

PSOs should consider the interests of Indigenous communities and organizations in exercising authority, control, and shared decision making in the collection, management, use and disclosure of information regarding Indigenous people and communities, consistent with relevant privacy legislation.

Indigenous data governance considerations vary between First Nations, Métis, and Inuit communities and organizations. There are common goals, including emphasis on the importance of engagement, transparency, and Indigenous ownership and control of information (including how it is collected, used, managed, analyzed, interpreted, and reported publicly).

Indigenous data governance principles aim to ensure that information collected from Indigenous communities is used to empower communities with knowledge and tools to work towards positive community outcomes.

Transparency is the focus in relationship building, proactive engagement, and strategic data governance partnerships with the government and/or other broader public service bodies, institutions, and agencies.

Data sharing agreements between PSOs and Indigenous communities and their representatives and partners can be an effective way to respect Indigenous interests in data governance, but such agreements must be undertaken in accordance with the requirements of the ARA and applicable privacy legislation.

Governance and Accountability

Standard 2. Establish Organizational Roles and Responsibilities

PSOs must establish clear accountability mechanisms and rules, with organizational roles and responsibilities, for all aspects of collection, management, use (including analysis), disclosure, and de-identification of personal information, and the public release and reporting of information. There must be at least one manager who is accountable for oversight and ensuring compliance with the ARA, the regulations and the Standards.

Rationale

Clear organizational roles and responsibilities help PSOs comply with the ARA, support transparency, and promote accountability for the proper management of personal information, as well as reporting for the purpose set out in the ARA, the regulations and the Standards.

Guidance

PSOs should work with their records and information management (RIM), privacy, and security professionals to ensure that the collection, use, disclosure, management, security, de-identification, and disposition of records containing personal information is

done in accordance with the Standards, applicable privacy legislation, and the *Archives and Recordkeeping Act,* 2006, if applicable.

PSOs should implement governance and accountability practices such as:

- Appoint a privacy point-person, such as a Privacy Officer or a senior official who has been delegated privacy responsibilities of the "Head" under FIPPA/MFIPPA, to ensure senior management commitment to privacy protection;
- Establish reporting mechanisms for overall compliance activities, as well as for reporting privacy and security breaches;
- Maintain a personal information inventory (know what personal information is held, its sensitivity, where it is held, and why it is collected, used, and disclosed); and
- Implement a privacy management plan to comply with the Standards, including measures for monitoring, assessing and reviewing privacy and security policies, practices, and controls.

Standard 3. Third Party Service Providers Acting on Behalf of PSOs

PSOs are accountable for ARA-related activities undertaken by a third party service provider acting on their behalf. PSOs must ensure that third parties understand and comply with all requirements under the ARA, the regulations and the Standards.

Rationale

When a service or activity is outsourced, a PSO continues to be accountable for complying with the ARA and applicable privacy legislation. Ensuring that third parties understand and abide by all ARA requirements when acting on behalf of a PSO is necessary to protect privacy.

Guidance

Agreements with third parties should require compliance with privacy obligations in the ARA and any other applicable legislation, including the FIPPA and MFIPPA.

The agreements should require that third party service providers be familiar with the requirements of the ARA and the Standards, applicable privacy legislation, and other legislative obligations relating to collecting, using, disclosing, de-identifying, managing, disposing, and reporting information, as well as the PSO's protocols for privacy breaches and management response to security incidents.

When contracting third party service providers that will have access to personal information or will be involved in collection, use (including analysis), and disclosure, consult with legal, procurement, records and information management, and privacy professionals to:

- Assess the privacy and security risks and the sensitivity of the information involved;
- Develop an information protection plan to ensure protection of access and privacy rights are key considerations in developing third-party agreements;
- Carefully vet potential service providers to assess their knowledge and capabilities to meet the PSO's defined privacy requirements in procurement and contracting; and
- Audit and monitor the service provider's activities for the duration of the agreement to ensure compliance.

Training and Supporting Resources

Standard 4. Training for Employees, Officers, Consultants and Agents to Perform their Duties

PSOs must provide relevant and effective training and supporting resources to their employees and officers who collect or have any access to personal information so that they clearly understand how to comply with the requirements of the ARA, the regulations and the Standards.

PSOs must ensure that their consultants and agents who collect or have any access to personal information have relevant and effective training and supporting resources so that they clearly understand how to comply with the requirements of the ARA, the regulations and the Standards.

Rationale

Training and supporting resources are essential for the proper application of the Standards.

Guidance

Employees, officers, consultants and agents of organizations should complete any necessary training before they begin their duties and should receive training regularly thereafter, as needed, to ensure ongoing compliance. In addition to establishing knowledge of how to protect personal information, training objectives should include building competencies and capacities in anti-racism and cultural safety.

Resources should reinforce learning and maintain knowledge, and should include relevant tools for applying skills and techniques.

Training and support resources should be periodically reviewed and evaluated so that they are relevant, effective, and delivered efficiently to relevant employees, officers, consultants, and agents.

2. Collection of Personal Information

The purpose of collecting personal information under subsection 7(2) of the ARA is to eliminate systemic racism and advance racial equity.

Manner of Collection

Subsection 7(3) of the ARA requires that personal information be collected directly from the individual to whom the information relates, unless the Standards authorize another (indirect) manner of collection.

Standard 5. Direct Collection

PSOs must collect personal information directly from the individual to whom it relates unless otherwise authorized by Standard 6.

Rationale

Collecting personal information directly from the individual to whom it pertains is critical to ensuring that voluntary express consent is sought and obtained. It also respects individual dignity.

Guidance

In addition to collecting personal information from the individual to whom it relates, direct collection can include collecting personal information from an individual who is legally authorized to act on behalf of another individual. This could be a parent with custody of a minor, a legal guardian, or an individual working under a power of attorney.

Prior to collection, PSOs should verify the individual's legal authority to act on behalf of the other individual. They should also document the verification (see Standards 8 and 9 for consent and notice requirements).

Standard 6. Indirect Collection

PSOs are authorized to collect personal information indirectly in the following circumstances:

- The individual to whom the information relates authorizes another person to provide their personal information
- The individual to whom the information relates is deceased
- Collection of participant observer information (POI) about another individual's race is undertaken in accordance with Standards 38-43 (see Section 7: Standards for POI).

Rationale

Indirect collection of personal information may be necessary in the circumstances described above because direct collection is not possible or because collecting POI is appropriate in the circumstances.

Guidance

At the time of collection, an individual may wish to authorize another person to provide their personal information. This could be a neighbor, friend, roommate, co-worker, support worker or interpreter. Such authorization can be given by the individual orally to the PSO (in person or over the telephone) or by written consent signed by the individual to whom the information relates. In both cases, the authorization should be recorded and retained by the PSO.

In the case of deceased persons, indirect collection should only take place where there is no apparent trustee for the estate of the deceased person. In this case, PSOs should collect the information from someone close to the deceased individual, like the individual's next of kin.

In specific circumstances, PSOs may collect POI about an individual's race only for the purpose of identifying and monitoring racial profiling or racial bias within a specific service, program, or function. Individuals providing POI are limited to employees, officers, consultants, and agents of the PSOs. Further standards and guidance on this form of indirect collection can be found in Section 7.

Consent

Personal information collected directly from the individual to whom it relates must be based on voluntary express consent that is freely given. Subsection 6(8) of the ARA states that no program, service or benefit shall be withheld because an individual does not provide, or refuses to provide, the personal information requested by the PSO. In obtaining consent, PSOs should be careful to make the request in a manner that does not pressure the individual.

Standard 7. Obtain Express Consent

PSOs collecting personal information directly (as set out under Standard 5) must obtain express consent in a way that respects the privacy and dignity of individuals.

Express consent must be knowledgeable and obtained after the individual has been directly provided the information set out in Part 1 of Standard 8 (direct collection).

The required information must be provided in an accessible manner, whether orally, or in writing, or both.

The individual may withdraw consent at any time by providing notice to the PSO, but the withdrawal of the consent does not have retroactive effect where the personal information has already been used by the organization to conduct analysis.

Rationale

Voluntary express consent is an essential part of respecting an individual's privacy and dignity. Every individual, at any time, has the right to give, deny or withdraw their consent for the collection, and use of their personal information.

Guidance

Express consent is permission for or agreement to the collection and use of personal information. It is given orally, in writing, or by some other positive action specifically by the individual to whom the personal information relates.

Under this form of consent, an organization needs to provide the individual with an opportunity to actively communicate positive agreement to the collection of their personal information. This is in contrast to implied consent, which is an assumption of permission inferred from silence or inaction, such as requiring individuals to "opt out" of the collection. Express consent is less likely to result in misunderstandings or complaints.

Openness, transparency, and accessibility are essential to obtaining meaningful consent. PSOs should clearly explain the voluntary nature of consent, how the requested personal information will be used and disclosed (where relevant), and how the information will be protected. This enables individuals to make informed decisions about what they are consenting to and ensures that they understand that they have the right to withhold or revoke their consent at any time.

When obtaining express consent, PSOs should give special consideration to the capacity of the individual to provide consent. When a PSO determines that an individual does not have the capacity to consent, consent may be obtained from a person legally authorized to act on the individual's behalf, such as a family member or legal guardian.

PSOs should maintain records of consent provided, withheld, or withdrawn and include the dates of consent. If the personal information is collected online, PSOs should provide a click-through notice that requires respondents to consent to the collection and use of personal information before they proceed.

Withdrawal of consent

Individuals should be informed that they may withdraw their consent to the continued use of their personal information at any time during the collection and over the period during which their personal information is held by the PSO.

Individuals may withdraw consent, and request that the organization delete or stop using their personal information (see Standard 23 Removal of Personal Information for required action after consent is withdrawn). An individual can withdraw their consent by oral or

written request to the organization. A withdrawal of consent does not require the PSO to re-conduct analyses that may have used the personal information (the withdrawal does not have retroactive effect).

Notices

The ARA requires PSOs to provide different types of notice for direct (s. 7(4)) and indirect (s. 7(5)) collection, and before they use personal information already in their possession that was collected for another lawful purpose (s. 9(5)).

Standard 8. Notices

Prior to collecting personal information, PSOs must provide notice, either orally or in writing, in a way that is inclusive, accessible, and respects individual privacy.

Part 1 - Notice to Individual - Direct Collection

The ARA (s. 7(4)) requires that when personal information is collected directly, the PSO must inform the individuals providing the information of the following:

- That the collection is authorized under the ARA;
- The purpose for which the personal information is intended to be used, including whether it will be combined with other information, including personal information;
- That no program, service or benefit may be withheld because the individual does not provide, or refuses to provide, the personal information; and
- The title and contact information, including an email address, of an employee who can answer the individual's questions about the collection.

Part 2 - Notice – Indirect Collection

The ARA (s. 7(5)) requires that when personal information is collected indirectly, before collecting the information, the PSO must first publish the following information on a website:

- That the collection is authorized under the ARA;
- The types of personal information that may be collected indirectly and the circumstances in which personal information may be collected in that manner;
- The purpose for which the personal information collected indirectly is intended to be used, including whether it will be combined with other information, including personal information; and
- The title and contact information, including an email address, of an employee who can answer an individual's questions about the collection.

Part 3 - Notice - personal information already collected under another Act

If the PSO is required or authorized to collect personal information under regulation, the organization may use for an ARA purpose other personal information it has lawfully collected. Before using the other personal information, the ARA s. 9(5) requires that

PSOs provide public notice on a website stating that the use is authorized under the ARA, and:

- The types of information that may be used and the circumstances it would be used, including whether it will be combined with other information, including personal information;
- That the purpose for which personal information may be used; and
- The title and contact information, including an email address, of an employee who can answer an individual's questions about the use of the personal information.

Part 4 - Notice -- Individual Authorizes Another Person to Provide Their Personal Information

If an individual authorizes a PSO to indirectly collect their personal information from another person, the PSO must provide notice to the authorized individual in the same manner as in the case of direct collection (Part 1, above).

Part 5 – Notice of Rights to Access, Correct and Withdraw Consent

When giving notice, PSOs must also provide notice that individuals may access and correct their personal information, or withdraw their consent.

In the case of POI, notice must be provided that individuals may access the POI that relates to them and may request that a statement of disagreement be attached to the POI.

Rationale

In both direct and indirect collection, notice informs individuals about why their information is being collected and how it will be used. It also enables those individuals to contact PSOs to get answers to any questions they may have about the collection and subsequent use of the information.

In addition, notice is an essential part of obtaining express consent from the individual to collect and use personal information. It ensures that individuals understand the purpose of the collection and use and know that providing their personal information is voluntary.

Guidance

Notice may be given orally, in written form, or both. PSOs collecting POI (indirect collection) must give notice on their websites.

PSOs should provide individuals with supporting materials, such as informative pamphlets or responses to frequently asked questions, particularly if notice is given orally.

PSOs should provide notice in a way that is inclusive and responsive to the individual's needs and respects individual dignity. Notices should be:

- Concise and accessible, in accordance with the *Accessibility for Ontarians with Disabilities Act, 2005* (AODA) and its regulations;
- In plain language and readily understandable; and
- Available in alternative formats and translations, as necessary.

Notices should inform individuals about what they are consenting to and why. PSOs should clearly explain the following:

- What information is being collected under the ARA;
- Why it is being collected;
- How it will be used, and whether it will be combined with other personal information; and
- Who will have access and how privacy will be protected.

Forms used to collect personal information, if separate from the notice, should also state clearly that the collection is voluntary, and that no program, service, or benefit will be withheld if the individual does not provide or refuses to provide the information requested.

Where a PSO's interaction with Indigenous peoples requires the application of a distinct legal analysis or process, PSOs should ensure that the client is also informed of the applicable provisions.

The ARA provides that nothing in the ARA limits the right of an individual to access and correct personal information held by the PSO in accordance with the access and correction provisions of another Act (e.g. FIPPA or MFIPPA). In providing notice with respect to both direct and indirect collections, PSOs should inform individuals about any limitations to accessing or correcting their personal information or withdrawing their consent, if such limitations exist under another Act. Similarly, individuals should be informed of their ability to access and request a statement of disagreement to POI information held by a PSO. Individuals should be informed that the correction and removal of personal information does not have retroactive effect.

How to Collect Personal Information

Standard 9. Collection Methods

PSOs must collect personal information using methods and processes that are accessible in accordance with the AODA and its regulations, and that protect individual confidentiality and privacy, and respect individual dignity.

Rationale

Appropriate collection methods and processes that are accessible, protect confidentiality and privacy, and respect individual dignity help to promote the quality of the information collected.

Guidance

Methods for collecting personal information may include online forms, paper or telephone surveys, registration forms, and oral interviews. Personal information collected through oral interview or telephone survey should be accurately recorded in an appropriate and secure manner.

Collection methods should be responsive to the needs of individuals and communities, which may include administering the collection in other languages. PSOs that are subject to the *French Language Services Act,* 1990 (FLSA) should ensure that notices and methods used to collect personal information are available in French.

It is important that employees, officers, consultants, and agents of PSOs are trained to collect personal information in a respectful, culturally safe, accessible way that ensures individual privacy and confidentiality. This is especially important when personal information is collected by interview.

A culturally safe and respectful method of collection means that individuals feel physically, socially, emotionally and spiritually safe. There is no challenge or denial of a person's identity and the experience does not diminish, demean, or disempower the cultural identity or well-being of the individual. In addition, this consideration recognizes that, due to the ongoing impacts and legacies of colonization and systemic racism, Indigenous, Black, and racialized people may be uncomfortable with giving personal information about Indigenous identity and race.

Employees, officers, consultants, and agents of PSOs collecting personal information should be prepared to address basic questions or concerns about the collection, including the purpose for the collection, how the information will be used when it can and cannot be disclosed, and how privacy will be protected.

Designing surveys to enhance data quality

PSOs should design their collection processes to support the accuracy and completeness of personal information collected. This includes careful consideration of response options that have been shown to negatively impact the quality and rate of responses.

Survey methodology research has shown that providing non-response options (such as "don't know" and "prefer not to answer") to socio-demographic questions tends to decrease data quality and response rates. It is generally *not* recommended to include these options unless they help to provide useful or valid information. PSOs should consider whether the non-response options can be used and analyzed if collected. For example, consider whether "don't know" is a valid response and whether that response would be used in analyzes or simply treated as a non-response (treated as missing data).

The potential usefulness of non-response options should be balanced against any compromise to data quality. In some contexts, such as when personal information is collected during an oral interview, "prefer not to answer" can be useful to distinguish

between a client who declined to answer the question and a client who was not asked the question by the interviewer.

Prior to asking questions that may be considered sensitive, PSOs should remind clients that the collection is voluntary. To promote higher response rates, they should make sure that all clients understand the purpose of the collection and how their information will be used and protected.

Particularly in the context of longer surveys, it is good practice to remind individuals that they are providing information voluntarily and remind them of the purpose and benefits of providing information.

PSOs using online collection methods should avoid forcing responses (for example, where a respondent must select a response in order to advance to the next question). If a forced-response design is used, then “prefer not to answer” is necessary to ensure that individuals can choose not to provide the information requested.

When to Collect Personal Information

Standard 10. Identifying an Appropriate Time to Collect Personal Information

PSOs must collect personal information at the earliest appropriate time in an individual’s interaction with a program, service, or function.

The collection process must respect the dignity of the individual from whom personal information is collected and minimize repeated requests for the same personal information.

Rationale

Collecting personal information at the earliest appropriate opportunity helps to identify and monitor an individual’s outcomes throughout their participation in a program, service, or function.

Guidance

When feasible and appropriate, it is best to collect personal information at an individual’s first interaction with the program, service, or function, such as at recruitment, registration, or enrolment.

There may be circumstances when direct collection from the individual at the earliest opportunity is overly intrusive or could injure a person’s privacy and dignity. For example, accident victims still at the scene of the accident or individuals being booked into a detention centre may be in crisis, which may make it an inappropriate time to collect personal information. In such cases, the earliest appropriate opportunity should be found.

In other instances, for example in the case of Indigenous accused persons, it may be necessary to gather personal information at the earliest possible stage to ensure that the individual receives relevant services and supports. Federal and provincial legislation,

including the *Criminal Code of Canada,* the *Youth Criminal Justice Act,* and the *Child, Youth and Family Services Act* distinguish Indigenous people and require judges and various justice personnel to apply distinct principles, provisions, and processes. Training is essential to ensure that an Indigenous person has the opportunity to self-identify as soon as possible and that the relevant justice personnel are informed.

Order of Questions

Standard 11. Sequence of Indigenous Identity and Race-Related Questions

Where personal information about Indigenous identity, ethnic origin and race are collected, PSOs must sequence the questions so that Indigenous identity and ethnic origin are asked immediately prior to race.

Rationale

The order in which questions are asked helps to promote the accuracy of responses.

Guidance

Research on survey methods shows that the order of questions affects how people respond. Questions that come first provide a frame of reference that influences how respondents interpret and answer later questions.

The sequence of questions can help to improve response rates and the accuracy of the race information provided. When individuals are asked to provide information about more specific identities (such as Indigenous identity and ethnic origin) before they are asked about race, they are more likely to select a race category and less likely to write in a unique response or refuse to answer.

The question about religion can be placed either before the Indigenous identity question or after the race question.

Collection of Personal Information

In accordance with subsection 6(6) of the ARA, the Standards specify the personal information that PSOs may be required or authorized to collect under a regulation made under s. 7(1) of the ARA.

Standard 12. Collecting Personal Information to Better Understand Systemic Racism

The regulations under the ARA may require or authorize PSOs to collect the following personal information:

- Indigenous Identity
- Race

- Ethnic origin
- Religion
- Age
- Sex
- Education
- Geospatial information, such as postal code for place of residence, or place of work
- Socio-economic information, such as educational level, annual income, employment status, occupation, or housing status
- Citizenship
- Immigration status
- Gender identity and gender expression
- Sexual orientation
- Place of birth
- Languages
- Marital status
- Family status
- (Dis)abilities

Rationale

The types of personal information listed above may be relevant for analyzing systemic racial inequalities in outcomes by considering the intersection of race with other social identities. It also supports a better understanding of the factors that potentially contribute to, reinforce, or underlie systemic racial inequalities in outcomes.

Guidance

Collecting personal information about Indigenous identity, race, religion and ethnic origin is essential to the purpose of the ARA. However, additional types of personal information may be necessary to understand the nuances of systemic racial barriers. This means recognizing the ways in which people's experiences of racism or privilege, including within any one racialized group, may vary depending on the individual's or group's additional overlapping or intersecting social identities.

For example, a race-based intersectional analysis could explore whether systemic racial barriers are different for men and women, or for different age groups. Indigenous, Black and racialized individuals may experience unique and distinct systemic barriers shaped by multiple and overlapping identities and social locations such as disabilities, low income, language barriers, etc. The use and analyses of additional personal information can help identify other factors that impact group outcomes.

PSOs should seek to limit the personal information requested to the minimum necessary to fulfill the purposes of collecting the information. For example, if annual household

income is relevant but the analysis will not require narrow brackets or exact amounts, consider using the broadest meaningful income brackets.

Collection of Personal Information about Indigenous Identity

Standard 13. Collecting Personal Information about Indigenous Identity

PSOs must collect personal information about Indigenous identity (First Nations, Métis, and Inuit) to assist in the identification and monitoring of Indigenous people's unique experiences of systemic racism and marginalization.

The collection of personal information about Indigenous identity must follow the question and response rules set out below.

The question and response values may deviate from the below at the request of Indigenous communities, or if data sharing agreements are in place between PSOs and Indigenous communities or organizations. However, responses have to map to "First Nations," "Métis," and "Inuit" for the purpose of analyses and reporting under the ARA.

Indigenous Identity Question and Categories

Question: Do you identify as First Nations, Métis, and/or Inuit? If yes, select all that apply.

Values (valid code list):

1. No
2. Yes, First Nations
3. Yes, Métis
4. Yes, Inuit

Optional Value: Prefer not to answer (permitted only in oral interview processes to record that the question was asked and the respondent chose not to answer).

Response rules: If yes, respondents may select multiple options – First Nations, Métis, and/or Inuit. Respondents may not select both no and yes.

Rationale

Collecting personal information about Indigenous identity in the manner described above (First Nations, Métis, and Inuit) is consistent with the approach undertaken by Statistics Canada, in which "First Nations" includes status and non-status Indians. Collecting this information helps to identify and understand Indigenous peoples' unique experiences of systemic racism resulting from a history of colonialism and the impacts of intergenerational trauma. This contributes to the Ontario government's commitment to identify and eliminate anti-Indigenous racism in programs, services, and functions.

Flexibility in collecting information about Indigenous identity respects Indigenous interests in determining cultural expression and identification.

The option “prefer not to answer” is allowed when information is collected through oral interview (in person or by telephone). The purpose is to differentiate a client who decides not to answer from a client who was not asked the question.

Guidance

PSOs should work with Indigenous communities and partners to help determine best practices for collecting personal information about Indigenous identity. At the community’s request, or as part of data sharing agreements, a PSO may change how it collects information about Indigenous identity so that Indigenous peoples can self-identify in other, more specific ways, such as:

- Allowing an additional level of response (e.g. provide an open text or drop-down list option for individuals who select “First Nations,” “Métis,” or “Inuit”); or
- Adding “Another Indigenous identity” as a fourth option and allowing open text (write in response option); or
- Including a separate question allowing for individuals to identify a specific First Nations band or community.

It is important to train all employees, officers, consultants, and agents of PSOs to collect personal information about Indigenous identity in a respectful, culturally safe, accessible way that ensures individual privacy and confidentiality and is responsive to the needs of individuals and communities. They should be prepared to address questions or concerns about the collection of Indigenous identity information, including the purpose and benefits of the collection, and how the information will be collected, used, when it can and cannot be disclosed and protected.

Collecting personal information about specific Indigenous cultures, communities, and nationhood

Collecting personal information about Indigenous identity can inform more effective delivery of programs and services that support Indigenous cultural expression and self-determination. It is important that collection processes respect Indigenous culture and nationhood and capture the diversity of Indigenous people who access public services. This supports the advancement of racial equity, and respects Indigenous peoples’ constitutional status.

Indigenous identity categories limited to “First Nations, Métis and Inuit” may not be enough to capture information relevant to policy implementation and service and program delivery or to meet the needs of Indigenous individuals and communities across the province. In frontline service settings, requesting more specific cultural information may be necessary to ensure culturally appropriate services, including language of service, spiritual accommodations, and other required supports. For example, the questions may

help identify need for increased access to services in an Indigenous language, or offering basic spiritual supports appropriate to a specific community.

Collection of Personal Information about Race

Standard 14. Race Question

PSOs must collect personal information about race using a preamble and question that enables individuals to self-report race as a social description or category. The following preamble and question are consistent with this approach:

> Pre-amble: In our society, people are often described by their race or racial background. For example, some people are considered “White” or “Black” or “East/Southeast Asian,” etc.
>
> Question: “Which race category best describes you? Select all that apply.”

Rationale

Systemic racism is shaped by how society categorizes individuals into racial groups. Race is a social construct, not a reflection of personal identity (as distinct from individual, ethnic or cultural identity). The approach to “race” reflected in the Standards best serves the purpose of identifying and monitoring systemic racism.

Guidance

PSOs should use the preamble and question provided in this Standard unless there is strong evidence that a more plain language version is appropriate and improves the collection of race information.

Wherever feasible, a preamble should be placed immediately before the race question to help respondents understand what the question will be asking. If collecting information online, PSOs may choose to provide the preamble and category descriptions or examples as an “info tip” or “tool tip” (text that appears when a curser hovers over the item without clicking) to make the question clearer.

For the purposes of identifying and monitoring systemic racism barriers and disadvantages, it is important to recognize race as a social construct. Ideas about race are often ascribed to or imposed on people, and individuals and groups can be racialized by others in ways that affect their experiences and how they are treated. Race as a social category is distinct from but may overlap with how people identify themselves, which can be much more varied and complex.

The race question provided in this Standard aligns with how researchers and organizations in other jurisdictions ask questions about race. Using race categories that measure and reflect how an individual may be described by others helps to better identify Indigenous, Black, and racialized communities’ experiences and treatment in society.

Standard 15. Race Categories

PSOs must collect personal information about race using the race categories and applying the response rule set out in the table below.

PSO must present the categories in alphabetical order unless there is evidence that a different order might increase response rates, such as most to least frequent responses to reflect local demographics or individuals most likely to access a program, service, or function.

Wherever feasible, online surveys, forms, and interviews must include the examples or descriptions provided to help individuals select the appropriate responses. Organizations must not introduce subcategories under the required race categories, except where noted in Table 1.

Table 1. Valid Values for Race Categories

Race categories*	**Description/examples**
1. Black	African, Afro-Caribbean, African-Canadian descent
2. East/Southeast Asian (Optional**: May collect as two separate categories – East Asian and Southeast Asian)	Chinese, Korean, Japanese, Taiwanese descent Filipino, Vietnamese, Cambodian, Thai, Indonesian, other Southeast Asian descent
3. Indigenous (First Nations, Métis, Inuk/Inuit) ***	First Nations, Métis, Inuit descent
4. Latino	Latin American, Hispanic descent
5. Middle Eastern	Arab, Persian, West Asian descent, e.g. Afghan, Egyptian, Iranian, Lebanese, Turkish, Kurdish, etc.
6. South Asian	South Asian descent, e.g. East Indian, Pakistani, Bangladeshi, Sri Lankan, Indo-Caribbean, etc.
7. White	European descent
8. Another race category	Another race category not described above [optional to allow write-in response]
Prefer not to answer (Optional value)	Permitted only in oral interview processes to record that the question was asked and the respondent chose not to answer.

Response rule: Respondents may select all that apply.

Notes:

* A separate standard for race categories applies for POI data (Section 7 Standards for Participant Observer Information).

** Organizations may collect ‘East/Southeast Asian’ as two separate categories, with appropriate examples provided, where there is evidence this would improve data quality.

*** If providing examples on the form, then “First Nations, Métis, Inuit” need only be included once.

Rationale

The race categories reflect how people generally understand and use race as a social descriptor in Ontario. These are considered commonly used categories, but individuals may describe their racial backgrounds in ways that are not equivalent to the categories above. Therefore, the open text or “Another race category” option is included.

Some people have more than one racial background. Allowing multiple selection instead of a generic “mixed race” option provides more accurate information.

Guidance

Race categories are used to identify and track the impacts of potential systemic racism, including how individuals may be racialized and may experience inequitable treatment or access to programs, services, and functions as a result.

PSOs choosing to provide an open text response option for “another race category,” should give additional instructions to respondents that they should not to write in “mixed” or “bi-racial” but rather select as many categories as apply.

East Asian and Southeast Asian may be separated into two response options instead of one. This should only be done if the PSO has evidence that presenting them separately is more responsive to clients’ needs and would improve the accuracy of responses.

“Indigenous” refers to people who are indigenous to North America (First Nations, Métis, Inuit), and is included to help with understanding how Indigenous peoples may be racialized as a group. This is distinct from the question about whether an individual self-identifies as First Nations, Métis, and/or Inuit, which is collected separately.

Identifying race categories used in Ontario

The categories in this Standard are the main race categories commonly used as social descriptors in Ontario. They are not based on science or biology but on differences that society has created (i.e. is “socially constructed”). Over time, stereotypes and biases associated with racial categories can function to produce and maintain unequal levels of

power between social groups on the basis of perceived differences, often based on physical appearance, with unfair advantages for some and disadvantages for others.

Race is distinct from ethnic origin and religion. For example, “Black” is a racial category that includes people of diverse cultures and histories. “Jamaican,” on the other hand, is an ethnic group with a widely shared heritage, ancestry, historical experience, and nationality. Some Ontarians with Jamaican origins may self-report as White, South Asian, or East/Southeast Asian. Similarly, people from many different racial backgrounds can share the same or similar religion, and people can share a racial background but hold different religious beliefs.

Race categories are distinct from geographic regions. Names of geographic regions are used in this Standard (East/Southeast Asian, Middle Eastern, and South Asian) to refer to groups of people perceived to belong to a racial group with common ancestral origins in that particular region of the world.

Individuals described by some categories, such as “Black,” “East/Southeast Asian,” “South Asian” and “White” may currently live anywhere in the world.

Collection of Race-Related Personal Information

Standard 16. Collecting Personal Information about Religion

PSOs must collect personal information about religion using the question and response rules below to identify and monitor systemic racism and racial disparities in outcomes that people may experience on the basis of religion.

Religion refers to an individual’s self-identification or affiliation with any religious denomination, group, or other religiously defined community or system of belief and/or spiritual faith practices.

PSOs may include examples for the values below, or subcategories as needed, to be responsive and inclusive and help individuals select the appropriate response. However, responses must be mapped to the nine categories below for analyses and reporting under the ARA.

Religion Question and Categories

Question: What is your religion and/or spiritual affiliation? Select all that apply.

Values (valid code list):

1. Buddhist
2. Christian
3. Hindu
4. Jewish
5. Muslim
6. Sikh
7. Indigenous Spirituality
8. No religion
9. Another religion or spiritual affiliation (option to provide open text response)

Optional Value: Prefer not to answer (permitted only in oral interview processes to record that the question was asked and the respondent chose not to answer).

Response Rule: Respondents may select all that apply.

Rationale

People can experience racism based on their religion, or perceived religion, which may lead to unique adverse impacts and unequal outcomes. In addition, there may be differences in experiences of systemic racism within and between religious groups.

Guidance

Where authorized under the regulations, PSOs should consider collecting personal information about religion where there have been human rights complaints or cases involving religious grounds, particularly where racism is an alleged factor.

The OHRC's Policy on Preventing Discrimination Based on Creed states that religious differences are racialized when they are:

- Ascribed to people based on appearances or outward signs (e.g. visible markers of religion, race, place of origin, language or culture, or dress or comportment);
- Linked to, or associated with, racial difference;
- Treated as fixed and unchanging (naturalized) or in ways that permanently define religious or ethnic groups as the "other" in Ontario;
- Ascribed characteristics or negative stereotypes as uniformly shared by all members of a faith tradition; or
- Presumed to be the sole or primary determinant of a person's thinking or behaviour.

Islamophobia and antisemitism are examples of how religion can be racialized. People can experience racism not only based on skin colour but also other apparent differences based on perceived characteristics associated with religion.

Islamophobia includes racism, stereotypes, prejudice, fear, or acts of hostility directed at individual Muslims or followers of Islam in general. In addition to individual acts of intolerance and racial profiling, Islamophobia can lead to viewing and treating Muslims as a greater security threat on an institutional, systemic, and societal level.

This may result in Muslims being treated unequally, evaluated negatively, and excluded from positions, rights, and opportunities in society and its institutions (see OHRC Policy on Preventing Discrimination Based on Creed).

Antisemitism includes latent or overt hostility, hatred towards, or discrimination directed at individual Jews or the Jewish people for reasons connected to their religion, ethnicity, and cultural, historical, intellectual and religious heritage. Antisemitism can take many forms, ranging from individual acts of discrimination, physical violence, vandalism and hatred, to more organized and systematic efforts, including genocide, to destroy entire communities (see OHRC Policy on Preventing Discrimination Based on Creed).

It is important to understand the complexities and differences in experiences of systemic racism. This may mean examining intersections between race and religion; for example to identify whether Middle Eastern Muslims experience unique barriers compared with non-Muslims, or Muslims who are described as White.

Standard 17. Collecting Personal Information about Ethnic Origin

PSOs must collect personal information about ethnic origin using the question and response rules below to identify and monitor systemic racism and racial disparities in outcomes that people may experience based on ethnic origin.

Ethnic origin refers to a person's ethnic or cultural origins. Ethnic groups have a common identity, heritage, ancestry, or historical past, often with identifiable cultural, linguistic, and/or religious characteristics.

Ethnic Origin Question and Categories

Question: What is your ethnic or cultural origin(s)?

For example, Canadian, Chinese, East Indian, English, Italian, Filipino, Scottish, Irish, Anishnaabe, Ojibway, Mi'kmaq, Cree, Haudenosaunee, Métis, Inuit, Portuguese, German, Polish, Dutch, French, Jamaican, Pakistani, Iranian, Sri Lankan, Korean, Ukrainian, Lebanese, Guyanese, Somali, Colombian, Jewish, etc.

Values (valid code list):

Open text box (specify as many ethnic or cultural origins as applicable) or provide drop-down list of values as reported in Ontario, Census 2016.

Optional Value: Prefer not to answer (permitted only in oral interview processes to record that the question was asked and the respondent chose not to answer).

Response Rule: Respondents may select or write-in more than one ethnic origins.

Rationale

Perceived differences based on ethnic origin may be racialized and lead to adverse impacts and unequal outcomes. In addition, there may be ethnic differences in experiences of systemic racism within and between racial groups.

The examples of ethnic origin set out in the question are provided in order of most commonly reported single ethnic origins in Ontario in the 2016 Census. They include five examples of Indigenous origins, and one from each world region.

Guidance

Personal information collected about ethnic origin is used for the purpose of identifying and monitoring systemic racism and advancing racial equity. Individuals may experience systemic barriers in unique ways on the basis of ethnic origin. Collecting and analyzing this information can help to identify and evaluate the underlying systemic racial barriers more precisely. For example, an accent associated with a particular ethnic origin can be racialized.

Personal information about ethnic origin lawfully collected by PSOs for other purposes may also be used to help identify distinct ethno-cultural needs and to support the development and delivery of culturally responsive programs and services.

3. Protection and Management of Personal Information

Securing Personal Information

Subsection 7(11) of the ARA requires PSOs to take reasonable steps to secure personal information throughout its life cycle; for example, during transmission, storage and disposal (transportation, handling and destruction or transfer to an archive).

Standard 18. Secure Personal Information and Manage Privacy Breaches

PSOs must document and have in place reasonable measures to ensure that:

- Personal information is protected against theft, loss, unauthorized access or use, tampering, disclosure, or destruction; and
- Records (hard copy and electronic) containing personal information are protected against unauthorized copying, modification, or disposal.

PSOs must have in place a privacy breach management and response protocol that documents:

- The steps needed to identify, assess, contain, manage and respond to known or suspected privacy breaches;
- Requirements for third party service providers;
- When it is appropriate to notify affected individuals; and
- When it is appropriate to report a breach to the IPC.

Rationale

Maintaining the confidentiality, integrity, and availability of personal information is necessary to carry out requirements of the ARA, the regulations and the Standards.

This includes protecting against privacy breaches resulting from theft, loss, unauthorized access, use, or disclosure, and unauthorized copying, modification, or disposal. Having clear privacy breach management and response protocols is essential for mitigating harm arising from such incidents.

Guidance

PSOs should develop, document, implement, and maintain security policies and procedures that address obligations under the ARA, the regulations and the Standards, and other relevant legislation, including FIPPA/MFIPPA. This should be done in consultation with the organization's privacy officer or FIPPA/MFIPPA coordinator and security professionals.

PSOs' security measures should include administrative, technical and physical safeguards (see Appendix B). These measures should cover people, processes and technology and protect the confidentiality, integrity, and availability of information. In addition, PSOs should identify and address security risks presented by remote access (e.g. use of mobile devices), internet/web applications, and electronic transmission of personal information.

PSOs should also make sure that security measures are appropriate and proportional to the nature of the personal information to be protected by considering the following:

- Sensitivity and amount of personal information;
- Number and nature of people with access to the personal information; and
- Threats and risks associated with the personal information.

Organizations should have protocols for employees, officers, consultants and agents of organizations to identify and report security issues to an accountable manager. They should also implement routine maintenance and updates of database management systems used to store, retrieve, and manage records.

Detailed guidance on security safeguards may be found in the Government of Ontario Information Technology Standards (GO-ITS) related to security.

Privacy breaches can have significant impacts on the individual to whom the information relates. Upon learning about a privacy breach, PSOs should take the following immediate action:

- Implement the organization's privacy breach protocols;
- Identify the scope of the breach and take action to contain it;
- Identify the individuals whose privacy was breached, and when appropriate, notify them accordingly;

- Inform the IPC of the breach when appropriate, including information about the circumstances; and
- Investigate the causes and take steps to address deficiencies and avoid breaches in the future.

The IPC's guidelines on *Preventing and Managing Breaches* is a helpful resource.

Secure Storage in Databases

Standard 19. Storage of Personal Information in Electronic Format

PSOs must maintain all personal information collected under the ARA in a secure database that is part of, or can be linked to administrative records.

If the personal information is collected for both the purpose of the ARA and another lawful purpose, it must be maintained in accordance with the privacy and security requirements under applicable legislation (e.g. FIPPA or MFIPPA).

Rationale

Storage of personal information in a secure database enables the analysis of individual outcomes and long-term trends in order to identify potential systemic racial inequalities.

Guidance

PSOs should make sure that their security measures related to the storage of personal information (including hard copy and electronic, on-site and off-site, third-party service providers) are appropriate and proportional to the nature and sensitivity of the personal information and records to be protected.

If personal information collected under the ARA is kept in a data set that is separate from the administrative data set, a unique pseudonym or identification number can be assigned to each record so that only a designated manager is able to link the data sets as necessary to facilitate analyses.

Limiting Access to Personal Information

Subsection 7(13) of the ARA requires organizations to limit access to personal information to only those individuals who need it in the performance of their duties, in connection with requirements under the ARA, the regulations and the Standards. The ARA prohibits the use of personal information if other information could meet the purpose, and requires that no more personal information be used than is reasonably necessary to meet that purpose (s. 7(8)).

Standard 20. Limit Access on a Need-to-Know Basis

PSOs must determine the level of access to personal information that their employees, officers, consultants, and agents require in the performance of their duties under the ARA, the regulations and the Standards. Access to personal information must be limited according to the determination.

Rationale

To protect personal privacy and confidentiality, access to specific personal information is limited to those who need it to do their jobs. They should have access to no more than is necessary for the purpose. This reduces the risk of privacy breaches caused by unauthorized access and therefore helps protect privacy.

Guidance

Employees, officers, consultants, and agents of the PSO should not have access to personal information collected under the authority of the ARA unless it is needed for the performance of their duties. For example, frontline staff do not have access to individuals' Indigenous identity or race information unless they need that information to perform their job responsibilities.

In addition, PSOs should define role-based access by each data element rather than by entire databases (i.e. avoid broad or blanket access unless such access is necessary). Access should not be allowed to:

- Personal information if access to other information will meet the same purpose; or
- More personal information than is reasonably necessary to meet the purpose.

In conducting analyses, organizations should extract from original datasets only the personal information required for the analysis at hand. Remove any personal information that directly identifies specific individuals (e.g. names, addresses, telephone numbers) and/or replace direct identifiers with pseudonymous or encrypted information ("masking").

Accuracy

Subsection 7(12) of the ARA requires that, before using personal information, PSOs take reasonable steps to ensure that the information is as accurate as is needed for the use.

Standard 21. Accuracy of Personal Information

PSOs must document and have policies and procedures in place to monitor and maintain the accuracy of personal information collected, stored, used, and disclosed for the purposes of the ARA.

PSOs must take reasonable steps to enter personal information accurately into electronic records ("databases").

Variables related to Indigenous identity and race must be coded in electronic records as specified below. PSOs must assign and enter codes for religion and ethnic origin variables using values that correspond with how personal information is collected under Standards 16 and 17.

Coding of Indigenous Identity Information

Where PSOs collect information using discretionary options, such as “Another Indigenous identity” as an open text field, then additional fields and codes may be created as appropriate.

Data element: Indigenous Identity

Description: Indicates if a person identifies as First Nations, Métis and/or Inuit

Field Names: There are separate fields for each Indigenous identity category under this data element, and labelled as follows:

- Non-Indigenous only
- First Nations
- Metis
- Inuit
- Prefer not to answer (Where this is a valid option)

Field type and format: Field type is discrete, and format is numeric (1)

Code set (Valid values): Binary, e.g. 0= Not indicated, 1= Yes

Missing data (Null value): Blank or “.” (period) for null value, if no valid response is provided i.e. both no and yes are selected, unknown/value not provided for all categories

Default values: Blank or “.” (null value)

Multiplicity: A person may change their Indigenous group identification over time or change their response from one collection point to another. Systems may need to consider and take into account how to record changes or deal with different responses recorded for the same individual if collected from a number of sources.

Coding of Race Information

See Section 7 for separate data entry rules for participant observer information data (POI).

Data element: Race

Description: Indicates an individual’s race(s) as a social category or descriptor

Field Names: There are separate fields for each race category and labelled as follows:

- Black
- East/Southeast Asian (may be two fields if collected separately)
- Indigenous
- Latino
- Middle Eastern
- South Asian
- White
- Another Race
- Prefer not to answer (Where this is a valid option)

Field type and format: Field type is discrete, and format is numeric (1)

Exception: If “Another race category,” is open text, then the field type is qualitative and format is alphanumeric (25).

Code set (Valid values):
For numeric fields: Binary, e.g. 0= not indicated and 1= yes
For alphanumeric field: (i.e. Another Race) any character string.

Missing data (Null value): Blank or “.” (period) for null value, if Race is unknown/value not provided.

Default values: n/a

Multiplicity: A person may change their perception of their race over time or change their response from one collection point to another. Systems may need to consider and take into account how to record changes or deal with different responses recorded for the same individual if collected from a number of sources.

Rationale

To promote the integrity of analyses, continuous efforts are necessary to ensure that personal information is accurate, complete, and up to date.

Quality assurance protocols help to ensure accuracy. They also increase public confidence and trust in the integrity of the personal information collected, used, and disclosed, as well as in the information published and reported.

Guidance

PSOs’ quality assurance plan should set out their policies and practices to check accuracy including the following:

- Documented methods, processes, data dictionaries and codebooks, and protocols for information management; and

- Systematic data quality assurance checks to monitor and maintain data quality (accuracy, reliability, validity, consistency, timeliness, and completeness of personal information), such as verifying the accuracy of personal information, data entry, output tables, and analyses.

PSOs should take reasonable steps to check for accuracy, including errors or omissions, according to a quality assurance plan. They should do so at the point when personal information is collected and when it is processed and entered into databases. The coding rules above are minimum requirements for consistently entering information into databases. Where PSOs collect information using discretionary options such as “another Indigenous identity” as an open text field, then additional fields may be created, as appropriate.

Before using or disclosing personal information, PSOs should assess and document its quality, such as whether and to what degree:

- The accuracy of the information has been verified;
- The information is current (e.g. individuals had appropriate opportunities to update their personal information); and
- The information is complete (e.g. the information that is collected represents the population of all eligible individuals).

PSOs should take reasonable steps to make sure that they do not use personal information unless it is accurate and up to date. Before use, PSOs should also check to see if the personal information has been corrected or if there is a statement of disagreement attached to the record. In the limited instances where personal information collected under the ARA may be disclosed (e.g. for research purposes) PSOs should also take reasonable steps to make sure they only disclose accurate and up to date information.

PSOs regulated under the ARA are required to report on the quality of information used (see Standard 36).

If the collection is done using hard copy and then entered into electronic systems, PSOs should conduct random audits to assess the accuracy, validity, completeness, and timeliness of the electronic information.

Access to, and Correction and Removal of Information

The ARA (s. 7(17)) and Standards do not limit the rights of individuals under any Act (e.g. FIPPA or MFIPPA) to access and correct their own personal information.

Standard 22. Access to and Correction of Personal Information

PSOs must document and have procedures in place to allow individuals to request access to or correction of their own personal information in the custody or control of the organization.

These procedures must provide and ensure that individuals can

(a) Request correction of the personal information where the individual believes there is an error or omission; and

(b) Require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and

(c) Require that any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required be notified of the correction or statement of disagreement.

Rationale

The ability of individuals to access and correct their personal information is important to respect individual dignity and to support the accuracy of the personal information. It also enhances the transparency of PSOs' practices under the ARA.

Guidance

This Standard does not apply to POI (see Standard 43).

PSOs should provide clear, plain language instructions on how individuals can request access to and correction of their personal information. The instructions should be included in notices to individuals and posted on PSOs' websites. PSOs should allow individuals to make written or oral requests to access their personal information or to correct a record. They should also verify the requester's identity before responding to a request.

For both access and correction requests, PSOs should document the following:

- Who was given access, when and how access was provided, and who was the authorizing decision maker; and
- What correction was made and why; or
- The reason(s) for denying access or correction, and how and when this decision was communicated to the requestor.

Information technology systems should be able to record statements of disagreement to be attached to the personal information if a request for correction is not accommodated.

Corrections to personal information do not require organizations to redo analysis that has already been conducted.

Standard 23. Removal of Personal Information

PSOs must document and have procedures in place to remove personal information when an individual to whom the information relates withdraws their consent for its continued use and disclosure and requests the removal of their personal information.

Rationale

An important aspect of voluntary express consent and respect for individual dignity is that individuals must be able to withdraw their consent and effect the removal of their personal information.

Guidance

This Standard does not apply to POI (see Standard 43).

If the personal information was collected under the authority of the ARA, withdrawal of consent means that the personal information is removed and can no longer be used for ARA purposes.

Removal of personal information may mean deletion, sequestering, or suppressing the personal information so that it can no longer be used or disclosed. In some circumstances, a withdrawal of consent may not require destruction or deletion of the information. For example, the PSO may have a duty to document decision-making associated with the information. The removal of personal information should take effect within a reasonable time after the request is made.

The PSO should provide clear information to individuals, at the time of collection, that they may withdraw their consent at any time. Individuals should also receive clear instructions on the procedures to request removal of personal information should they wish to do so. This information should be given in the notice as well as posted on the PSO's website.

PSOs should verify the individual's identity before responding to an oral or written request to remove personal information. PSOs should maintain a record of removal requests that includes the date of request, the response, the action taken, and the person who authorized the action.

Removal of personal information does not require PSOs to redo analysis conducted using the personal information that has been removed.

Retention of Personal Information

The ARA s. 7(10) requires PSOs to retain personal information for the period specified in the Standards or, if there is no such specified period, for at least one year after the day it was last used by the organization.

Standard 24. Five-year Retention Period

PSOs must retain personal information that is stored in electronic databases for at least five years after the day it was last used, or for as long as reasonable and necessary for the purposes of identifying systemic racism and advancing racial equity unless an individual requests removal of their personal information.

Rationale

Retaining personal information in databases for at least five years allows analysis of long-term trends and longitudinal analysis that requires personal information. It also enables the review and re-analysis of historical information based on issues that may arise over time.

Defined retention periods help PSOs ensure that they do not hold on to personal information for longer than is needed for the purposes of the ARA. Indefinite retention could be expensive and administratively burdensome and could create an increased risk of privacy breaches.

Guidance

The retention period defined in this Standard applies to POI entered into an electronic record in accordance with Standard 42.

However, this retention period does not apply to personal information kept in transitory records, such as paper or online forms used to collect the information. Transitory records are records of temporary usefulness in any format or medium, created or received by PSOs to carry out information collection activities.

Once personal information is transferred into a database for secure storage, the transitory records should be destroyed in a secure manner, following the organization's records disposal schedule and protocols, or disposed of according to the ARA default retention period (at least one year after last use).

Hard copy records that are not transitory and have been entered into an electronic database should be retained according to the organization's records retention schedules, where the organization is subject to the *Archives and Recordkeeping Act, 2006*, or otherwise in accordance the organization's recordkeeping policies or any other legal requirement..

Public sector organizations may need to update their retention schedules for electronic records to comply with the Standards. If planning to conduct longitudinal analysis over a period greater than five years, PSOs should define reasonable retention periods for the personal information and should not retain it indefinitely.

PSOs should consult with their information management staff, as well as their privacy officer or FIPPA/MFIPPA coordinator, to determine if there are other operational or legal obligations that may require longer retention of personal information.

When personal information is updated or corrected, the outdated information may be retained in some form so that it is available for the retention period defined in the Standard.

If withdrawal of consent results in removal of personal information before the approved retention period expires, PSOs should to document the action taken.

Disposal of Personal Information

Standard 25. Secure Disposal

PSOs must take reasonable steps to securely dispose of personal information maintained in records (hard copy or electronic), including:

- Protecting the security and confidentiality of personal information that is to be destroyed or transferred to an archive, including protecting its security and confidentiality during storage, transportation, handling, and destruction;
- Ensuring that personal information is securely destroyed in such a way that it cannot be reconstructed or retrieved; and
- Securely disposing of devices with memory capabilities (e.g. computers, phones, photocopiers, fax machines).

Where a PSO is subject to the *Archives and Recordkeeping Act*, 2006 the personal information kept in records must be disposed of either by transferring it to the Archives of Ontario (if such transfer is required by an approved records retention schedule) or by securely destroying it.

PSOs must maintain a disposal record that sets out the authority for the disposal, the personal information disposed of, who approved disposal, how it was disposed of, and the date of the disposal. This disposal record must not contain personal information.

Rationale

Secure disposal of personal information protects privacy and reduces the risk of privacy breaches.

Guidance

PSOs should implement a protocol and schedule for the systematic permanent destruction of hard copy and electronic records, and maintain a disposal record.

PSOs should work with a records and information management and privacy professional to create schedules for records series that contain personal information collected under the ARA. The schedules should specify disposition requirements, including disposal or transfer to the Archives of Ontario, subject to the approval of the Archivist of Ontario, for those organizations subject to the *Archives and Recordkeeping Act*, 2006.

Organizations not subject to any legal requirements related to the destruction of personal information should follow the provisions of the related FIPPA regulation (O.Reg.459) *Disposal of Personal Information*, in order to implement Standard 25.

Methods for the destruction of personal information should be appropriate to the level of sensitivity of the information and the type of storage medium.

Where the disposal is undertaken by a third party service supplier, the PSO should require the supplier to provide a “certification of destruction” signed by an officer of the company. This certificate should be linked to the disposal record maintained by the PSO.

Limits on Use

According to subsection 7(6) of the ARA, personal information collected may only be used for the purpose of eliminating systemic racism and advancing racial equity as defined in subsection 7(2). In addition, subsections 7(8) and 9(3) of the ARA provide that PSOs shall not use the personal information if other information would meet the same purpose (if de-identified information may serve the purpose, personal information should not be used).

Section 9 of the ARA permits a PSO to use personal information it has already lawfully collected for the purpose of eliminating systemic racism and advancing racial equity, subject to requirements specified in the ARA, the regulations and the Standards.

This enables organizations to use personal information collected for another lawful purpose for the analysis of racial impacts and outcomes of a program, service, or function. For example, an organization that is already collecting personal information about individuals (e.g. age and sex) or tracking individual outcomes (e.g. performance measures) within a program, service, or function may use this information for the purpose of identifying and monitoring systemic racism and racial disparities.

Standard 26. Limiting Use of Personal Information

PSOs must only use personal information collected under the authority of the ARA to the extent that it is needed to eliminate systemic racism and advance racial equity in its services, programs or functions.

PSOs must only use personal information collected under the authority of the ARA in the least identifiable form required to fulfill the purpose of the use, including the purpose of conducting analyses.

Rationale

Minimizing the amount of personal information used to the meet the purposes of the ARA protects privacy and reduces the risk of privacy breaches (i.e. unauthorized use of personal information).

Guidance

PSOs should not use personal information collected under the ARA for any purpose that are not directly related to eliminating systemic racism and advancing racial equity.

Under the ARA, analysis is a core use (see Section 4: Analyses of Information Collected).

Before using personal information for any authorized purpose, PSOs should first determine whether personal information is needed for the activity or analysis. For

example, they should consider whether the analysis could be done with de-identified information. If personal information is required, then PSOs should minimize the identifiability of the personal information by using appropriate de-identification techniques (see Appendix C). The data should only be used in the least identifiable form required to fulfill the purpose.

PSOs should assess the appropriate level of de-identification required for the use according to a spectrum ranging from fully identifiable personal information to de-identified data:

> *Fully identified personal information*: Data containing direct and indirect identifiers.
>
> *Pseudonymous data*: Data from which direct identifiers have been removed or replaced with a confidential code or pseudonym.
>
> *De-identified data:* Data that has been transformed or modified so that there is no reasonable expectation in the circumstances that the information could be used, either alone or with other information, to identify an individual.

Where direct and indirect identifiers are not required in the analysis of a program, service, or function, remove any information that directly identifies a specific individual and assign a unique pseudonym or identification number to the record (masking) so that it can be linked back to databases containing administrative records by a designated decision maker.

De-identification is contextual. What is considered de-identified data in one context may not be considered de-identified data in another. For example, when names, addresses, and telephone numbers are removed from a data set (pseudonymous data), but case numbers are left in, that data set is considered de-identified only if it is accessed by authorized individuals without access to clients' case file information. However, that same data set is not considered de-identified if it is accessed by authorized individuals who also have access to data sets containing case numbers and clients' names, addresses, and other personal information.

The need to de-identify personal information prior to public release and reporting is defined in Standards 33 and 34.

Limits on Disclosure

Subsection 7(14) of the ARA restricts disclosure of personal information to the following circumstances:

- The individual to whom the information relates consents to the disclosure;
- It is required by law, including as required under section 31 of the *Code*;
- It is for the purpose of a legal proceeding, or contemplated proceeding;
- It is for research purposes, in accordance with section 8 of the ARA; or
- It is being disclosed to the IPC.

Subsections 7(15) and 7(16) establish exemptions to these disclosure rules. In this respect, if personal information has been collected for a lawful purpose in addition to the ARA purpose that information may be disclosed subject to the permissions and limits on disclosure under any other applicable law.

Section 8 of the ARA sets out the circumstances under which a PSO may disclose personal information for research purposes. This includes approval of a research plan by a research ethics board as well as justification that the research cannot be reasonably accomplished with information in de-identified form. The ARA and regulations define the requirements PSOs and researchers must follow.

4. Analyses of Information Collected

To achieve the purposes of the ARA, analyses of the collected personal information is necessary. The ARA and Standards require that PSOs minimize the amount of personal information used in analyses and use it in the least identifiable form possible. Access is limited to those who need it to perform their duties under the ARA.

In addition to information collected under the ARA, section 9 permits a PSO to use other personal information it has lawfully collected for the purpose of eliminating systemic racism and advancing racial equity, subject to rules specified in the ARA, the regulations and the Standards.

This enables PSOs to use that information to analyze racial impacts and outcomes of a program, service, or function. For example, an organization that is already collecting personal information about individuals (e.g. age and sex) or tracking individual outcomes (such as performance measures) within a program, service, or function, may use this information for the purpose of identifying and monitoring systemic racism and racial disparities.

Units of Analysis

Standard 27. Primary Units of Analysis

PSOs must conduct analyses using primary units of analysis, namely the disaggregated categories of Indigenous identity and race. The disaggregated categories of religion and/or ethnic origin may also be primary units of analysis wherever these are collected under the ARA.

Units of analysis (categories) must be aggregated if doing so is necessary to protect individual privacy and does not affect findings of racial inequalities.

Rationale

Although personal information is collected about individuals, the purpose of the analysis is to identify and monitor systemic racial inequalities in outcomes for groups. This

requires analyzing results by disaggregated categories of Indigenous identity and race, as well as other categories like religion and ethnic origin where these are collected under the ARA.

Guidance

The categories of Indigenous identity and race are the focus of analyses. Analyses using disaggregated categories are a minimum requirement. The Standard does not preclude additional analyses using merged or aggregated categories, such as “mixed or multiple race,” “racialized,” etc., as long as disaggregated analyses are also conducted.

Multiple Race Categories

Some people report more than one racial background. Analysis should be sensitive to commonalities and differences in experience and treatment among persons reporting multiple race categories.

In some cases, it may make sense to count persons who report White and some other race according to the other race category selected. For example, the experience of an individual reporting as Black and White may have experiences more closely resembling that of an individual reporting only as Black. For analytical purposes, therefore, it may be appropriate to categorize individuals that report both Black and White as Black. This approach is consistent with Statistics Canada’s practice (see Appendix D: Using Statistics Canada Data Sets for Benchmarking).

In other circumstances, it may be necessary and appropriate to aggregate or construct socially meaningful mixed-race categories. For example, a generic mixed-race category may be appropriate if there are insufficient or small numbers of individuals (fewer than 15) who select multiple race categories.

If a generic mixed-race category might obscure significant differences, and sample sizes are sufficient, consider using specific combinations of race categories such as ‘White and Black,” “White and South Asian,” “Black and South Asian,” “Black and Indigenous,” etc.

Intersectional Race Analysis

Analyses of racial disparities and disproportionalities may also include intersections among Indigenous identity, race, and/or religion, ethnic origin and any other relevant types of personal information (age, gender identity, immigration status, disabilities, sexual orientation, etc.).

Additional units of analysis may include categories of other personal information (if collected or used for the purpose set out in the Act) for intersectional analyses with Indigenous identity, race, and religion or ethnic origin. For example, in analyses of race and gender, the unit of analysis would be the combination of race and gender categories (interaction terms); for example, “South Asian male,” “South Asian female,” etc.

Analyses of Outcomes

Standard 28. Focus on Outcomes

PSOs must conduct disproportionality and/or disparity analyses using outcomes of individuals accessing a program, service, or function.

Rationale

Use of outcome data with Indigenous identity, race, and race-related data is necessary to identify and monitor potential systemic racial inequalities in programs, services, or functions.

Guidance

In addition to the personal information collected under the ARA, personal information that PSOs have already collected as part of administrative functions is an important source of data on the outcomes of programs, services, or policies. Personal information lawfully collected under another statute can be used for the purposes of analyses under the ARA (s. 9).

For the purpose of conducting analysis under this Standard, an outcome is client-focused. This could include outputs of an organization's programs, services, or functions, such as receipt of benefits or services provided, access to programs delivered, etc. Outcomes should include the results or impacts of interactions between a client and service provider, such as those arising from a decision, treatment, or assessment. Where possible, outcomes should reflect the results or impacts at any stage of the clients' interactions with the organization's program, service, or function and should including the final outcome.

Racial disproportionalities and disparities can result from decisions that have the effect of privileging some and disadvantaging others. It is important to identify outcomes for individuals within a policy, program, service, or function, such as:

- Penalties, sanctions, or fines;
- Awards or privileges;
- Promotions and appointments;
- Access to appropriate treatments, services, or programs; or
- Quality of treatment or experiences.

Outcomes that reflect an individuals' access, experiences, or treatment in the program, service, or function may have significant cumulative impacts on final outcomes for individuals. It may be helpful to map the pathway of potential outcomes at various stages of a clients' involvement in a program, service, or function (see Appendix A for an example of mapping outcomes in the child protection system).

PSOs should engage with Indigenous, Black, and racialized communities, partners and stakeholders to identify meaningful outcomes to analyze and report. Consider a balanced

approach that includes tracking and monitoring both positive and negative outcomes of policies, programs, services, and functions.

Minimum Requirements for Analysis

Standard 29. Racial Disproportionality and Disparity Indices

PSOs must produce racial disproportionality and/or racial disparity indices for each unit of analysis.

- A racial disproportionality index is a measure of a racial group's overrepresentation or underrepresentation in a program, service, or function relative to the group's representation in the reference population.
- A racial disparity index is a measure of group differences in outcomes by comparing the outcomes for one group with those of another.

Calculating Racial Disproportionality Index

The disproportionality index is calculated using this equation,

$$DISPROPORTIONALITY_A = \frac{\left(\frac{\#GroupA\_\mathrm{Pr}ogramPop}{\#Total\_\mathrm{Pr}ogramPop}\right)}{\left(\frac{\#GroupA\_BenchmarkPop}{\#Total\_BenchmarkPop}\right)}$$

where:

#GroupA_ProgramPop **is the number of individuals of Group A in a program population**

#Total_ProgramPop **is the total number of all individuals in the program population**

#GroupA_BenchmarkPop **is the total number of individuals of Group A in a benchmark population (or eligible population)**

#Total_BenchmarkPop **is the total number of all individuals in a benchmark population (or eligible population)**

Calculating Racial Disparity Index

The racial disparity index (also known as a risk ratio or relative risk index) is calculated as follows:

a)

$$DISPARITY_{A/B} = \frac{DISPROPORTIONALITY_{GroupA}}{DISPROPORTIONALITY_{GroupB}}$$

b) An equivalent equation is:

$$DISPARITY_{A/B} = \frac{\left(\frac{\#GroupA\_\text{Pr}ogramPop}{\#GroupA\_BenchmarkPop}\right)}{\left(\frac{\#GroupB\_\text{Pr}ogramPop}{\#GroupB\_BenchmarkPop}\right)}$$

c) The disparity index can be constructed using other statistics such as averages, rates, etc:

$$DISPARITY_{A/B} = \frac{Rates\_per\_thousand_{GroupA}}{Rates\_per\_thousand_{GroupB}}$$

Rationale

Racial disproportionality and disparity indices are reliable and valid measures that are widely used to quantify racial inequalities within a program, service, or function.

Guidance

The racial disproportionality or disparity index are methodologies commonly used by various levels of government in Canada, the U.S., and the United Kingdom to compare the outcomes of populations or groups in sectors such as child welfare, youth and adult justice (including policing, courts, and corrections), education, and health.

In determining whether to use the racial disproportionality or disparity index, PSOs should engage with Indigenous, Black, and racialized communities, representatives, and partners, subject matter experts, and internal and external stakeholders.

See Appendix E for further guidance on racial disproportionality and disparity analyses and some illustrative examples.

Benchmarks and Reference Groups

Standard 30. Appropriate Benchmarks for Disproportionality Analyses

PSOs must choose and document the source(s) of appropriate benchmark(s) that reflect the most relevant eligible population to which the outcome is applicable and that are useful for interpreting year-over-year trends.

Rationale

The appropriate benchmark population shapes the interpretation of disproportionality analyses and the identification of long-term trends.

Guidance

A benchmark is a baseline against which outcomes may be compared or assessed. Benchmarks are integral to the calculation of racial disproportionalities and disparities. Appropriate benchmarks should come from the best available data sets that contain relevant data about the applicable population for a specific outcome, such as:

- Administrative data sets that contain comparable Indigenous identity, race, religion, and/or ethnic origin information; or
- Statistics Canada's data sets, which are important and commonly used sources for establishing benchmarks of population groups in Ontario (see Appendix D for further considerations when using Statistics Canada data sets for benchmarking).

As an example of relevant benchmarks, when examining participation in a program, the number of people who are eligible for that program may be a more appropriate benchmark than the population of a city or region because not everyone in that population will be eligible.

Standard 31. Appropriate Reference Group for Disparity Analyses

PSOs must choose and document the source(s) of an appropriate reference group that allows for meaningful interpretation of patterns and trends that may be indicative of systemic racism. Where possible, the reference group should allow for interpreting results in the context of racial disparities reported in other sectors.

Rationale

The reference group is a type of benchmark used in racial disparity analyses to provide the contrast needed for meaningful interpretations of group differences in outcomes.

Guidance

Unlike benchmarks used to calculate disproportionalities, which may draw on a different data set, data used to construct the reference group should come from the same data set.

The choice of a reference group can affect the interpretation of findings by potentially hiding or revealing differences between groups. For example, using "all other groups" as a reference may result in lower disparities found if there are broad differences in outcomes between groups captured under that category.

In some circumstances, the appropriate reference group may be the group least likely to experience systemic barriers or systemic racism in Ontario. For example, to assess racial disparities in the justice sector, the outcomes of each group could be compared to the group least likely to experience systemic racism. In this case, the most appropriate reference group for consistent comparisons across the justice sector is the "White" category.

PSOs should engage with Indigenous, Black, and racialized communities and partners to determine the appropriate reference group. For example, in some cases, Indigenous communities or partners may not support or agree with comparisons between Indigenous peoples and non-Indigenous peoples.

Interpreting Analyses

Interpreting racial disproportionalities and disparities is a critical step in identifying potential notable racial inequalities.

Interpretation of disparity and disproportionality results involves attempting to understand the scope and magnitude of the results, and exploring possible explanations for the findings. This is done by:

1. Comparing disproportionality or disparity results against a threshold;
2. Examining the patterns of results over time; and
3. (Where feasible) conducting analysis of more than one variable (multivariate analysis) to assess the extent to which other factors help explain the outcome (e.g. gender, age, poverty).

Interpretation is best informed by a combination of the following:

- Input from subject matter experts, stakeholders, and affected communities;
- Reference to existing research literature and other sources of information; and
- Comparisons against cross-sector and national findings.

Standard 32. Setting Thresholds to Identify Notable Differences

PSOs must set thresholds for each outcome measure of a program, service, or function, which, if met or exceeded, indicates a notable difference. Thresholds must be

- Reasonable, set in good faith, and reflect engagements with affected communities;
- Set consistently for all racial groups (different thresholds may not be set for different groups); and
- Focussed on adverse impacts or disadvantageous outcomes that would require remedial action.

Rationale

Using an appropriate threshold helps the organization to interpret the meaning of numerical results. It indicates whether the magnitude of the disproportionality and disparity indices represents a notable difference for further investigation, monitoring, and potential action.

Guidance

Appropriate and meaningful thresholds are expected to vary based on the nature and context of the outcome being assessed. Having common criteria for identifying thresholds is important to ensure transparency in the interpretation of analyses.

Thresholds should be established based on an analysis of numerical information (using statistical methods) as well as advice from community partners, stakeholders, and subject matter experts. If applicable, the thresholds should also be informed by case law.

The following considerations should underpin the accurate interpretation of results:

- Even small racial disproportionalities and disparities can be the result of systemic racism and can have tangible impacts on an individual's or group's quality of life.
- Tests for statistical significance do not necessarily provide guidance on the interpretation of results as evidence of notable differences.
    - For small groups, tests of statistical significance may not show that significant differences exist in the sample used, even when they do exist in the population.
    - For large groups, tests of statistical significance tend to indicate significant differences, even when very small.
- Interpret with caution and use statistical tests that are appropriate for smaller sample sizes (e.g. where the number of individuals in the underlying population is 25 or less). The reliability of results is lower with smaller samples.

Using thresholds to interpret results

A disparity or disproportionality index greater than or less than 1, does not necessarily indicate that group differences exist within a service, program, or function that are unfair or cause for concern. For example, a program may be designed to support a particular group, in which case the over-representation of that group in the program is to be expected.

Focussing on adverse impacts when setting a threshold (i.e. for *either* over- *or* under-representation) is important because not all differences are of concern. For example, if an organization sets a threshold of 2.0 to indicate a notable racial disproportionality in high school drop-out rates within a specific program, and finds a racial disproportionality index of 1.3 for Group A in a school district, and 2.6 for Group B, then there is evidence of a notable difference for Group B, but not for Group A. All disparity or disproportionality results should be reported, regardless of whether they meet the threshold.

Further assessments to understand potential racial inequalities

Racial disproportionality or disparities on their own may not be conclusive evidence of systemic racial inequalities.

Methods of further analysis could focus on determining the extent to which a racial disproportionality or disparity may be attributed, in whole or in part, to systemic racism.

Multivariate analysis is one method used to identify other factors, such as socioeconomic conditions, that may help explain differences in group outcomes.

For example, a notable difference is found for Group A when compared with Group B. How much of this difference is due to a higher proportion of recent immigrants in Group A? A multivariate analysis helps to identify the unique effect of race on group differences, and how immigration status or other factors might contribute to outcomes independently of race.

Draw on other sources of information to help in the interpretation and understanding of findings. PSOs should use multiple methods, such as qualitative information obtained through focus groups, individual interviews with clients, employees, and experts, policy and program evaluations, research literature reviews, etc.

PSOs are encouraged to establish an advisory committee to support the analysis and interpretation of findings. To provide a diversity of perspectives, advisory committees could include clients, members of affected committees, subject matter experts, and internal and external stakeholders and partners.

5. Public Release and Reporting

De-identification of Personal Information

Subsection 7(9) of the ARA requires PSOs to de-identify the collected personal information as required by the Standards. This will require the PSO to have or engage appropriate expertise in de-identification.

Standard 33. De-Identification for Public Release of Data

Before releasing any data, PSOs must de-identify personal information.

When de-identifying data for public release, PSOs must seek to preserve as much utility in the data as possible, particularly with regard to Indigenous identity and race information, while protecting the privacy of individuals. PSOs should apply de-identification processes in such a way that the Indigenous identity and race categories are kept intact as much as possible.

Rationale

De-identification protects the privacy of individuals. Once de-identified, information or data no longer contains information about, or that can be attributed to, identifiable individuals.

Data about Indigenous identity and race should be maintained as intact as possible to support the public’s access to this information and promote public transparency and accountability.

Guidance

"De-identification" is the process of removing or transforming personal information in a record or data set so that there is no reasonable expectation in the circumstances that the information could be used, either alone or with other information, to identify an individual. PSOs should take into account other available information and data sets that might be used with the de-identified data to re-identify individuals.

Before publicly disclosing data, PSOs should take steps to reduce the risk of re-identification to a level appropriate for public release. The IPC's "De-identification Guidelines for Structured Data" (June 2016), sets out a nine-step process for de-identification, including information on how to assess re-identification risks and risks to groups of individuals. Model practices in the de-identification process involve the following considerations:

1. **Analyze the data, user needs, and data environment** to understand the data set and the context for release, including legal obligations.
2. **Assess re-identification risks**: Re-identification is any process that re-establishes the link between data and an individual. Re-identification risk analysis can be complex and results will differ for each data release.
3. **De-identify data to minimize risk and maximize utility**: Removing, mask or transform variables so that identifiable information is removed to the extent necessary to reasonably protect individual privacy while providing useful data.

PSOs should apply de-identification processes so that Indigenous identity and race variables remain intact to the extent possible. To protect individual privacy, PSOs should first apply de-identification techniques (see Appendix C) as appropriate to the other variables in the data set. In some cases, it may still be necessary to suppress or modify categories of Indigenous identity and race in order to protect individual privacy, for example where the number of individuals included within a category is small. Nevertheless, maintaining the Indigenous identity and race variables in the de-identified data set in a format as close as possible to the original helps to support public transparency and accountability with respect to race-based analysis.

Considering community interests before releasing potentially sensitive information

In addition to individual privacy, risks to groups of individuals should be considered. The de-identification process could also include considerations of community interests, such as the need to prevent the release of potentially sensitive information that could be linked to specific communities (i.e. First Nations communities or specific neighbourhoods).

Although de-identification techniques protect against the disclosure of individuals' identities, they do not specifically protect against the disclosure of potentially stigmatizing attributes relating to groups of individuals. Preventing this may require additional measures such as the removal of geographic information at the census subdivision level or below. For example, census subdivisions can be used to identify First Nations

communities and census tracts can be used to identify specific communities in defined neighbourhoods within cities.

Any decision to release or withhold potentially sensitive information that could be linked to a specific community should be done in consultation with the affected community. The de-identification process should also be done in consultation with the PSO's legal counsel, privacy officer or FIPPA/MFIPPA coordinator.

Managing potential impacts of public release

The release of de-identified data and analyses should be conducted in accordance with established governance and management policies and procedures set out in Standard 2. PSOs should develop and implement a plan to reduce and manage potential re-identification risks and mitigate potential negative impacts on communities:

- Maintain a record of all data released, including descriptions of release model, data types, and properties, as well as processes used for de-identification;
- Perform regular and ongoing re-identification risk assessment of released data by examining it against disclosures of new or overlapping data sets; and
- Identify and communicate with stakeholders, communities, and partners that could be negatively impacted by re-identification and have a plan to mitigate those impacts, including through community outreach, employee training, etc.

Standard 34. De-Identification of Results of Analyses

PSOs must de-identify the results of analyses prior to public reporting.

Rationale

The results of analyses may present re-identification risks depending on the types of data, analyses, and tables to be released. Re-identification risks also depend on the specific circumstances, such as other analyses and data that have already been released and sample sizes (including cell sizes).

Guidance

To minimize re-identification risks when reporting results, the PSO should ensure that it has appropriate expertise in de-identification of analyses and consider:

- Restricting tables to two or three dimensions (i.e. two-way or three-way tables);
- Suppressing results based on small cell sizes;
- Exercising caution when using and reporting results based on small samples; and
- Taking into account other results and data sets that are publicly available or have been previously released.

If other similar analyses are publicly available, PSOs should assess how they may be used to re-identify individuals and take appropriate precautions to address the risk of residual disclosure.

Organizations should consult with their legal counsel, privacy specialists and practitioners within their organizations when preparing to release of de-identified analyses to ensure that personal information is not inadvertently published or otherwise disclosed to the public.

Public Release of Data

Standard 35. Open Data

PSOs must publish de-identified data that they collected and used in reported analyses in a manner that is:

- Open by default (unless there are compelling privacy, security or legal reasons not to do so);
- Available in original, unmodified form, to the fullest extent possible;
- Timely, accurate, and in machine-readable format;, and
- Accessible, permanently available (except where published in error), and offered at no charge to the user.

Data sets must be released on or before the day that the PSO's public report is released.

The data set must be publicly released on the PSO's website or the Ontario Data Catalogue (where applicable), together with metadata containing the relevant key words: Anti-Racism Act, Indigenous identity, race, and where relevant, religion, and/or ethnic origin. Metadata must not include any personal information.

Rationale

Open data helps to ensure transparency and public accountability in identifying and monitoring systemic racism and racial disparities in Ontario's PSOs. It also supports evidence-based public dialogue and debate.

Guidance

Open data is published proactively in free, accessible, and machine-readable formats. Its use by the public as well as within PSOs is encouraged.

Open by default means that data should be open and available unless there are compelling privacy, security, or legal reasons not to do so. Where open by default is not possible for such reasons, the data should not be publicly released.

Metadata is information that describes the characteristics of data. It can be used to help organize, communicate, and exchange information about data. PSOs should take care that metadata does not contain personal information, such as IP addresses, names, or other information that can be used to identify a specific individual.

Where possible, PSOs should undertake the public disclosure of data in consultation with the organization's Open Government staff, privacy officer or FIPPA/MFIPPA coordinator, legal counsel, and parties to data sharing agreements, as applicable.

Organizations should consider the risk of residual disclosure, which can occur when confidential data can be inferred from what is released, or where the information could be used to re-identify individuals. It can also occur by cross-referencing the information released with other accessible information, including previous releases.

PSOs subject to Ontario's Open Data Directive must comply by those rules and submit data sets to the Ontario Data Catalogue (see Open Data Guidebook for more information). Other PSOs should determine whether they are required to follow any Open Government policies, practices and standards.

Organizations should use an open licence, and consider including terms of agreement specifying that the dataset is not to be used in a manner that contravenes the ARA, the *Code*, or any relevant privacy legislation. The Open Government License is an example of an open licence that PSOs can use.

A number of steps are necessary before data can be converted into open and machine-readable format. They include identifying and prioritizing data for release, assessing data quality, reviewing data for accuracy, legal, confidentiality, and privacy and security implications, making data accessible and compliant with any French language requirements, and ensuring that specific technical requirements are met (see Sharing Government Data for more information).

Organizations are encouraged to contact potentially affected communities regarding data sets that may include sensitive information about their communities. Data sharing agreements, if in place, may guide the use and type of release model for public release of data. Under such circumstances, organizations should consider releasing data under different release models. The release model chosen is based on an assessment of the following:

- The purpose and context of the release;
- The sensitivity of the data and re-identification risks;
- Legislative or other requirements to release data; and
- The public interest in access to data.

Public Reporting of Results of Analyses

Standard 36. Public Reporting of Results

On a regular and timely basis, PSOs must develop and make publicly available on their websites, a report that includes:

1. Results of analyses:
    - Descriptive statistics of all variables used in the analyses;
    - Description of benchmarks and/or reference groups; and

    - The racial disproportionality and/or disparity indices;
2. Thresholds set to identify notable differences, including the rationale for them; and
3. Information about collection method and data quality (accuracy, validity, completeness of data collected).

Rationale

Reporting the results of analyses demonstrates transparency and accountability to the public.

Guidance

The report should include a description of methods used to collect the data and relevant information about the population in the data set, including sample sizes, the period over which the data was collected, and any significant limitations in the data.

Descriptive statistics should include information about the data, wherever relevant:

- Frequency (the number of times an observation occurs);
- Mean (arithmetic, such as averages, or geometric means, such as rate of growth);
- Median (the value at which half the observations are below and half are above);
- Range (the minimum and maximum values); and
- Standard deviation (a value that indicates the amount of variation in the data).

Information about the accuracy of the data and statistics helps the public understand any limitations in the results of analysis and the appropriate level of confidence to place in the findings. Accuracy means the degree to which the data and results correctly describe the phenomena they were designed to measure. This is usually evaluated by identifying the potential sources of error. For example, the report should address the common sources of error that may be present:

- Measurement error: Does the data collected reflect the “true” value of the measurement as it was designed to do (is the data valid)?
- Coverage error: Is the population measured adequately covered in the data (to what extent are persons excluded or double-counted)?
- Non-response error: What is the rate of non-response, and does the population with non-response differ from the responding population in some relevant aspect (is there bias in the responses)?
- Sampling error: Does the sample represent the underlying population in relevant ways?

In addition to publishing disparity and/or disproportionality indices, organizations may also report on the results of any other analyses, such as intersectional and multivariate analyses.

Include findings from other sources of information to help provide context and additional perspectives to better understand the results.

Reporting on interpretations of results

Where possible, reports should include interpretations of results focussing on any potential systemic factors. They should be based on evidence, and informed by community and stakeholder engagement.

Evidence used to inform the interpretation of results may include qualitative information, such as historical accounts, descriptions of processes and practices, a systematic review of documents, focus groups, interviews, literature reviews, etc.

When reporting findings, organizations should provide sufficient context to avoid stigmatizing groups (e.g. highlight underlying social and historical disadvantages and marginalization faced by communities with poorer outcomes). Wherever possible, context and narrative should be informed by input from affected communities, stakeholders, partners, and subject matter experts.

Organizations should also be sensitive to histories of mistrust among marginalized communities about how government and PSOs have used data. Care should be taken to communicate clearly about the purpose, uses, and disclosure of the information collected, to respond to inquiries from the public and to engage with the communities affected.

Organizations should anticipate, manage, and mitigate any potential unintended negative impacts on affected communities, stakeholders, and partners. This may include preparing and training employees, communications planning, and outreach to potential affected parties as soon as possible.

Notifying the Minister Responsible for Anti-Racism

Standard 37. Notify the Minister Responsible for Anti-Racism

On the date of public release of open data and/or reporting of analyses, or within a reasonable time shortly thereafter, PSOs must provide the Minister Responsible for Anti-Racism with notice.

This notice must include:

- The name of PSO and a brief description of the program, service, or function;
- Metadata, including date published, location posted (URL); and
- The PSO’s contact information.

Rationale

Notice of public releases to the Minister Responsible for Anti-Racism supports transparency.

Guidance

PSOs should provide the notice to the Anti-Racism Directorate. The notice should include the name, title, division or branch, and contact information (telephone number and email) of an employee who can answer questions about the open data or public report.

Metadata includes information describing how, when and by whom a particular data set was collected and how the data set was formatted. Metadata provided in the notice should include the following, where relevant:

- Coverage: The time period (date range) to which the data set or report applies, and the geographic area or jurisdiction to which the data or report relates;
- Date Created/Modified: The date on which the data set or report was finalized or modified for public release;
- Date Released: The date on which the data set or report was released;
- Update Frequency – The frequency with which the data or report is to be updated;
- Key words: Terms to describe the major themes covered by the data set or report, including types of information and sector;
- Format: The media type or dimensions of the resource, such as comma-separated values (CSV), PDF, etc.; and
- Identifier: A reference to the data set or report using formal identification systems such as the Uniform Resource Locator (URL), the Digital Object Identifier (DOI) and the International Standard Book Number (ISBN).

6. Support and Promote Anti-Racism Organizational Change

Supporting Anti-Racism Organizational Change to Better Serve all Ontarians

Use de-identified data and analyses to support and promote evidence-based anti-racism organizational change and to meet organizational commitments and accountabilities to reduce systemic racism and advance racial equity.

Organizations should ensure that leaders and employees regularly review findings of analyses to:

- Assess potential racial equity impacts and outcomes of policies and programs; and
- Develop, review, and revise policies, programs, services, and functions as necessary to mitigate, remedy, or prevent systemic racial inequalities in outcomes.

PSOs should consider the findings when making strategic and operational plans and decisions in planning cycles.

Indigenous perspectives in decision-making

Indigenous communities are building ways to support their own decision-making processes, including applying data measurement and analysis to inform organizational change. In the wake of the findings of the Truth and Reconciliation Commission of

Canada, it is important to ensure Indigenous perspectives and involvement in decision-making so that services, programs, or functions better reflect the interests and priorities of diverse Indigenous communities in Ontario.

Ongoing Monitoring and Evaluation

Use de-identified data and analyses to monitor and evaluate the effectiveness of anti-racism initiatives in the organization. If personal information is necessary for this purpose, PSOs should use the least identifiable data possible.

Public Education and Engagement

De-identified data and analyses should be used to contribute to public education and advance public discussion about how systemic racial inequalities impact the lives of individuals and the broader society.

Public engagement and education efforts help to increase public confidence that the Government of Ontario is committed to intervening to mitigate and address systemic racial inequalities and advance racial equity. These efforts also help to build support to address systemic racism in Ontario.

7. Standards for Participant Observer Information (POI) Of Race

POI is a type of indirect collection authorized under Standard 6 (Manner of Indirect Collection).

Under the authority of the ARA, these Standards set out specific requirements for the collection, management, and use of participant observer information (POI). All the Standards in previous sections apply to POI except where noted, and with the necessary modifications or exceptions set out below.

POI is an individual's perceptions of another individual's race. This information is collected for the purpose of identifying and monitoring potential racial bias or profiling in a specific service, program, or function. Individuals providing POI (respondents) are limited to employees, officers, consultants, and agents of PSOs.

Planning for the Collection, Management, and Use of POI

Standard 38. Plan for the Collection of POI

Before undertaking POI collection, PSOs must develop and publish a plan for the collection, management, and use of POI that is informed by engagement with affected communities and an assessment of the need for and the risks and benefits of collecting this information.

Rationale

Collecting participant observer information of another person's race is a sensitive endeavour. Due diligence is required in the planning stage to consider the public interest in using this information to eliminate systemic racism and advance racial equity.

Guidance

In developing plans, organizations should consult with communities, stakeholders and partners to inform the assessment of the need for and implementation of POI collection. This can include public posting of notices of intention, holding public meetings, and inviting written submissions on the proposed plans.

Organizations should convene an advisory group to provide critical input on the design, implementation and evaluation of plans. The advisory group should include representatives from the PSO, Indigenous, Black, and racialized communities, stakeholders, and partners.

Circumstances Permitting the Collection of POI

Standard 39. Circumstances in which POI is permitted

PSOs must collect POI only for the specific purpose of assessing racial profiling or bias within a service, program, or function.

The collection of POI may only occur in circumstances that meet the following conditions:

1. The PSO has published a plan as described in Standard 38; and
2. There is a discrete interaction between an individual employed or retained by the organization (“representative of the organization”) and an individual client or member of the public that leads to a decision that determines an outcome; and
3. The representative of the organization involved in the interaction described above has the authority to exercise discretionary decision-making powers over the individual that can have a significant outcome for the individual; and
4. Decisions and/or outcomes arising from that interaction can be measured or documented, such as an individual’s receipt of benefits, penalties, or services, and treatment and/or experiences within a service, program, or function.

Rationale

Identifying and monitoring racial profiling or bias is an important aspect of understanding and addressing systemic racism and racial disparities. Racial profiling or bias arises from a decision maker’s or service provider’s perception of another person’s race, where it impacts their treatment of that person and the outcome.

Guidance

Racial bias is a predisposition, prejudice or generalization about a group or persons based principally on race. The OHRC currently defines "racial profiling" as: any action undertaken for reasons of safety, security or public protection, that relies on stereotypes about race, colour, ethnicity, ancestry, religion, or place of origin, or a combination of these, rather than on a reasonable suspicion, to single out an individual for greater scrutiny or different treatment (refer to the OHRC for the most current definition).

The application of rules, informal practices or decision-making criteria often involves the exercise of discretion on the part of the individual representative of the organization (i.e. service provider or decision maker). In using that discretion, the service provider may draw on racial stereotypes and bias. Discrete interactions with service providers or decision makers, depending on their perceptions of race, can create racial disproportionalities or disparities and significantly impact individual outcomes, as in the following examples:

- A law enforcement worker’s decision to stop or detain individuals.
- A social worker’s decision to bring a child into protective care.

Failing to monitor the impact of such discretionary decision-making may itself constitute a form of systemic racism where it leads to significant racially inequitable outcomes.

POI Race Question and Categories

Standard 40. Mandatory POI Race Question and Categories

PSOs collecting POI for purposes of investigating racial bias or profiling must use the following mandatory race question and categories.

POI Race Question and Categories

“What race category best describes this individual?” (select only one)

1. Black
2. East/Southeast Asian
3. Indigenous (First Nations, Métis, Inuit)
4. Latino
5. Middle Eastern
6. South Asian
7. White

Response rule: The representative of the organization (the respondent) providing the POI may only select one valid response in relation to a particular individual. “Don’t know” and “Prefer not to answer” are not valid response options.

Rationale

Racial bias or profiling occurs when people rely on race-based stereotypes and make assumptions about other people based on visual cues and other information. Thus, racialization is often simply the categorization of individuals. To identify and monitor racial profiling, it is important to capture the perceptions of the persons to assess whether conclusions are being made and acted on based on stereotypes. In this respect the “actual” racial background of the individual to whom the POI relates is less important to the assessment.

“Another race category” is not available under POI. This is based on lessons learned from other jurisdictions and research that shows including that option compromises the validity of responses.

Guidance

A service provider’s perception of another person’s race is based on information that can be readily observed, such as skin colour, hair texture, facial features, and other information that may be used to inform assumptions about a person’s racial background such as accent, dress, surname, etc.

If a person is perceived to be of mixed race, the respondent should choose the race category that, in their view, the person most resembles. That perception would be the most likely driver of any stereotypes or biases.

Non-response options, such as “don’t know” and “prefer not to answer” are not allowed. They are not valid options because they could be used to avoid recording the information.

Organizations should provide instructions and appropriate training to respondents (representatives of the organization) so that they:

- Give their best assessment of the individual, honestly and in good faith; and
- Understand that the collection of this information is authorized or required under the ARA and any other authority where relevant.

Validity of Participant Observer Information

Standard 41. Quality Assurance

PSOs must document and have reasonable measures in place to ensure that the collection of POI is done in good faith and accurately captures perceived race.

Rationale

Before the information can be used, quality assurance methods must be applied to ensure that, to the greatest extent possible, the POI reflects the honest perception of the respondents.

Guidance

Accuracy or validity of POI means the extent to which the POI reflects the honest perception of the respondent during the interaction in question. It does not matter whether the perception reflects the “actual” race of the individual who was assessed.

Quality assurance includes accountability measures and appropriate training for service providers so that they report POI in good faith and understand the purpose of collection. PSOs should have mechanisms in place to identify and address situations where there is evidence that POI collection was given in bad faith or there was willful misrepresentation on the part of an individual who provided the POI.

The validity of POI should be assessed through the organization’s established data quality assurance procedures, and in compliance with any relevant legislation. This could include periodic and random audits or evaluations of POI data collection processes for completeness, validity, and reliability. This helps to promote the integrity of the data collected so that it serves the intended purposes of the data collection.

If the collection is done using hard copy, and then entered into electronic systems, PSOs should conduct random audits to assess the accuracy, validity, completeness, and timeliness of the electronic information.

Standard 42. Accurate Entry and Storage of POI

PSOs must document and have policies and procedures in place to monitor and maintain the accuracy of POI collected, stored, used, and disclosed for the purposes of the ARA.

PSOs must take reasonable steps to enter POI accurately into electronic records (databases) that are stored separately from administrative records containing personal information.

PSOs must code POI in electronic records as specified below.

Coding POI of Another Individual's Race

Data element: POI Race

Description: Indicates the race of an individual as perceived by a service provider

Field Name: POI Race

Field type and format: Field type is discrete, and format is alphanumeric (25)

Code set (Valid values): Field contains alphanumeric values:
- Black
- East/Southeast Asian
- Indigenous (First Nations, Métis, Inuit)
- Latino
- Middle Eastern
- South Asian
- White

Missing data (Null value): Blank or "." (period) for null value, if value is not provided

Rationale

Entering POI accurately and consistently ensures the quality of the data to be used. POI cannot be stored in data sets that are structured such that each record relates to a unique individual. POI should instead be stored in data sets structured so that each record relates to a unique service interaction.

Guidance

To enable disproportionality or disparity analyses, POI may be stored in a secure database that can be linked to information about the outcomes of that interaction. Databases containing outcomes may be maintained in the PSO's administrative databases that contain additional personal information required for the analyses.

For example, records that contain POI may include identification numbers that can be used to link to the PSO's databases containing personal information about the outcomes of interactions with the service provider.

A unique identification number assigned to the respondent should also be recorded for each interaction to enable linking to administrative databases. This allows for analyses to

identify trends or differential patterns of decisions by individual employees, officers, consultants, and agents.

Access to and Disagreement with POI

Standard 43. Access to and Disagreement with POI

PSOs must document and have procedures in place for individuals to request access to POI pertaining to them. If they disagree with the information in the POI, individuals must be able to require that a statement of disagreement be attached to the record.

Rationale

Allowing individuals access to the POI about them is an important aspect of respecting individual dignity. Although a POI relates to an individual, it reflects the perceptions of the representative of the organization giving the information at the moment of collection. To preserve the integrity of the information collected, neither the individual who provided the information nor the individual to whom the information relates may change it.

Guidance

PSOs should be prepared to explain to individuals who request access to the POI related to them why they cannot correct the information. If the individual requests a statement of disagreement, a record of the request and the statement of disagreement must be attached to the POI. This information could be used to verify the accuracy of data collection, and help inform training needs.

Individuals may make written or oral requests for access to personal information or a statement of disagreement. PSOs should verify the requester’s identity before responding to a request.

Information technology systems must be able to record statements of disagreement attached to the personal information.

GLOSSARY

Administrative records: Administrative records is information collected for the purpose of carrying out various non-statistical programs (i.e. to administer programs and provide services). For example, administrative records are maintained to regulate the flow of goods and people, to respond to the legal requirements for registering particular events such as births and deaths, and to administer benefits such as pensions or obligations such as taxation (for individuals or for businesses).

Affected communities: Refers to communities or groups that are directly affected by systemic racism in ways that negatively impact or disadvantage individual members and/or the group as a whole.

Anti-Black racism: Anti-Black racism is prejudice, attitudes, beliefs, stereotyping and discrimination that is directed at people of African descent and is rooted in their unique history and experience of enslavement and its legacy. Anti-Black racism is deeply entrenched in Canadian institutions, policies and practices, to the extent that anti-Black racism is either functionally normalized or rendered invisible to the larger White society. Anti-Black racism is manifest in the current social, economic, and political marginalization of African Canadians, which includes unequal opportunities, lower socio-economic status, higher unemployment, significant poverty rates and overrepresentation in the criminal justice system.

Anti-Indigenous racism: Anti-Indigenous racism is the ongoing race-based discrimination, negative stereotyping, and injustice experienced by Indigenous Peoples within Canada. It includes ideas and practices that establish, maintain and perpetuate power imbalances, systemic barriers, and inequitable outcomes that stem from the legacy of colonial policies and practices in Canada.

Systemic anti-Indigenous racism is evident in discriminatory federal policies such as the Indian Act and the residential school system. It is also manifest in the overrepresentation of Indigenous peoples in provincial criminal justice and child welfare systems, as well as inequitable outcomes in education, well-being, and health. Individual lived-experiences of anti-Indigenous racism can be seen in the rise in acts of hostility and violence directed at Indigenous people.

Anti-racism approach: Anti-racism is a process, a systematic method of analysis, and a proactive course of action rooted in the recognition of the existence of racism, including systemic racism. Anti-racism actively seeks to identify, remove, prevent, and mitigate racially inequitable outcomes and power imbalances between groups and change the structures that sustain inequities.

Antisemitism: Antisemitism is latent or overt hostility, or hatred directed towards, or discrimination against, individual Jewish people or the Jewish people for reasons

connected to their religion, ethnicity, and their cultural, historical, intellectual, and religious heritage.

Benchmark: A benchmark is a point of reference, or standard, against which things can be compared, assessed, or measured.

Colonialism: Colonialism is the historical practice of European expansion into territories already inhabited by Indigenous peoples for the purposes of acquiring new lands and resources. This expansion is rooted in the violent suppression of Indigenous peoples' governance, legal, social and cultural structures. Colonialism attempts to force Indigenous peoples to accept and integrate into institutions that are designed to force them to conform with the structures of the colonial state. "Colonialism remains an ongoing process, shaping both the structure and the quality of the relationship between settlers and Indigenous peoples." (TRC Final Report, 2016 What We Have Learned: Principles of Truth and Reconciliation)

Cultural safety: A culturally safe environment is physically, socially, emotionally, and spiritually safe. There is recognition of and respect for the cultural identities of others, without challenge or denial of an individual's identity, who they are, or what they need. Culturally unsafe environments diminish, demean, or disempower the cultural identity and well-being of an individual.

Data: Data consists of facts, figures, and statistics objectively measured according to a standard or scale, such as frequency, volumes or occurrences, but does not include information (as defined by this directive).

Database: A database (also called electronic database**)** is any collection of data or information that is specially organized for rapid search and retrieval by a computer. Databases are structured to facilitate the storage, retrieval, modification, and deletion of data through various data-processing operations.

Data set (or Dataset): An organized collection of data. The most basic representation of a data set is data elements presented in tabular form. A data set may also present information in a variety of non-tabular formats, such as an extensible mark-up language (XML) file, a geospatial data file, or an image file, etc.

De-identify: In relation to the information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual.

Dignity: Recognition of a person's inherent worth and right to be valued and respected.

Direct identifier: Direct identifiers consist of one or more variables that can be used to identify a single individual, either by themselves or in combination with other readily available sources of information (e.g. name, date of birth, address, email address, etc.).

Disaggregated data: Disaggregated data is broken down into component parts or smaller units of data for statistical analysis. In the context of race-based data, this means breaking down the composite (aggregate) “racialized” category into its component parts such as Black, South Asian, East/Southeast Asian, Latino, Middle Eastern, White, etc.

Ethnic groups: Refers to a person’s ethnic or cultural origins. Ethnic groups have a common identity, heritage, ancestry, or historical past, often with identifiable cultural, linguistic, and/or religious characteristics.

Express consent: Express consent is permission or agreement for the collection, use and disclosure of personal information that is given specifically by the individual to whom the information relates, either orally, in writing, or by some other positive action.

Inclusive: Inclusive processes, policies, services, program and practices are accessible to and useable by as many people as possible, regardless of race, ethnic origin, gender, age, disability, language, etc. An inclusive environment is open, safe, equitable and respectful. Everyone can enjoy a sense of trust, belonging and involvement, and everyone is are encouraged to contribute and participate fully.

Indigenous: Indigenous people identify as being descended from the Original Peoples of what is currently known as Canada. In this context, Indigenous peoples include people who may identify as First Nations (status and non-status), Métis and/or Inuit and any related identities.

Indirect identifier: Indirect identifiers, or quasi-identifiers, are variables for which there is a reasonable expectation that they can be used, either alone or in combination with other information, to identify an individual. Some examples are Indigenous identity, race, ethnic origin, religion, gender, date of birth or age, event dates (death, admission, procedure, discharge, visit), locations (postal codes, building names, regions), country of birth, languages spoken, profession, marital status, level of education, total years of schooling, criminal history, and total income.

Some indirect identifiers may be more likely to lead to the identification of individuals due to their rare occurrence. Characteristics that are highly uncommon in the population or in a data set, such as an unusual occupation or medical diagnosis, can increase the likelihood that the identity of an individual could be revealed.

Individual outcome: Refers to the results of an activity, treatment, program, service or process for an individual (person who is directly or indirectly identified or identifiable).

Information: Ideas, thoughts, knowledge or memories, irrespective of format or medium, constitute information. Information may be represented in manuals, reports, and similar work products and may contain data.

Intergenerational trauma: Historic and contemporary trauma that has compounded over time and been passed from one generation to the next. The negative effects can impact individuals, families, communities and entire populations, resulting in a legacy of physical, psychological, and economic disparities that persist across generations.

For Indigenous peoples, the historical trauma includes trauma created as a result of the imposition of assimilative policies and laws aimed at attempted cultural genocide, including the annihilation of Indigenous Nations, the imposition of the Indian Act system, and the forcible removal of Indigenous children to Indian Residential Schools. Contemporary trauma includes the disparities in access to basic human rights, including clean water, safe housing and minimum standards of income as well as ongoing lack of access to equity in justice, health and child welfare services. Contemporary trauma also includes forced relocation away from ancestral territories and ongoing disputes about Indigenous governance, jurisdiction and decision-making related to resource and other development occurring within Indigenous territories.

Other examples of intergeneration trauma include the ongoing legacies of slavery of people of African descent, as well as the impacts of racial segregation, and the long histories and contemporary forms of racial oppression and violence directed at Black and racialized individuals and communities.

Intersectionality: Intersectionality is the way in which people's lives are shaped by their multiple and overlapping identities and social locations, which, together, can produce a unique and distinct experience for that individual or group, for example, creating additional barriers, opportunities, and/or power imbalances.

In the context of race and Indigenous identity, this means recognizing the ways in which people's experiences of racism or privilege, including within any one group, may vary depending on the individual's or group's relationship to additional overlapping or intersecting social identities, like religion, ethnic origin, gender, age, disabilities or citizenship and immigration status.

An intersectional analysis enables better understanding of the impacts of any one particular systemic barrier by considering how that barrier may be interacting with other related factors.

Islamophobia: Islamophobia is racism, stereotypes, prejudice, fear, or acts of hostility directed towards individual Muslims or followers of Islam in general. In addition to individual acts of intolerance and racial profiling, Islamophobia can lead to viewing and treating Muslims as a greater security threat on an institutional, systemic, and societal level.

Longitudinal analysis: Longitudinal analysis examines measures that involve repeated observations, including observations of people, over a period of time.

Machine readable: In machine readable format, data (or metadata) can be understood and directly used by a computer. See Open Data Guidebook for a list of Machine-Readable file formats.

Marginalization: Marginalization is a long-term, structural process of systemic discrimination that creates a class of disadvantaged minorities. Marginalized groups become permanently confined to the fringes of society. Their status is perpetuated

through various dimensions of exclusion, particularly in the labour market, from full and meaningful participation in society.

Masking: Masking is the process of removing a variable such as directly identifying personal information, or replacing it with pseudonymous or encrypted information.

Metadata: Metadata is information that describes the characteristics of data.

Notable difference: A notable difference is a magnitude of racial disproportionality or disparity that meets or exceeds a threshold considered potentially indicative of a meaningful difference in outcomes.

Open by default: A presumption in favour of disclosure over non-disclosure.

Open data catalogue: A collection of information about data sets, files, or databases that describes where a data set, file or database entity is located, and may also include other information, such as the type of device on which each data set or file is stored.

Open data: De-identified data that are released free of charge to the public in one or more open and accessible formats.

Open format: A set of specifications used to store and transmit digital data that is platform independent, machine-readable, vendor-neutral, standardized where possible, and made available to the public without restrictions that would impede the re-use of that data.

Open government licence: A legal agreement that sets out the terms and conditions relating to Ontario's Open Data.

Open licence: A document that states restrictions and sets out the terms and conditions relating to what can and cannot be done with open data. An open licence grants permission to access, publish, re-use, adapt, copy, redistribute, transmit, or otherwise use open data with few or no restrictions in any medium, mode or format for any lawful purpose.

Participant observer Information (POI): POI is an individual's perception about another individual with who they are interacting, based on observation.

Personal information: Defined under the Freedom of Information and Protection of Privacy Act (FIPPA) as "recorded information about an identifiable individual." FIPPA provides a non-exhaustive list of the types of information considered personal information (see FIPPA).

To be personal information, the information must be:

- "recorded" - personal information is limited to information which is recorded or retrievable in some physical form. It does not include oral comments that have not been recorded.

- about an "individual" - an "individual" is a natural person, a human being. Information about corporations, businesses, groups or organizations is generally not personal information.
- about an "identifiable" individual - if an individual is named in a record or it is possible to determine his or her identity from the contents of the record or from other available information, the record is about an "identifiable" individual.

Race: Race is a term used to classify people into groups based principally on physical traits (phenotypes) such as skin colour. Racial categories are not based on science or biology but on differences that society has created (i.e. “socially constructed”), with significant consequences for people’s lives. Racial categories may vary over time and place and can overlap with ethnic, cultural or religious groupings.

Racial bias: Racial bias is a predisposition, prejudice or generalization about a group or persons based principally on race (see definition of race).

Racial disparity: Racial disparity is unequal outcomes in a comparison of one racial group to another racial group.

Racial disproportionality: The over-representation or under-representation of a racial group in a particular program or system, compared with their representation in the general population.

Racial equity: Racial equity is the systemic fair treatment of all people. It results in equitable opportunities and outcomes for everyone. It contrasts with formal equality where people are treated the same without regard for racial differences. Racial equity is a process (such as meaningfully engaging with Indigenous, Black, and racialized clients regarding policies, directives, practices and procedures that affect them) and an outcome (such as equitable treatment of Indigenous, Black, and racialized clients in a program or service).

Racial inequality: A disparity in opportunity and treatment that occurs as a result of someone's race.

Racial profiling: Racial profiling is any action undertaken for reasons of safety, security or public protection, that relies on stereotypes about race, colour, ethnicity, ancestry, religion, or place of origin, or on a combination of those traits, rather than on a reasonable suspicion, to single out an individual for greater scrutiny or different treatment.

Racialization: Racialization is a process of delineating group boundaries (races) and allocation of persons within those boundaries by primary reference to (supposedly) inherent and/or biological (usually phenotypical) characteristics. In this process, societies construct races as ‘real,’ different, and unequal in ways that matter to economic, political, and social life.

Racialized (person or group): Racialized persons and/or groups can have racial meanings attributed to them in ways that negatively impact their social, political, and economic life. This includes but is not necessarily limited to people classified as “visible

minorities" under the Canadian census and may include people impacted by antisemitism and Islamophobia.

Racism: Racism includes ideas or practices that establish, maintain or perpetuate the racial superiority or dominance of one group over another.

Re-identification: Re-identification is any process that re-establishes the link between de-identified information and an identifiable individual.

Religion: Religion is any religious denomination, group, sect, or other religiously defined community or system of belief and/or spiritual faith practices.

Stereotypes: Qualities ascribed to individuals or groups that are based on misconceptions, false generalizations, and/or oversimplifications that potentially result in stigmatization. A race-based stereotype is a quality ascribed to individuals/groups related to race. Stereotypes can perpetuate racism and racial discrimination and give rise to racial inequalities.

Systemic racism: Systemic racism consists of organizational culture, policies, directives, practices or procedures that exclude, displace or marginalize some racialized groups or create unfair barriers for them to access valuable benefits and opportunities. This is often the result of institutional biases in organizational culture, policies, directives, practices, and procedures that may appear neutral but have the effect of privileging some groups and disadvantaging others.

Threshold: A threshold is a value that, if met or exceeded, indicates an inequality. Determining an appropriate threshold helps to interpret the meaning of the numerical results and indicates whether the magnitude of the disproportionality and disparity indices represents a notable difference for further investigation, monitoring, and/or potential action.

Transitory records: Transitory records are records with temporary usefulness in any format or medium, created or received by a public sector organization in carrying out its activities. Transitory records have no ongoing value beyond an immediate and minor transaction or the preparation of a subsequent record.

APPENDICES

APPENDIX A: Example of Outcomes in Child Protection Services

Using the anti-racism data standards to track and monitor outcomes at different stages of a program, service, or function can help public sector organizations understand where potential systemic racial barriers or disadvantages may be occurring. Visit the Ontario Association of Children's Aid Societies for an example of a typical pathway through the child protection system.

APPENDIX B: Security Safeguards

Organizations should implement appropriative administrative, technical and physical measures to secure personal information, including safeguards such as:

1. Administrative safeguards:
    - Develop, document and implement security management plans, policies and procedures including user access management, access controls and authorization
    - Develop, document and implement security incident management response protocols
    - Develop, document and implement a third party service provider management plan that defines security requirements for service providers including contract provisions, confidentiality agreements, training and education, use of sub-contracting, audits requirements, and appropriate management of personal information when creating, receiving, maintaining, or disposing of it on behalf of the PSO.
    - Define accountability in accordance with Standard 2 to ensure security rules are defined, documented and consistently implemented.
    - Ensure employees, officers, consultants and agents have appropriate security training so they understand required security measures, including appropriate encryption, proper information handling procedures, defenses against improper password use, phishing, malware and ransomware (in accordance with Standard 3).
    - Develop a contingency plan to identify, protect and recover personal information in event of a natural disaster, or loss of power.
    - Monitor and evaluate security plans, policies and procedures, including security incident management response protocols and, when necessary, update and revise.

2. Physical Safeguards:
    - Limit physical access to PSOs' premises and, within premises, to where personal information is used and stored (e.g. electronic information systems, workstations, etc.).

- Restrict access to authorized users of personal information (i.e. use access cards and key, ID badges, screen and supervise visitors, etc.).

3. Technical Safeguards:
   - Restrict access only to those individuals who have been granted access rights by using strong authentication and access controls such as:
     - detailed logging, auditing, monitoring;
     - strong passwords, encryption; and
     - verifying identity prior to access.
   - Record and examine activity in information systems containing or using personal information through detailed logging, auditing, monitoring.
   - Protect personal information from improper alteration or destruction through such measures as:
     - patch and change management;
     - firewalls, anti-virus, anti-spam, anti-spyware;
     - protection against malicious code; and
     - Threat Risk Assessments.
   - Guard against unauthorized access to personal information transmitted over an electronic communications network (i.e. ensure secure transmission of personal information).

APPENDIX C: De-identification of Personal Information

It is important to note that there are different levels of de-identification. The appropriate level depends upon the context (i.e. type of information, proposed use or disclosure, etc.). Also, de-identification does not reduce the risk of re-identification to zero. Rather, the process can produce data sets for which the risk of re-identification is very small.

Classifying and treating information for de-identification

“De-identification” refers to the process of removing or transforming personal information in a record or data set so that there is no reasonable expectation in the circumstances that the information could be used, either alone or with other information, to identify an individual.

Direct identifiers are information that can be used to uniquely identify an individual; for example names, street addresses, telephone numbers, email addresses, Internet protocol (IP) addresses, any other unique identifying number, characteristic, or code.

Masking is the removal of information classified as direct identifiers and/or replacement of direct identifiers with pseudonymous or encrypted information (i.e. unique identification key) to enable linking back to the original data set, if appropriate. Data sets with direct identifiers masked is called a pseudonymous data set.

Indirect, or quasi-identifiers, are information that can be used individually or in combination, usually by someone with background knowledge, to re-identify an individual in the data set. Some examples are gender, dates of events (e.g. birth, marriage, etc.),

income, education, language, etc. Classifying personal information that may be quasi-identifiers requires understanding what other information or data is available, how much someone is motivated to re-identify an individual, and what they know about one or more individuals in the data set.

De-identification techniques

There are a number of de-identification techniques that can be applied to quasi-identifiers, such as removing, suppressing, generalizing or transforming the personal information. Depending on the level of re-identification risk, de-identification techniques may be applied to individual data points (i.e. a specific variable for a specific individual), to a specific variable for all individuals, or to the entire record for a specific individual. Organizations should apply the appropriate techniques necessary to de-identify personal information while maintaining the usefulness of data about Indigenous identity and race.

The de-identification of personal information involves applying different techniques on direct or indirect identifiers to reduce the risk of re-identification to an acceptably low level. Techniques to achieve this include:

- Masking – the removal of personal information classified as direct identifiers or replacement of direct identifiers with pseudonymous or encrypted information.
- Removal – eliminating the variable from the data set
- Suppression – removing or withholding the values of a sensitive cell or variable for particular individual(s), or removing all the personal information of individual(s) from the data set.
- Generalization – reducing precision in the values of a variable, for example, by recording as age intervals instead of exact age; 10-14 years, 15-19 years, etc.
- Top- or bottom coding – restricting the upper and lower range of a variable
- Collapsing categories and/or combining variables – merging two or more categories of a variable, or combining two variables to create a new variable
- Sampling – rather than providing all of the original data, releasing a random sample of sufficient size to yield reasonable inferences
- Swapping – matching unique cases on the indirect identifier, then exchanging the values of key variables between the cases to limit disclosure risk
- Disturbing – adding random variation or stochastic error to the variable.

Types of release models

Organizations may need to consider various release models for use and disclosure for research purposes, with the necessary de-identification and security controls applied.

The following release models represent a spectrum of ways that data can be made available that range from restricted (non-public) to open (public):

- Non-public (restricted): Data is available only to authorized users with specified conditions and terms regarding the privacy and security of the data (i.e. oaths of confidentiality, data-sharing agreements). Personal information is masked and security controls are in place (i.e. administrative, technical, or physical controls to protect privacy and confidentiality of information used).
- Quasi-public (semi-restricted): Data is released with some controls over access, such as requirement to register and/or agree to some restrictions or conditions for the release of data (e.g. terms-of-use agreements). Personal information is de-identified, and security controls are in place (i.e. administrative, technical, or physical controls to protect privacy and confidentiality of information used).
- Public (open data): Data is released to the public with minimal controls, conditions or limits over public access. Users may be requested to agree to terms under an open license. Personal information is fully de-identified.

APPENDIX D: Using Statistics Canada Data Sets for Benchmarking

The Ontario race categories in the Standards are compared to the appropriate Statistics Canada population group categories as follows:

Table 2. Conversion Table of Categories Collected

Ontario's Mandatory Race Categories	**Statistics Canada Population Group Categories**
Black	Black
East/Southeast Asian	Chinese Korean Japanese Southeast Asian Filipino
Indigenous	Aboriginal
Latino	Latin American
Middle Eastern	Arab West Asian
South Asian	South Asian
White	White
Another	Other

Statistics Canada's Immigration and Ethnocultural Diversity Highlight tables contain derived categories for multiple race responses. In order to benchmark appropriately, it is important to be aware of the methodology that Statistics Canada applies to individuals who select more than one population group; for example, someone who identifies as Black and White is classified only as Black, under the Visible Minority variable, and more generally as a "visible minority." Those who select multiple non-white backgrounds are classified as "multiple visible minorities," or "VM n.i.e."

Wherever feasible, PSOs should use public use microdata files which contain disaggregated multiple response data. Disaggregated data allows analysts and researchers to parse out the specific combinations of multiple 'visible minority' responses, and apply consistent methodology to the data used for benchmarking and analyses. The microdata are available only through Statistics Canada Research Data Centres or by subscription.

In using Statistics Canada population group as benchmarks, it is important to recognize differences in the way race is framed and categorized in Ontario's standard, compared to Statistics Canada's "population groups" (see Table 3).

Table 3. Comparisons between the Standards and Statistics Canada's approach

Differences	**Ontario's approach**	**Statistics Canada's approach**
Question framing	Names race as a social category used to describe individuals: "Which race category best describes you?"	May be interpreted as a fact, social identity, and/or a social category: "Are you….?"
Question logic	Allows all individuals to respond to the question	Only allows non-Indigenous individuals to respond to the question
Categories	• Individuals can self-report "Indigenous" as a race category, separate and distinct from the question about Indigenous identity group. • The treatment of multiple or mixed race responses is based on the specific analytic needs and context of the program area or sector.	• Individuals are identified as Indigenous based on their responses to a separate question about Aboriginal group (Q18) • Individuals with multiple or mixed race are included in categories based on specific rules established by Statistics Canada[2].

[2] See http://www12.statcan.gc.ca/census-recensement/2016/ref/guides/006/98-500-x2016006-eng.cfm

The objective of Ontario's approach is to capture race and racialization as experienced in Ontario for the purposes of identifying and monitoring systemic racism. This includes asking Indigenous peoples about the racial diversity that exists in their communities, in addition to their Indigenous identification. The 2016 Census results for Ontario show that about 80% of respondents with Indigenous (First Nations, Métis, and Inuit) ancestries also reported non-Indigenous origins.

APPENDIX E: Using Racial Disproportionality and Disparity Indices

Depending on the question you want to answer, either a disproportionality, or a disparity index may be more appropriate. For example, the desired equity outcome may be that individuals of specific racial groups should be represented in a given program or service at the same proportion as their presence in the wider population. In this case, the racial disproportionality index is appropriate to assess whether there might be an overrepresentation or underrepresentation of racial groups in a service, program or function.

A racial disproportionality index however, does not help answer questions about whether individuals served by a PSO are receiving equitable treatment or outcomes in a program, service, or function.

If the desired equity outcome is that individuals are receiving the same treatment or outcomes within a given program, service, or function, regardless of their race, then a racial disparity index is the appropriate measure to use to identify and track any potential racial inequalities.

In some contexts, both racial disproportionality and racial disparity indices may be used to evaluate different outcomes within a program or service, and to understand systemic racial barriers or inequalities.

For example, where racialized children are shown to be over-represented in the child welfare system using the racial disproportionality index, the racial disparity index may be used to identify whether there is equal access to supervised family visits for the children within the system.

Using disproportionality and disparity indices to identify racial inequalities

A disproportionality or disparity index of '1' indicates equal representation or parity in outcomes within a given program, service, or function, and any number over or under '1' represents an inequality.

For example, if children from Group A are 10% of the general population, but consist of 20% of the child welfare population, the disproportionality index is 2.0. This means that children from Group A are over-represented in the child welfare system, and are two times more likely to be in the child welfare system than their presence in the general population would predict.

Conversely, if students from Group A are 15% of the high school graduating class, but make up only 7% of those receiving diplomas that year, then the disproportionality index is 0.47. This means that students from Group A are under-represented among those graduating, and are about half as likely to complete high school, than would be expected given their presence in the graduating class.

Disparity indices may also be represented as rates. For example, if the homicide rate for Group A is 5 per 100,000 and the homicide rate for Group B is 1 per 100,000, the disparity indicator would be 5.0, meaning that the homicide rate for Group A is 5 times greater than the homicide rate for Group B.

Other kinds of analyses using disproportionality and disparity indices

The disproportionality and disparity equations can be readily adapted for intersectional analyses of race with other factors, such as Indigenous identity, ethnic origin, religion, or other socio-demographic categories.

For example, compare children of Group A from religion X with children of Group B from religion X; or males from Group A with males from Group B, and females from Group A with females from Group B.

Disproportionality and disparity matrices may be constructed to evaluate systemic trends in outcomes across different events in a program or system. The representation of a racial group, or disparities between groups, at a particular decision point in a system or program can be compared to their representation or disparities at a prior decision point.

Consider the example of outcomes in the child protection system presented earlier. Below is a chart showing how to construct a disproportionality matrix to analyse a specific pathway and outcomes for Group A. In the example chart below, Group A's percentage in the general population is P_A. The benchmark for comparison at each decision point is the percentage of Group A at a prior decision point.

Table 4. Racial Disproportionality Matrix - Example

Decision Point:	**% Group A** (at specific points)	**Disproportionality equation**
General Population	P_A	
1) Referral received	A_1	A_1 / P_A
2) Investigation	A_2	A_2 / A_1
3) Placed in protection services:	A_3	A_3 / A_2
i. Placed in protection services: Child remains at home	A_4	A_4 / A_3
ii. Placed in protection services: Short-term foster care	A_5	A_5 / A_3
iii. Placed in protection services: Kinship care	A_6	A_6 / A_3

Disparity matrices may also be constructed to analyse systemic trends in outcomes for different groups across various stages of a program, service, or function. Below is a chart to show how to construct a disparity matrix to compare Group A against Group B along a specific pathway and outcomes. The percentage of Group A and Group B in the general population is P_A and P_B, respectively.

Table 5. Racial Disparity Matrix - Example

Decision Points:	**% Group A** (at specific points)	**% Group B** (at specific points)	**Disparity equation**
General population	P_A	P_B	
1) Referral received	A_1	B_1	$A_1 / P_A \div B_1 / P_B$
2) Investigation	A_2	B_2	A_2 / B_2
3) Placed in protection services:	A_3	B_3	A_3 / B_3
i. Placed in protection services: Child remains at home	A_4	B_4	A_4 / B_4
ii. Placed in protection services: Short-term foster care	A_5	B_5	A_5 / B_5
iii. Placed in protection services: Kinship care	A_6	B_6	A_6 / B_6