Government of Ontario

Data Standards for the Identification and Monitoring of Systemic Racism

DRAFT

Anti-Racism Directorate

2-12-2018

CONTENTS

LIST OF TABLES

INTRODUCTION

Data collection enables evidence-based decision-making and public accountability to help create an inclusive and equitable society for all Ontarians.

LEGAL AUTHORITY

The Data Standards for the Identification and Monitoring of Systemic Racism (“Standards”) have been established under the authority of the *Anti-Racism Act, 2017* (“ARA”) and approved by the Lieutenant Governor in Council (LGIC).

The Standards set out requirements and guidance for the collection, use and management of information, including personal information, to identify and monitor systemic racism and racial disparities in public sector organizations (PSOs) in Ontario.

The Standards should be read in conjunction with the *Anti-Racism Act, 2017.*

PURPOSE

The Standards establish consistent data collection, use and management practices for public sector organizations in Ontario to identify and monitor systemic racial disparities for the purpose of eliminating systemic racism and advancing racial equity.

CONTEXT [TO COME]

- Understanding systemic racism within the context of colonialism
- Understanding Indigenous peoples’ unique experiences of systemic racism and colonialism, and how that impacts considerations around data collection, etc.

APPLICATION

The Standards apply to public sector organizations, as defined in the *Anti-Racism Act, 2017,* that have been required or authorized to collect personal information in relation to specific programs, services and functions in a regulation made under the ARA.

Public sector organizations that have been prescribed in regulation must comply with the specific standards.

Other public, not-for-profit, and private sector organizations may voluntarily adopt the Standards for the purpose of identifying, monitoring, and eliminating systemic racism and advancing racial equity in Ontario.

SCOPE

The Standards set out minimum requirements and/or guidance for each stage of the data life cycle – including planning and preparation, collection, management, analysis, reporting and use of personal information.

The Standards include the collection of personal information related to Indigenous identity, race, religion and ethnic origin. Other factors may be collected when relevant to understanding how systemic racism impacts Indigenous and racialized groups and/or to explaining potential racial inequalities.

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

PRINCIPLES

The following principles support the mandatory requirements and guide organizations to interpret and apply the Standards.

Principle 1: Privacy, Confidentiality, and Dignity

The privacy of individuals, and confidentiality of personal information are protected. The dignity of individuals, groups and communities are respected.

Principle 2: Organizational Commitments and Accountability

Organizations are committed to and accountable for employing the data standards to help eliminate systemic racism and advance racial equity.

Principle 3: Impartiality and Integrity

The application of the Standards is impartial and promotes public confidence in efforts to eliminate systemic racism and advance racial equity.

Principle 4: Quality Assurance

Continuous efforts are made to ensure the quality of the personal information that is collected, the robustness of analyses conducted, and the accuracy of findings reported.

Principle 5: Organizational Resources

Organizational resources are used in such a way as to fulfill the requirements of the data standards.

Principle 6: Transparency, Timeliness and Accessibility

The collection and reporting of information is conducted in a timely manner, accessible to the public, and is clear and transparent.

HOW TO USE THIS GUIDE

This document outlines requirements (“Standards”), as well as recommendations and exemplary practices (“Guidance”).

- Standards are minimum requirements that apply to public sector organizations that are regulated under the ARA.
- Rationales provide reasons for the standards.
- Guidance are recommended exemplary practices and/or considerations to help apply a given standard.

The Standards reflect considerations for the diverse functions, needs and operational realities of public sector organizations in Ontario. Organizations have the discretion to determine how to best comply with the Standards.

PERIODIC REVIEW

The Standards will be reviewed periodically through engagement with affected communities to ensure that they continue to fulfill the purpose set out under s. 6(1) of the *Anti-Racism Act,* 2017.

The Minister Responsible for Anti-Racism is responsible for overseeing the periodic review of the Standards.

OVERVIEW OF THE STANDARDS

This is a summary of how the data standard and guidance applies throughout the typical data life cycle:

1. Plan and Prepare

- Identify need and establish specific organizational objectives for data collection based on stakeholder and community input.
- Determine organizational priorities and resources, and conduct a privacy impact assessment.
- Develop and plan data collection procedures, and provide training.

2. Collect Personal Information

- Communicate the purpose and manner of data collection to clients and communities.
- Provide training and implement the collection of personal information.

3. Manage and Protect Personal Information

- Establish data governance, and plan and implement processes for quality assurance and protection of personal information.
- Maintain and promote secure systems and processes for the retention, storage, and disposal of personal information.

4. Analyse Data

- Identify meaningful policy, program or service delivery outcomes.
- Establish thresholds to identify notable racial inequalities.
- Calculate and interpret racial disproportionality and disparity statistics.

5. Public Disclosure of De-identified Data and Analysis

- De-identify data sets and analyses to make it accessible and publicly available, consistent with Open Government principles.
- Publicly report racial disproportionalities and disparities results.

6. Use Data and Analyses

- Use information to better understand and inform decisions to address racial inequalities and advance racial equity.
- Continue to monitor and evaluate progress and outcomes.
- Promote public education and engagement about anti-racism.

STANDARDS AND GUIDANCE

1. PLAN AND PREPARE

Assessing, Planning, and Preparing for Data Collection

Standard 1. Assess, Plan and Prepare for Data Collection

Public sector organizations assess its data collection objectives, priorities, and sufficiently plan and prepare for data collection to ensure it serves the purpose of the ARA and is informed by input from affected communities, stakeholders, and partners.

Guidance

Assess what personal information is needed for the purpose of the *Anti-Racism Act, 2017* to identifying and monitoring racial inequalities in outcomes in order to close gaps for people.

Prior to collecting personal information, organizations should consider the following (in general order of logical sequence):

Community input: Engage on an ongoing basis, with Indigenous and racialized communities, stakeholders, clients, and partners to understand their priorities, concerns, needs, and interests in data collection, analysis and use.

Organizational objectives: Identify clear organizational need and objectives for data collection in consideration of the interests and priorities of communities and the requirements of the ARA.

Collection priorities: Scan policies, practices, services, and/or programs to identify needs and prioritize where to track and monitor potential systemic racial inequalities. [See OHRC Count me in! Guide]

Organizations should look to what other personal information is already collected under the authority of other Acts and that may also be used for the purpose of identifying and monitoring systemic racial inequalities.

Privacy Assessment: Conduct a Privacy Impact Assessment (PIA) to identify privacy implications, risks and mitigation strategies. A useful resource is “Planning for Success: Privacy Impact Assessment Guide” developed by Information and Privacy Commissioner of Ontario. (https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf)

Resources and Training: Assess and/or review organizational resources, capacities and competencies needed to collect, use, and manage personal information. This includes reviewing existing processes, information technology and software capabilities. In most cases, training employees is necessary to ensure the proper implementation of the Standards.

Public Communication and Outreach: Communicate about the organization’s data collection objectives and plans to the public, affected communities, and/or clients.

Indigenous Interests in Data Governance

In the planning process, public sector organizations should take into account the interests of Indigenous communities and organizations in being able to exercise authority, control, and shared decision making over the collection, management and use of information about Indigenous people and communities.

Information sharing agreements between public sector organizations and Indigenous communities, representatives, and/or partners are recommended to realize Indigenous interests in data governance (i.e., ownership, control, access, and possession of information).

Information sharing agreements should be responsive to the needs and interests of Indigenous communities, and support implementation of Indigenous data governance principles.

2. COLLECTION OF PERSONAL INFORMATION

Manner of Collection

The *Anti-Racism Act,* section 7(3) requires that personal information is collected directly from the individual to whom the information relates, unless the data standards authorize another manner of collection.

<u>Standard 2. Direct Collection</u>

Direct collection includes the collection of personal information from an individual who is authorized at law to act on behalf of another individual. This could include family members or a legal guardian, an individual working under a power of attorney.

<u>Standard 3. Indirect Collection</u>

PSOs authorized to indirectly collect personal information about an individual to whom the information relates are permitted to do so in the following circumstances:

- The individual authorizes another person to provide his or her personal information
- The individual is deceased, and for whom there is no apparent trustee
- Where participant observer information (POI) about another individual's race is required under specific circumstances for a defined purpose that is consistent with the Act (for additional specific information, see Supplementary Section: POI Standard).

Notices and Obtaining Consent

Each individual has the right to give, refuse or withdraw their consent for the collection, use, and disclosure of their personal information. By posting or providing the appropriate notice(s) as set out below, public sector organizations meet the conditions necessary to obtain informed consent from individuals.

Section 6(8) of the ARA states that no program, service or benefit shall be withheld because a person does not provide, or refuses to provide, the personal information requested.

Notice to Individual - Direct Collection

The *Anti-Racism Act, 2017* (s. 7(4)) requires that when personal information is collected directly, the individual providing the information must be informed of the following:

- That the collection is authorized under the *Anti-Racism Act*, 2017
- The purpose for which the personal information is intended to be used
- 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.

Notice – Indirect Collection

The *Anti-Racism Act*, 2017 (s. 7(5)) requires that if personal information is collected indirectly, before collecting the information, a notice must be published on a website by the public sector organization which states the following

- That the collection is authorized or required under the *Anti-Racism Act*, 2017
- 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, and
- The title and contact information, including an email address, of an employee who can answer an individual's questions about the collection.

Notice - Personal Information Already Collected Under Another Act

If the personal information is already being collected under another Act, the *Anti-Racism Act* s.9(5) requires that public notice is provided on a website stating that the already collected personal information may now be used for the purposes of the ARA, and:

- The types of information that may be used and the circumstances it would be used

- That the personal information is being used for the purposes of eliminating systemic racial inequalities and advancing racial equity, and
- The title and contact information, including an email address, of an employee who can answer an individual's questions about the collection.

Standard 4. Notice -- Individual Authorizes Another to Provide Their Personal Information

Where an individual authorizes another individual to provide their personal information (indirect collection), PSOs provide the same notice directly to the authorized individual as would be provided under direct collection.

Rationale

Notice is an essential part of obtaining informed consent from the individual to collect their personal information to ensure that individuals understand the purpose and intended use of their personal information, and that providing personal information is voluntary.

Guidance

PSOs collect personal information on the basis of voluntary, informed consent and in a way that is inclusive, responsive to the individual's needs, and respects individual dignity.

Informed consent entails that individuals are informed that they may request to withdraw their consent or correct the personal information kept about them.

Wherever feasible, the organization should maintain a record that consent was provided or refused, and that includes the date when consent was given.

Notice to individuals may be provided verbally and/or written.

All notices provided should be:

- Concise, easily readable and accessible
- Given in plain language, and in a style that the audience can understand, and
- Available in alternative formats, and translations, as necessary.

Where the law distinguishes Indigenous people and requires the application of a distinct legal analysis and/or process, ensure that the client is informed of those distinct provisions.

Records used to collect personal information (such as forms or questionnaires) should, if separate from the notice, also state clearly that the data collection is optional, and that no services will be withheld as a result of the individual's refusal to provide the requested information.

At the time the information is collected, or a reasonable time thereafter, additional information is provided to individuals that they may request to access, correct or remove personal information that pertains to them, and provide clear instructions on how to do so.

How to Collect Personal Information

Standard 5. Data Collection Methods

PSOs use methods and processes to collect personal information that are accessible to individuals that will be providing their personal information.

Data collection methods and processes protect individual confidentiality and privacy, and respects individual dignity.

Rationale

Data collection methods must meet requirements under the *Accessibility for Ontarians with Disabilities Act* (AODA), French Language Services Act (FLSA), and applicable privacy requirements under the ARA, *Freedom of Information and Protection of Privacy Act* (FIPPA), *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), or any other act.

Guidance

Methods used to collect personal information could include online, paper or telephone surveys, registration forms, and verbal interviews. Where data is collected by an interview process, it is important that all employees are trained to collect personal information in a respectful, culturally safe way that ensures individual privacy and confidentiality, and is responsive to the needs of individuals and communities.

When to Collect Personal Information

Standard 6. Identifying an Appropriate Time to Collect Personal Information

PSOs collect personal information at the earliest appropriate time in an individual's interaction with a program, service or function, and the collection process is designed to:

- Respect the dignity of the individual from whom personal information is collected, and
- Minimize repeated requests for personal information.

Rationale

Personal information is collected at the earliest appropriate opportunity in an individual's interaction with a program, service or function to identify and monitor adverse racial impacts and inequitable outcomes.

Guidance

Wherever feasible and appropriate, personal information is best collected at registration or enrolment in a program, service, or function.

There may be circumstances in which direct collection from the individual at the earliest opportunity is overly invasive or may be an affront to an individual's dignity.

For example, accident victims at the scene of the accident or individuals being booked into a detention centre may be in crisis and as such it might not be an appropriate time to collect personal information. In such cases, the next available appropriate opportunity should be found to collect personal information.

In other instances, it may be necessary to gather this information at the earliest possible stage in order to ensure that relevant services and supports are provided, particularly in the case of Indigenous accused persons. Federal and Provincial Legislation, including the *Criminal Code of Canada, Youth Criminal Justice Act,* and *Child and Family Services Act* distinguish Indigenous people and require judges and various justice personnel to apply distinct principle, provisions, and processes.

Training is therefore essential that an Indigenous person have the opportunity to self-identify at the earliest possible stage in a manner that will inform the relevant justice personnel.

Collection of Personal Information about Indigenous Identity

Standard 7. Collecting Personal Information about Indigenous Identity

PSOs collect personal information about Indigenous identity (i.e., First Nations, Métis and/or 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 follows the question and data response values set out below, which are consistent with conventions established by Statistics Canada.

Table 1. Indigenous Identity Question and Categories

Question	**Do you identify as First Nations, Métis, and/or Inuit? If yes, select all that applies**	
Values *(valid code list)*	1. No 2. Yes, First Nations 3. Yes, Métis 4. Yes, Inuk/Inuit	Indicates whether a person identifies as First Nations (includes Status and non-Status Indians), Métis and/or Inuit.
Response rule	If yes, respondents may select multiple options – First Nations, Métis, and Inuit. Respondents may not select both no and yes.	

When Indigenous communities have requested, or where information sharing agreements are in place between PSOs and Indigenous communities and/or organizations, the question and response values about Indigenous identity may deviate from the above, so long as responses can be mapped to "First Nations," "Métis," and "Inuit."

Rationale

Personal information about Indigenous identity (First Nations, Métis, and/or Inuit) helps to identify and understand Indigenous peoples' unique experiences of systemic racism as a result of the history of colonialism and the impacts of inter-generational trauma. This contributes to the government's commitment to identify and eliminate anti-Indigenous racism in programs, services and functions.

Collecting personal information about Indigenous identity also helps to facilitate better and more consistent delivery of programs and services.

Guidance

Organizations should work with Indigenous communities and partners to help determine best practices for collecting personal information about Indigenous identity. If the community requests it, or as part of data sharing agreements, organizations may provide for Indigenous peoples to self-identify in more specific ways, such as asking to identify specific First Nations band or community as an additional question or level of response (e.g., open text or drop-down list options if an individual selects "First Nations," "Métis," or "Inuit").

It is important that the collection of personal information about Indigenous identity be done in a way that is culturally safe. Due to ongoing impacts and legacies of colonization, Indigenous people may be uncomfortable with identifying as Indigenous, and perceive questions about Indigenous identity as rooted in racism or perceive that the information will be used in a discriminatory way in the provision of services.

Ensuring that there is an easily understood explanation of why Indigenous identity questions are being asked is key, so that the benefits of doing so are clear, as well as asking the questions in a way that is safe for Indigenous people to identify.

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

How Indigenous self-identification data is collected can help support Indigenous cultural expression and self-determination. It is important that data collection processes respect Indigenous culture and nationhood, and capture the diversity of Indigenous people who access public services.

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 to meet the needs of Indigenous individuals and communities across the province. In front-line service settings, specific cultural information may be necessary to ensure culturally-appropriate services, including language of service, spiritual accommodations, and other required supports. For example, identifying 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 8. Race Question

PSOs collect personal information about race using the preamble and question set out below 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.’
>
> Question: “Which race category best describes you? Select all that apply.”

Rationale

The approach to ‘race’ reflected in this standard best serves the purpose of identifying and monitoring systemic racism because systemic racism is shaped by how society categorizes individuals into racial groups. Race is framed as a social construct rather than a matter of personal identity (i.e., as distinct from an individual’s ethnic or cultural identity).

Guidance

To identify and monitor systemic racism and racial barriers, it is important to ask about race as a social construct that is often imposed on people. Individuals and groups can be racialized by others in society in ways that affect their experiences and treatment.

Race as a social category is distinct from, but may overlap with, how people personally identify, which can be much more varied and complex. For the purposes of identifying and monitoring systemic barriers and disadvantages, it is important to focus on race as a social descriptor rather than personal identity, i.e., as a category that is used to describe an individual, whether or not an individual personally identifies with it.

The race question aligns with how researchers and organizations in other jurisdictions ask about race as a social construct.

Using race categories that measure and reflect how an individual is perceived helps to better identify Indigenous and racialized communities’ experiences and treatment in society.

Standard 9. Race Categories

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

Present the categories in alphabetical order but may be varied in cases where a different order might increase response rates, such as most to least frequent responses to reflect the demographic make-up of a geographic area or individuals accessing a program, service or function.

Table 2. Race Categories

	Race categories*	**Description/examples**
Values **(Valid code list)**	1. Black	African, Afro-Caribbean descent / African-Canadian
	2. East/Southeast Asian	Chinese, Korean, Japanese, Filipino, Vietnamese, Cambodian, Indonesian, and other Southeast Asian descent
	3. Indigenous (First Nations, Métis, Inuk/Inuit)	First Nations, Métis, and/or Inuit **
	4. Latino	Latin American or Hispanic descent
	5. Middle Eastern	Arab, Persian, or West Asian descent, e.g., Afghan, Egyptian, Iranian, Lebanese, Turkish, Kurdish, etc.
	6. South Asian	Indian Subcontinent 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; provide instruction -- do not report “mixed” or “biracial.”]
Response rules	Respondents may select all that applies. Survey forms and interviews may include the examples and/or descriptions provided above to help individuals select the appropriate responses.	

** Where participant observer information (POI) is collected, a separate standard for race categories applies (Supplementary Standard for Participant Observer Information).*

*** With regards to the Indigenous category, if description/examples are provided on the form, then need only be provided once.*

Rationale

The race categories reflect how people generally understand and use race as a social descriptor in Ontario. While these are considered commonly used categories, people may choose to describe their racial backgrounds differently, therefore an open text, or “Another race category” option is included.

Some people have more than one racial background, therefore allowing multiple selection enables more information to be collected, rather than a generic “Mixed” option.

Guidance

Racial categories are not based on science or biology but on differences that society has created (i.e., is “socially constructed”). Over time, race categories can function to produce and/or maintain unequal relations of power between social groups in society on the basis of perceived differences, often based on physical appearance.

It is a concept that is distinct from ethnic origin and religion. For example, “Jamaican” is an ethnic group with a common heritage, ancestry and historical experience, whereas “Black” is a racial category that includes people with diverse cultures and histories. Furthermore, some Ontarians with Jamaican ethnic or cultural origins may self-report their racial background as ‘White,’ ‘South Asian,’ or ‘East/Southeast Asian.’ Similarly, people may share the same or similar religion, but may have many different racial backgrounds, and vice versa.

Race categories can be used to identify and track the impacts of potential systemic racism, including how individuals from some groups may experience inequitable treatment or access to programs, services and functions.

Wherever possible, race categories are distinct from geographic regions. However, names of geographic regions are currently used to refer to groups of people perceived to be dominant in a particular region, such as “East/Southeast Asian,” “South Asian,” “Middle Eastern.”

Individuals described by some categories, such as “Black,” “East/Southeast Asian,” “South Asian” and “White” may have origins in different regions of the world.

Survey methodology research has shown that removing non-response options such as “don’t know” and “prefer not to answer” generally increases data quality and response rates to socio-demographic questions. The decision to include these options or not should consider whether the responses provide valid information that can be used in analyses.

In some contexts, “prefer not to answer” may be useful to identify if this is a valid response to being asked the question or if the service provider failed to ask the question in the first place. In all circumstances, it should be clear to all respondents that it is their choice to answer the question or not (i.e., voluntary).

Collection of Race-Related Personal Information

Standard 10. Collecting Personal Information about Religion

PSOs may collect personal information about religion but only if it is used to identify and monitor systemic racism and racial disparities in outcomes experienced in distinct ways by religious groups.

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.

The standard question and data response values (e.g., religious categories) align with Statistics Canada and OHRC.

Table 3. Religion Question and Categories

Religion	
Question	What is your religion and/or spiritual affiliation? Check 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 (please specify): __________
Response Rule	Respondents may select all that applies.

Rationale

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

Guidance

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

This refers to a way of thinking where people are put into categories, viewed negatively and/or treated badly based on apparent religious differences and negative stereotypes about religious communities.

Islamophobia and antisemitism includes racism, stereotypes, prejudice, fear or acts of hostility directed towards individuals based on religion, or the perception of being part of religious community, e.g., Muslims, followers of Islam, or people perceived to be Muslim (e.g., Sikhs, Hindus, people from Middle Eastern countries, etc.).

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, dress or comportment, etc.)
- linked to, or associated with, racial difference
- treated as fixed and unchanging (i.e., naturalized) and/or in ways that permanently define religious or ethnic groups as the "other" in Ontario

- ascribe characteristics and/or negative stereotypes as uniformly shared by all members of a faith tradition
- presumed to be the sole or primary determinant of a person’s thinking or behaviour.

Consider collecting personal information about religion where there have been human rights complaints and/or cases involving those grounds.

In addition to individual acts of intolerance and racial profiling, Islamophobia and antisemitism can lead to viewing and treating Muslims, Jewish people or people of other religions as a greater threat on an institutional, systemic and societal level.

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

Standard 11. Collecting Personal Information about Ethnic Origin

PSOs may collect personal information about ethnic origin but only if used to identify and monitor of systemic racism and racial disparities in outcomes experienced in distinct ways by ethnic groups.

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

The standard question and data response values (e.g., ethnic origin categories) follow conventions established by the government of Ontario.

Table 4. Ethnic Origin Question and Categories

Ethnic origin	
Question	What is your ethnic or cultural origin(s)? For example, Canadian, Chinese, East Indian, English, Italian, Filipino, Scottish, Irish, Ojibway, Mi'kmaq, Cree, 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 [and/or provide drop-down list of values reported in Ontario, 2016]
Response Rule	Respondents may select or write-in more than one ethnic origins

**Examples are provided in order of most commonly reported single ethnic origins in Ontario in the 2016 Census, and includes five examples of Indigenous origins, and one from each world region.*

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.

Guidance

Personal information about ethnic origin collected must be used for the purpose of identifying and monitoring systemic racism and advancing racial equity. Racism can take many forms and change over time. For example, an accent can be racialized and have nothing to do with skin colour. While different forms of racism can share common features, we recognize that each community is made up of individuals who may have unique experiences with racism.

Consider collecting ethnic origin where there have been human rights complaints and/or cases involving those grounds.

Individuals may also experience systemic barriers uniquely on the basis of religion or ethnic origin, regardless of their race. Collecting and analyzing this information can help to identify and evaluate the underlying issues more precisely.

Sequencing of Indigenous Identity and Race-related Questions

Standard 12. Sequencing of Indigenous Identity and Race-Related Questions

PSOs ask individuals to provide personal information about Indigenous identity, ethnic origin, and/or religion prior to race.

Rationale

The sequence of questions can help to improve response rates and the accuracy of race information provided. Individuals may more readily provide personal information about race after they have been given the opportunity to provide personal information about their Indigenous Identity, ethnic origin, and/or religion.

Research on survey methods have found that the order of questions affect how people respond. Prior questions provide a frame of reference that influences how respondents interpret and answer later questions.

When individuals are asked to provide information about more specific identities, such as Indigenous identity, ethnic origins, or religion prior to race, respondents are more likely to select a race category, and less likely to write in a unique response or refuse to answer.

Collecting Other Personal Information

Standard 13. Collecting Other Personal Information to Better Understand Systemic Racism

PSOs may not collect other personal information unless they are specified in regulations to assist in further understanding systemic racism and racial disparities in outcomes within a program, service or function.

The collection of other personal information should be the least intrusive necessary to fulfil the purposes of data collection, and may include the following types of personal information:

- Age
- Sex
- Education
- Geo-spatial information
- Socio-economic information
- Citizenship
- Immigration status
- Gender identity and gender expression
- Sexual orientation
- Place of birth
- Languages
- Marital status
- Family status
- (Dis)abilities

Rationale

Under s. 6(6) of the ARA, the Standards must specify the personal information that PSOs may be authorized or required to collect under a regulation.

The collection of other types of personal information are relevant for the purpose of analysis and identifying factors that shape different experiences (i.e., intersectional identities) as well as factors that potentially contribute to, reinforce, or underlie systemic racial inequalities in outcomes.

Guidance

Other personal information collected should be used in analyses to further understand and/or explain systemic racism and potential racial inequalities in outcomes.

For example, it may be necessary to understand if systemic racial barriers are different for men and women, and/or for different age groups. Individuals may experience multiple disadvantages that contribute to systemic barriers, such as disabilities, low income, language barriers, etc. The use of other personal information can help identify other factors that impact group outcomes.

Wherever possible and appropriate, the questions and categories used in the collection of other types of personal information should be consistent with Statistics Canada or other Data Standards developed by the government of Ontario.

3. PROTECTION AND MANAGEMENT OF PERSONAL INFORMATION

Data Governance and Accountability

Standard 14. Establish Organizational Roles and Responsibilities

PSOs clearly establish accountability mechanisms and rules, with organizational roles and responsibilities for all aspects of data collection, use, and management. There is at least one manager who is accountable for oversight and compliance with the ARA and the race data standards.

Rationale

Clear organizational roles and responsibilities help ensure that personal information is protected and used for the purpose set out in the *Anti-Racism Act*, 2017.

Guidance

PSOs should work with their records and information management (RIM) professionals to ensure that the creation, management and disposition of records containing personal information collected under the ARA is facilitated in accordance with the recordkeeping requirements in the *Archives and Recordkeeping Act 2006,* effected by the Corporate Policy on Recordkeeping.

Organizations should train all employees, officers, consultants and agents who need access to personal information in the performance of their duties on the requirements of the Act and the Standards to ensure their roles and responsibilities are clearly understood and carried out.

Indigenous interests in data governance

Indigenous data governance considerations vary between First Nations, Métis, and Inuit communities and organizations but there are common goals between these: an emphasis on the importance of engagement, transparency, and Indigenous communities having ownership and control over data about them, including how it is collected, managed, analysed, interpreted, and reported publicly.

Indigenous data governance principles aim to ensure that information that is gathered about Indigenous communities is used to empower communities with knowledge and tools to work towards positive community outcomes in areas they identify as important, such as health, education, economics, justice, and well-being.

The focus is on transparency in relationship building, proactive engagement, and strategic data governance partnerships with the government and/or other broader public service bodies, institutions, and agencies that collect information about Indigenous peoples to affect positive changes through data collection and analysis.

Communities affected by systemic racism may also have an interest in data governance principles, and may seek similar considerations of engagement, transparency, and access to information about their communities.

External Service Providers ("third party")

Standard 15. Third Party Service Providers Collecting on Behalf of PSOs

PSOs are accountable for all collection of personal information under the ARA by a third party on behalf of the institution.

Guidance

There should be agreements in place between the PSO and the third party to ensure compliance with privacy obligations in the *Anti-Racism Act* (ARA), and any other applicable legislation, including the *Freedom of Information and Protection of Privacy Act* (FIPPA), or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Agreements should require that third party staff collecting personal information be familiar with the privacy requirements of the ARA, other legislative obligations and the Standards relating to the collection, use and management of personal information, and the organization's privacy breach management and response protocols.

Protecting Personal Information

Sections 7(11) and (13) of the ARA require organizations to take reasonable measures to secure the collected personal information in its custody and control, and limits access on a need-to-know basis to only those who need it to fulfill their duties.

Standard 16. Protecting Personal Information

PSOs have in place practices to ensure that:

- Personal information is protected against theft, loss, unauthorized access, use, tampering, or disclosure.
- Records containing the personal information are protected against unauthorized copying, modification, or disposal.

Rationale

The protection of individual privacy and confidentiality of personal information necessary to maintain the integrity of personal information, and protect against its misuse.

Guidance

Personal information should be stored in a secure manner that strictly limits access to only as much personal information as is necessary for employees, officers, consultants and agents of the organization (i.e., "users") to fulfill their duties.

To the degree that the "direct identifiers" (e.g., name, street addresses, telephone numbers, etc.) are not required in the analysis of a program, service or function the identifying information should be removed and no longer retained by the PSO. For example, if there is no ongoing need to track or re-identify the individual who provided the information.

PSOs should review, develop, implement, and maintain a data security program with administrative, technical and physical safeguards to secure personal information. This should be done in consultation with the organization's privacy officer or FIPPA coordinator. The following are examples of recommended practises:

1. *Administrative Security*
   - All employees should understand the importance of data security and privacy breach protocols
   - Implement user account systems that require user authentication through strong passwords and different levels of access and administrative privileges
   - Actively monitor account activity, such as access and log-in attempts
   - Remove any information that directly identifies a specific individual and assigning a unique pseudonym or identification number to the record (i.e., masking) so that it can be linked back to personal information banks containing administrative records by a designated manager (see Appendix X for definitions of terms).
   - Provide sufficient training to all users to understand how to protect privacy and confidentiality, and their privacy obligations under the ARA, FIPPA, and/or MFIPPA
   - Require users to sign information security agreements and/or providing regular reminders (i.e., through an opening screen that users see when logging in about the conditions of access and use, privacy standards, and the applicable penalties for any unauthorized activities or misuse, etc.)

2. *Technical and physical security*
   - Take reasonable measures to protect the physical security of records, computers and other hardware, such as securing access to areas of buildings or server rooms where personal information is stored
   - Protect personal information stored on servers or mobile devices, such as laptops, data keys, and using firewalls and/or encryption of data
   - Optimize security of new hardware and software through security testing, applying accurate configurations, and regularly updating software updates and patches

When contracting third party service providers that will have access to personal information, or will be involved in the collection, use and disclosure of such information on behalf of government, the PSO should consult the Ontario *Guidelines for the Protection of Information When Contracting For Services (2008)*, which provides guidance regarding risk assessment, protection planning, procurement and auditing.

Data Entry, Storage and Quality Assurance

The *Anti-Racism Act, 2017* s. 7(12) requires that before using collected personal information, reasonable steps are taken to ensure that the information is accurate.

Standard 17. Data Entry and Storage

Personal information that is collected for the purposes of the ARA shall be maintained by the organization in a secure manner where access is restricted only to those individuals who require the information for the purposes of the ARA.

If the personal information is collected for both the ARA and another lawful purpose, then it shall be maintained in accordance with the privacy requirements of the legislation applicable to the organization e.g., FIPPA.

Personal information about Indigenous identity and race are entered and coded correctly and accurately into electronic records ("personal information banks") as specified below:

Table 5. Coding of Indigenous Identity Information

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 labeled as follows: - Non-Indigenous only - First Nations - Metis - Inuit
Field type and format	Field type is discrete, and format is numeric (1)
Code set **(Valid values)**	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 records for the same individual if collected from a number of sources.

Table 6. Coding of Race Information

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 labeled as follows: - Black - East/Southeast Asian - Indigenous - Latino - Middle Eastern - South Asian - White - Another Race NOTE: *may be collected as closed or open text option*
Field type and format	Field type is discrete, and format is numeric (1) Exception: If "Another racial category," is an open text, then the field type is qualitative and format is alphanumeric (25)
Code set **(Valid values)**	For numeric fields: 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 records for the same individual if collected from a number of sources.

**See Supplementary Section for separate data entry rules for participant observer information data (POI)*

Rationale

Entering personal information accurately and in a consistent manner ensures the quality of the data to be used.

Guidance

Being able to link personal information to administrative records enables the analysis of disparities in individual outcomes and long-term trends in order to identify potential systemic racial inequalities. Personal information not needed is masked (see Protecting Personal Information) until such time as it is required for analysis, and accessed only by those who need it to fulfill their duties under the ARA.

The development and implementation of a quality assurance plan is recommended to help ensure accuracy and security of personal information. The plan would set out the organization’s policies and practices and may include the following:

- Protocols for employees to identify and report data quality and security issues to an accountable manager in a timely manner
- Documented methods, processes, definitions and codebook, and/or protocols for information management, which includes security, retention, disposal, analyses and de-identification
- Systematic data quality assurance checks to establish and maintain data quality (i.e., accuracy, reliability, validity, consistency, timeliness, and completeness of personal information), such as verifying accuracy of data entry, output tables, and analyses
- Routine maintenance and update of database management systems used to store, retrieve, and manage data files

Internal audits and/or periodic independent reviews of data collection processes and quality assurance protocols are also recommended to identify compliance with established policies.

Access, Correction and Removal of Information

Nothing in the *Anti-Racism Act*, s. 7(17) or the Data Standards limits the right of an individual under any Act to access and correct personal information.

Standard 18. Access, Correction and Removal of Personal Information

PSOs have procedures in place to allow individuals to request access to the personal information held about them by the organization.

Every individual who is given access to their personal information is able to request correction or removal of the personal information held about them, where the individual believes there is an error or omission, or wishes to withdraw consent for the organization to continue to hold and use the personal information that was voluntarily collected (directly or indirectly).

Rationale

Being able to access, correct, and remove provided personal information held about individuals is an important aspect of informed consent and respecting individual dignity.

Guidance

The PSO should provide individuals access to their personal information, and an opportunity to correct their personal information by requiring individuals to make such requests in writing, and provide verification of their identity before a response to the request is provided. The individual may also make an oral request to correct the record.

If an individual consents to have a PSO collect, use or disclose personal information about the individual, the individual may withdraw the consent, whether the consent is express or implied, by providing a written request to the organization to remove the personal information.

The withdrawal of the consent does not require the organization to reconduct analyses or reports that may have used the personal information.

Individuals should be able to request that a statement of disagreement be attached to the information to reflect any correction or removal of personal information that was requested but not made.

Retention of Personal Information

The *Anti-Racism Act, 2017* s. 7(10) requires organizations to retain personal information for the period specified in the applicable data 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 19. 5-year Retention Period

Personal information is retained for at least five years after the day it was last used, and/or as long as reasonable and necessary for the purposes of identifying systemic racism and advancing racial equity, unless where applicable the individual requests earlier correction or removal of their personal information.

Rationale

Retaining personal information for at least 5 years enables the analysis of long-term trends and longitudinal analysis that requires individual-level data over time. It also enables the review and re-analysis of historical information based on issues that may arise over time.

Guidance

Public sector organizations named under ARA regulations may need to update their retention schedules to comply with the Standards.

Disposal of Personal Information

Standard 20. Secure Disposal

PSOs dispose of personal information maintained in records in accordance with any applicable legislation.

Where a public sector organization is subject to the Archives and Recordkeeping Act, the personal information kept in records is disposed of in accordance with records retention schedules, by transferring it to the Archives or by destroying it.

Where an organization is not subject to a legal requirement to destroy personal information, the organization takes all reasonable steps to ensure that personal information is securely destroyed in such a way that it cannot be reconstructed or retrieved.

A disposal record is maintained which sets out what personal information has been disposed, and the date of that disposal. This disposal record must not contain personal information.

Guidance

For the secure permanent disposal of personal information, the organization should implement a protocol and schedule for the systematic permanent destruction of data files as an essential part of secure data management, including maintaining a disposal record.

PSOs should work with a records and information management professional to create schedules for records series that contain personal information collected under the ARA, which will specify disposition requirements, including disposal or transfer to the Archives of Ontario, subject to the approval of the Archivist of Ontario.

As best practice, organizations not subject to any legal requirements to the destruction of personal information should follow the requirements of FIPPA regulation (O.Reg.459) *Disposal of Personal Information*. Organizations should ensure that all reasonable steps are taken to protect the security and confidentiality of personal information that is to be destroyed or transferred to the Archives, including protecting its security and confidentiality during its storage, transportation, handling and destruction.

Methods for the physical destruction of personal information should be appropriate to the level of sensitivity, and type of media in which it is stored, including using certified shredding services.

Limits on Disclosure

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

- The individual to whom the information relates consents to having it disclosed
- It is required by law
- It is for the purpose of two types of legal proceedings (the public sector organization is expected to be a party or a former employee/consultant/agent of the public sector organization is expected to be a witness)
- It is for research purposes, in accordance with s.8 of the ARA
- It is being disclosed to the Information and Privacy Commissioner.

Sections 7(15) and 7(16) allows exemptions to disclosure where if personal information has been collected for a lawful purpose in addition to the ARA purpose, the personal information is only disclosed in accordance with the privacy rules that apply to that information under another statute.

4. ANALYSES OF DATA COLLECTED

Units of Analyses

Standard 21. Primary Units of Analyses

The primary units of analyses are the disaggregated categories of Indigenous identity, race, and/or religion and/or ethnic origin wherever collected for this purpose.

Units of analyses may be aggregated only if doing so is to protect individual privacy, and does not minimize findings of racial inequalities.

Rationale

Although the personal information is collected about individuals, the purpose of the analysis is to assess and report progress on the outcomes of groups of individuals stratified by Indigenous identity, race, ethnic origin, religion, and other characteristics (for intersectional race analyses).

Guidance

The categories of Indigenous identity, race, religion, and/or ethnic origin are the focus of analyses. The disaggregated categories are a minimum requirement, and the standard does not prevent organizations from conducting additional analyses using aggregated categories such as “mixed or multiple race,” “racialized,” etc.

‘Mixed Race’ or Multiple Race Categories

Some people have more than one racial background. Analysis should be sensitive to commonalities and differences in experience and treatment among persons reporting multiple race categories, and to how racialization can operate in different ways.

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

In other circumstances, it may be necessary and appropriate to aggregate or construct socially meaningful mixed race category(ies), for example, a generic ‘mixed race’ category, or distinct multiple race categories where a generic “mixed race” category might obscure significant differences. Small numbers of individuals (i.e., where fewer than 15) who select multiple race categories may also be a rationale for aggregation for analytical purposes.

Intersectional Race Analysis

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

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

Analyses of Outcomes

Section 9 of the *Anti-Racism Act*, 2017 permits a public sector organization 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.

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, sex, health status, etc.) or tracking individual outcomes within a program, service or function, may use this information for the purpose of identifying and monitoring systemic racism and racial disparities.

Standard 22. Focus on Outcomes

Disproportionality and disparity analyses focus on individual outcomes within a program or service, and where possible, the final and/or long-term outcomes of programs, services and functions.

Rationale

Personal information lawfully collected under another statute can be used for the purposes of analyses under the ARA.

Personal information that is already collected as part of administrative functions are an important source of data on the outcomes of programs, services, or policies. Use of outcome data with Indigenous identity, race, and race-based data are necessary for the identification and monitoring of potential systemic racial inequalities in programs, services, or functions.

Analyses of outcomes helps to identify and monitor where systemic racial barriers and disparities might be occurring within a given program, service or function.

Guidance

Outcomes in a program or service that reflect an individuals’ access, experiences, or treatment in the program or service may have significant and/or cumulative impacts on individuals’ final program or service outcomes, and/or long-term outcomes.

Racial disproportionalities and/or 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 or service, such as:

- penalties, sanctions, or fines
- awards or privileges
- promotions and appointments
- access to appropriate treatments, services or programs

- quality of treatment or experiences

It may be helpful to map the pathway of individuals' (e.g., clients) 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 and racialized communities, partners and stakeholders to identify meaningful outcomes. 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 23. Racial Disproportionality and Disparity Indices

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

- A racial disproportionality index is a measure of overrepresentation or underrepresentation of a racial group in a program, service or function relative to their 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:

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

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 to compare the outcomes of different populations or groups in sectors such as child welfare, youth and adult justice (including policing, courts, and corrections), education, and health at different levels of government in Canada, U.S., and United Kingdom.

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

See Appendix B for further guidance on racial disproportionality and disparity analyses.

Benchmarks and Reference Groups

Standard 24. Appropriate Benchmarks

PSOs choose appropriate benchmark that reflect the eligible population to which the outcome is applicable and is useful for interpreting year-over-year trends.

Rationale

The appropriate benchmark population and reference group shapes the interpretation of analysis, and the identification of long-term trends.

Guidance

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

- administrative records that contain information for specific subsets of the population.
- Statistics Canada's data sets are important and commonly used sources for establishing benchmarks of population groups in Ontario (see Appendix C for further considerations when using Statistics Canada data sets for benchmarking).

For example, if you are examining police traffic stops, the number of drivers may be a more appropriate benchmark than the number of persons in a city or region, since not all such persons will be among the driving population. To compare disproportionalities or disparities in charges laid, the appropriate benchmark may be the population of arrested individuals.

Standard 25. Appropriate Reference Group

PSOs choose an appropriate reference group that allows for meaningful interpretation of patterns and trends that may be indicative of systemic racism, and where possible, 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

Consider how 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 "all other."

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.

It is recommended that organizations engage with Indigenous 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 of findings. This is done by:

1. comparing disproportionality or disparity results against a threshold,
2. examining pattern of results over time, and
3. (where feasible) conducting 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:

- Input from subject matter experts, stakeholders, and affected communities,
- Reference to existing research literatures, other sources of information, and/or
- comparisons against cross-sector and national findings.

Standard 26. Setting Thresholds to Identify Notable Differences

Thresholds are set 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 (i.e., different thresholds may not be set for different groups); and,
- focused on adverse impacts or disadvantageous outcomes that would require remedial action

Rationale

Determining an appropriate threshold helps the organization to interpret the meaning of the numerical results, and indicate whether the magnitude of the disproportionality and disparity indices represents a notable difference for further investigation, monitoring, and/or 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 developed based on an analysis of numerical information (i.e., using statistical methods) as well as advice from community partners, stakeholders, and subject matter experts, and/or 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 that have tangible impacts on a person's quality of life.
- Tests for statistical significance do not necessarily provide guidance on the interpretation of results as evidence of systemic inequalities.
    - For small groups, tests of significance may not indicate that significant differences exist in the sample used, even if they do exist in the population.
    - For large groups, tests of significance tend to indicate significant differences, even if very small.
- Interpret with caution analyses where the number of individuals in the underlying population is 25 or less. This is because the reliability of results are lower with smaller samples.

Using thresholds to interpret results

A disparity or disproportionality index greater or less than 1, however, does not necessarily indicate that group differences exist within a service, program or function. For example, a program may be designed to support a particular group, in which case you would expect to find an over-representation of that group in the program.

Focusing 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, an organization may set a threshold of 2.0 to indicate a notable racial disproportionality in high school drop-out rates within a specific program. If the organization 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.

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 analyses is one method used to identify other factors, such as socio-economic conditions, that may help explain differences in group outcomes.

For example, a notable difference is found for Group A when compared against Group B; but how much of this difference is due to higher proportions of recent immigrants among Group A? A multivariate analysis helps to parse out how immigration status or other factors affect outcomes independently of race, and to identify the unique effect of race on group differences.

Draw on other sources of information to help in the interpretation and understanding of findings. It is recommended for organizations to use multiple methods, such as qualitative information obtained through focus groups, individual interviews with clients, employees, and experts, program evaluations, research literatures, etc.

Organizations 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, internal and external stakeholders and partners.

5. PUBLIC DISCLOSURE AND REPORTING

De-identification of Personal Information

Standard 27. De-Identification for Public Disclosure of Data

Before PSOs publicly disclose any data set, it must be de-identified using a risk management approach to minimize the risk of identifying individuals and maximize the utility of the information about Indigenous identity, race, religion and/or ethnic origin.

Rationale

The ARA requires organizations to de-identify the data set prior to disclosure. This involves removing any personal 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.

“Personal information” is recorded information about an identifiable individual. De-identification protects the privacy of individuals because once de-identified, a data set no longer contains personal information. As such, the use or disclosure of the data set cannot violate the privacy of individuals.

Guidance

“De-identification” refers to the process of removing or transforming personal information in a record or data set so that there is a reasonable expectation that the information could not be used, either alone or with other information, to identify an individual.

In addition to individual privacy, de-identification could also include considerations of community privacy to prevent potentially sensitive information being linked to specific communities (i.e., First Nations communities or specific neighbourhoods). This may mean the removal of geographic information at the 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.

It is important to remember that de-identification is a means to make useful data available to the public in a way that also protects individual privacy, with considerations for community interests. As such, the goal is to minimize the risk to an acceptable level while still providing useable data.

Where possible, de-identification should be done in consultation with the organization’s privacy officer or FIPPA coordinator and legal counsel. The IPC’s “De-identification Guidelines for Structured Data” (June 2016), sets out a process and considerations to assess re-identification risks and release models.

Best practices in the de-identification process involves the following major steps to:

1. **Analyse the data, user needs, and data environment** to understand your data set and the context for disclosure, 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 is complex and results will differ for each data release.
3. **De-identifying data to minimize risk and maximize utility**: removing, masking or transforming variables so that identifiable information is removed to the extent necessary to reasonably protect individual privacy while providing useful data.

Classifying and treating variables for de-identification

Direct identifiers are personal information that can be used to uniquely identify an individual; for example names, street addresses, telephone or fax numbers, email addresses, fingerprints and voiceprints, full-face photographic images, iris scans, social insurance numbers, health card numbers, medical record or health plan numbers, bank account numbers, certificate/license numbers, vehicle identifiers and serial numbers, license plate numbers, Internet protocol (IP) addresses, any other unique identifying number, characteristic, or code.

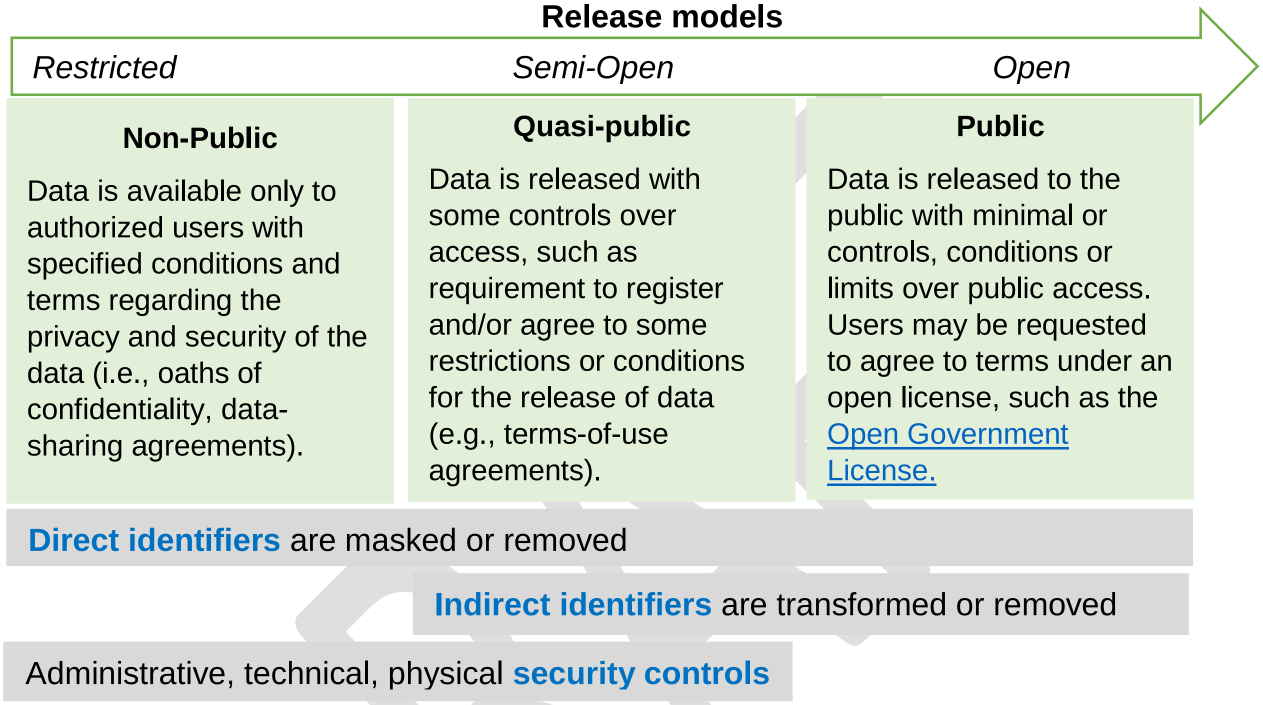
Masking is the removal of personal information classified as direct identifiers and/or replacement of direct identifiers with pseudonymous or encrypted information (i.e., unique identification key) to enable linking back to the original data set.

Indirect, or quasi-identifiers, are personal 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 (birth, marriage, etc.), income, education, language, etc. Classifying personal information that may be quasi-identifiers in your data set requires understanding what other information or data is public and/or readily 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 is contextual, meaning that what is considered de-identified data in one context may not be considered de-identified data in another context. For example, a data set with names, addresses, and telephone numbers removed (i.e., pseudonymous data), but account numbers are intact may be considered de-identified if it’s only accessible by authorized individuals who do not have access to clients’ account information. However, that same data set is not considered de-identified if it is used by employees who also have access to data sets that contain account numbers connected to clients’ names, addresses, and other personal information.

Types of de-identification and controls required under different release models

De-identification involves removing both direct identifiers, and indirect identifiers (or quasi-identifiers), and application of security controls. The degree to which personal information is de-identified depends on the release model chosen, based on an assessment of the risks of re-identification, and the public interest in access to data. Release models represent a spectrum of ways that data can be made available that range from restricted (non-public) to open (public) – see diagram below.



Release models

Restricted — *Semi-Open* — *Open*

Non-Public

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).

Quasi-public

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).

Public

Data is released to the public with minimal or controls, conditions or limits over public access. Users may be requested to agree to terms under an open license, such as the Open Government License.

Direct identifiers are masked or removed

Indirect identifiers are transformed or removed

Administrative, technical, physical **security controls**

Managing potential disclosure impacts

Good governance and management is an important part of releasing de-identified data. Organizations should develop and implement a plan to reduce and manage potential re-identification risks and impacts.

- Maintain a record of all the data released, including descriptions of release model, data types, and properties
- Regular and ongoing re-identification risk assessment of released data by examining against the disclosures of new and/or overlapping datasets
- Identify stakeholders, communities, and partners that could be impacted, and
- Establish and implement plans in the event of a privacy breach, including training of staff, and communicating with potential affected parties as soon as possible.

Standard 28. De-Identification of Results of Analyses

Results of analyses must be de-identified prior to public disclosure to minimize the risk of re-identification.

Rationale

The results of analyses may present re-identification risks under certain circumstances, such as where sample sizes are small, and/or there are unique cases with outcomes that are far from the other values in the sample (i.e., outliers).

Guidance

To minimize disclosure risks when presenting results, consider:

- Removing outlier cases from the sample prior to conducting analyses
- Restricting tables to two or three dimensions
- Suppressing results based on small cells sizes, and
- Be cautious when reporting results based on small samples.

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

Open Data

Standard 29. Open Data

De-identified data sets used in reported analyses are publicly disclosed in a manner that is consistent with the Open Data Directive; that is:

- Open by default and available to the public
- 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 at no charge to the user.

Data sets are released on or before the day that the organization’s public report is released.

The data set is publically released on the public sector organization’s website with metadata that contains the relevant key words: Anti-Racism Act, Indigenous identity, race, and/or where relevant, religion and/or ethnic origin.

Rationale

Open data helps to ensure transparency and public accountability in identifying and monitoring systemic racism and racial disparities in Ontario’s public sector organizations.

Guidance

Where possible, the public disclosure of data should be done in consultation with the organization's privacy officer or FIPPA coordinator, legal counsel, and parties of data sharing agreements (as applicable).

Where public sector organizations are subject to the Open Data Directive, they must comply by those rules and submit datasets to the Ontario Data Catalogue (see Open Data Guidebook for more information https://www.ontario.ca/document/open-data-guidebook-guide-open-data-directive-2015).

It is recommended that organizations use an open license, and consider including terms of agreement that the dataset is not used in a manner that contravenes the Anti-Racism Act and the Ontario Human Rights Code. The Open Government License is an example of an open license that public sector organizations can use.

A number of necessary steps are required before information can be converted into open and machine-readable data. This includes identifying and prioritizing data for release, assessing data quality, reviewing data for accuracy, legal, privacy and security implications, making data accessible and compliant with any French language requirements, and ensuring specific technical requirements are met (https://www.ontario.ca/page/sharing-government-data).

Organizations are encouraged to contact potentially affected communities regarding data sets that may include sensitive information about their communities. Information sharing agreements, where in place, may guide the use and public release of data.

Public Reporting

Standard 30. Public Reporting of Results

On a regular and timely basis, a report is developed and made publically available on the public sector organization's website, and that includes:

1. Results of analyses:
   - Descriptive statistics of all variables used in the analyses
   - Description of benchmarks and/or reference groups
   - The racial disproportionality and/or disparity indices
2. Thresholds set to identify notable differences
3. Information about data quality (i.e., accuracy, validity, completeness of data collected).

Rationale

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

Guidance

Descriptive statistics should include information about the data used in the report, such as the relevant information about the population in the dataset, including sample size. The report should also stipulate the period that the data covers.

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

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

Reporting on interpretations of results

Where possible, reports should include interpretations of results such that the focus is on any potential systemic factors, is based on evidence, and informed through community and stakeholder engagements.

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

Organizations should provide the appropriate context to avoid stigmatizing groups, and is 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 public sector organizations have used data. Care should be taken to clearly communicate about the purpose and uses of data collection, respond to inquiries from the public, and engage with affected communities.

Notifying the Minister Responsible for Anti-Racism

Standard 31. Notifying the Minister Responsible for Anti-Racism

Provide the Minister Responsible for Anti-Racism with notice of open data and public reporting of de-identified data and analyses upon disclosure, and that includes: metadata, date published, and location posted (URL link), and brief description of the program, service or function.

Rationale

Enables the Anti-Racism Directorate to track the data that is collected and reported under the authority of the ARA.

6. USES OF DATA AND ANALYSES

Supporting Evidence-based Decision-making and Organizational Change

According to sections 7(6) of the ARA, personal information collected may only be used for the purpose of eliminating systemic racism and advancing racial equity. However, as per section 7(7), this does not apply to personal information that is lawfully collected for another purpose.

Guidance

Data and analyses should be used to support and promote anti-racism culture change to meet organizational commitments and accountabilities to reduce systemic racism and advance racial equity.

It is recommended that organizations regularly review data 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 give considerations to the findings when making strategic and operational plans and decisions in planning cycles.

Ongoing Monitoring and Evaluation

Wherever possible, personal information collected under the ARA is used to monitor and evaluate the effectiveness of anti-racism initiatives in the organization.

Public Education and Engagement

Data and analyses should be used to contribute to public education and advance public discussions about how systemic racial inequalities impact the lives of individuals and the broader society.

Public engagement and education efforts help to increase public confidence government to intervene to mitigate and address systemic racial inequalities, and advance racial equity. This helps to build support to address systemic racism in Ontario.

SUPPLEMENTARY SECTION

STANDARDS FOR PARTICIPANT OBSERVER INFORMATION (POI)

This section sets out standards that are unique to the collection, management, analysis, reporting, and use of participant observer information (POI). The standards in the main portion of this document continue to apply, with the necessary modifications or exceptions as set out in this section.

Planning for the Collection of Participant Observer Information (POI)

Standard S1. Planning for the collection of POI

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

Rationale

The collection of participant observations of another person's race is a sensitive endeavor and due diligence is required in the planning stage to consider the public interest.

Guidance

In developing plans, organizations should consult with communities, stakeholders and partners to inform its assessments of the need for and implementation of POI collection. This can include public posting of notices of intention, conducting public meetings, inviting written submissions, and engaging with Indigenous and racialized communities and partners.

It is recommended that the Ontario Human Rights Commission (OHRC) reviews and assesses the quality of organization's proposed approach against the public interest.

Circumstances Permitting the Collection of POI

Standard S2. Circumstances in which collection of POI is permitted

The collection of POI is 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. Is a Police Services Board or an organization that has a plan as described in Standard S1 that has been reviewed by the OHRC [TBD], and

2. There is a discrete interaction between a service provider and an individual client or member of the public that leads to a decision that determines an outcome, and
3. The individual service provider 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, such as an individual’s receipt of benefits, penalties, or services, 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. This information enables the monitoring of a decision-maker or service provider’s perception of an individual’s race and any subsequent treatment or outcome for that individual.

Guidance

The Ontario Human Rights Commission 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.

The application of rules, informal practices or decision making criteria often involves the exercise of discretion on the part of the individual service provider or decision-maker.

The exercise of discretion in the application of rules and practices may draw on racial stereotypes and bias. Racial disproportionalities or disparities that may arise from discrete interactions with a single decision-maker or service provider in which their perceptions of race could directly and significantly impact individual outcomes, for example:

- A police officer’s decision to stop, arrest or detain individuals.
- A court judge’s bail decisions.
- 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 this leads to significant racially inequitable outcomes.

POI Race Question and Categories

Standard S3. Mandatory POI Race Question and Categories

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

Table 7. POI Race Question and Categories

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

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

Response rule: The service provider or decision-maker providing their best assessment of another individual’s race may only select one valid response. “Don’t know” and “Prefer not to answer” are not valid response options.

The question must be prefaced with instructions to respondents (i.e., decision-maker or service provider) that:

- they provide their best assessment of the individual honestly and in good faith, and
- the collection of this information is authorized or required under the *Anti-Racism Act*.

Validity of POI Information

Standard S4. Quality Assurance

PSOs take reasonable measures so that the collection of POI is done in good faith and accurately captures perceived race as much as possible.

Guidance

Quality assurance measures include accountability measures and appropriate training to individual service providers to provide the POI data in good faith.

The validity of POI should be assessed through the organization’s established data quality assurance procedures. This could include periodic audits or evaluations of POI 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.

Standard S5. Data Entry and Storage

POI is accurately entered, stored and managed in a secure manner and stored separately from administrative records that contain personal information that is collected directly (or collected indirectly from family/guardians or powers of attorney).

POI about another individual’s race are entered and coded correctly and accurately into electronic records as specified below:

Table 8. Coding POI Race Information

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)**	For 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 not provided

Guidance

POI may be stored in a database that can be linked to information about the outcomes of that interaction.

Access and Correction of POI

Standard S6. Access and Correction of POI

PSOs have procedures in place for individuals to whom the POI information pertains to request access to that, and if they disagree with the accuracy of that information, individuals may request that the nature of their disagreement be attached to the record.

PSOs do not allow requests for correction of POI from individuals to whom the POI pertains, nor from individuals providing the POI.

Rationale

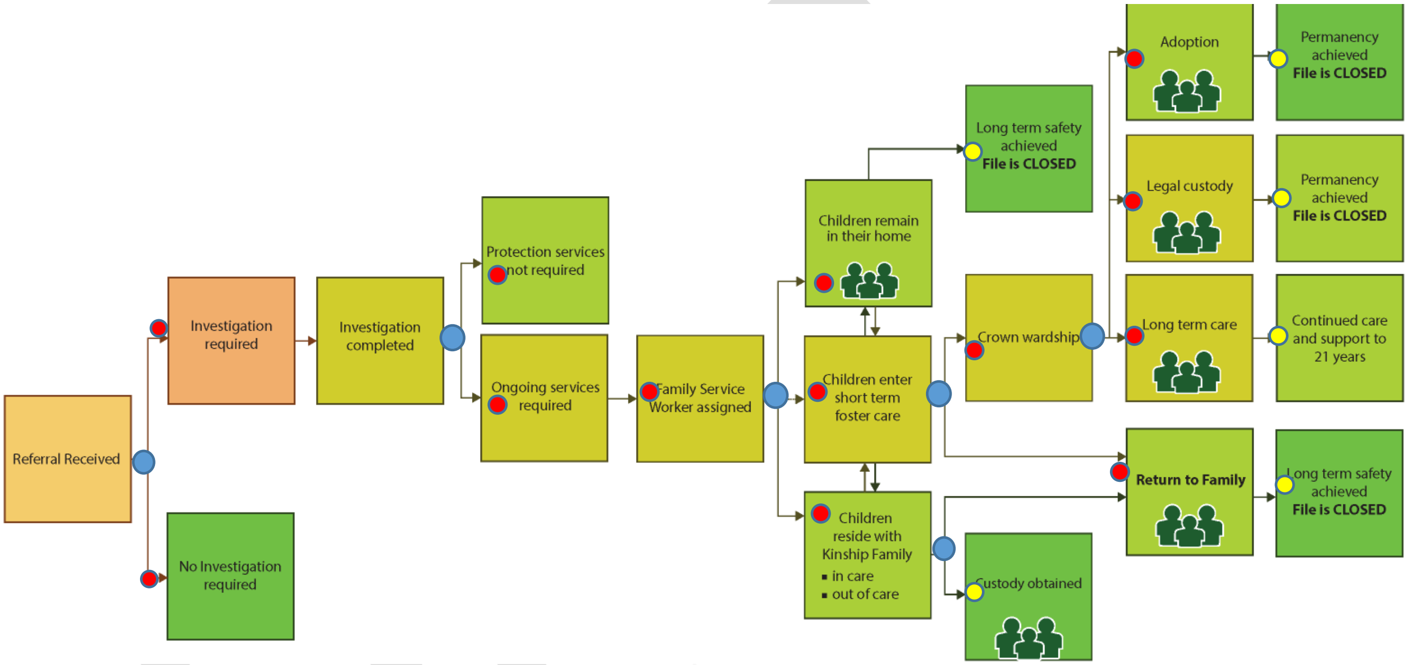
While POI relates to an individual, it reflects the perceptions of the service provider giving the information at the moment of collection. Neither the individual who provided the perception information nor the individual to whom the information relates may change or correct this information.

APPENDICES

APPENDIX A: EXAMPLE OF OUTCOMES IN CHILD PROTECTION SERVICES

Consider a typical pathway through the child protection system and outcomes as a result of decisions (indicated by blue dots● below).

To understand where potential systemic racial barriers or disadvantages may be occurring, it is necessary to track and monitor outcomes (● red dots), as well as the long-term or final outcomes (●yellow dots).


Referral Received
Investigation required
No Investigation required
Investigation completed
Protection services not required
Ongoing services required
Family Service Worker assigned
Children remain in their home
Children enter short term foster care
Children reside with Kinship Family
▪ in care
▪ out of care
Long term safety achieved
File is CLOSED
Crown wardship
Custody obtained
Adoption
Legal custody
Long term care
Return to Family
Permanency achieved
File is CLOSED
Permanency achieved
File is CLOSED
Continued care and support to 21 years
Long term safety achieved
File is CLOSED

Source: http://www.oacas.org/childrens-aid-child-protection/how-to-report-abuse/

APPENDIX B: 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 accessing a particular program, service are receiving equitable treatment or outcomes.

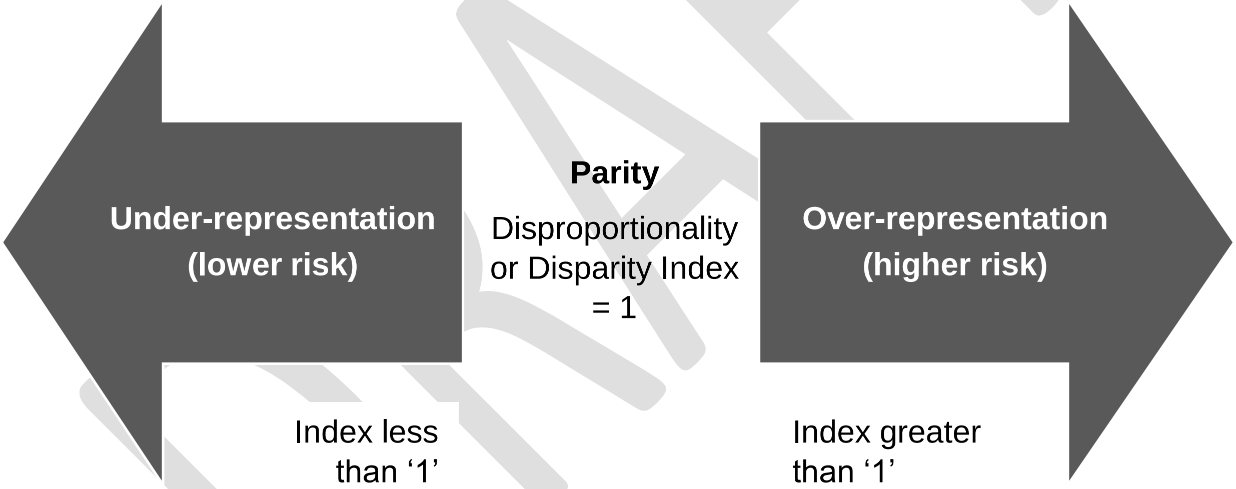
If the desired equity outcome is that individuals are receiving the same treatment or outcomes within a given program, service or function, regardless of their race, then a racial disparity index is the appropriate measure to use to identify and track any potential racial inequalities.

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’ represent an inequality.


Under-representation (lower risk)
Parity
Disproportionality or Disparity Index = 1
Over-representation (higher risk)
Index less than ‘1’
Index greater than ‘1’

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 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 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 9. 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. Child remains at home	A_4	A_4 / A_3
ii. Short-term foster care	A_5	A_5 / A_3
iii. 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 10. 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. Child remains at home	A_4	B_4	A_4 / B_4
ii. Short-term foster care	A_5	B_5	A_5 / B_5
iii. Kinship care	A_6	B_6	A_6 / B_6

APPENDIX C: USING STATISTICS CANADA DATA SETS FOR BENCHMARKING

The Ontario race categories are matched to the appropriate Statistics Canada population group categories as follows:

Table 11. Conversion Table for Statistics Canada Benchmarks

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

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 7).

Table 12. Comparisons between this data standard 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.	Individuals are identified as Indigenous based on their responses to a separate question about Aboriginal group (Q18)
	The treatment of multiple or mixed race responses is based on the specific analytic needs and context of the program area or sector.	Individuals with multiple or mixed race are included in categories based on specific rules established by Statistics Canada.

The objective of Ontario's approach is to capture the reality of 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 self-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.

Statistics Canada's Immigration and Ethnocultural Diversity Highlight tables contain only collapsed multiple race responses; 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."

Public use microdata files contain disaggregated multiple response data that allows researchers to parse out the specific combinations of multiple 'visible minority' responses. The microdata are available only through Statistics Canada Research Data Centres or by subscription.