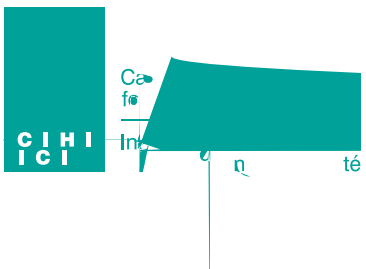

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Population Grouping Methodology Privacy Impact Assessment, June 2023*. Ottawa, ON: CIHI; 2023.

Cette publication est aussi disponible en français sous le titre *Méthodologie de regroupement de la population : évaluation des incidences sur la vie privée, juin 2023*.

Table of contents

Quick facts about the Population Grouping Methodology

1. The Population Grouping Methodology (POP Grouper), formerly referred to as population risk adjustment grouping or PRAG, was developed using the data and expertise of the Canadian Institute for Health Information (CIHI).
2. The key components of the POP Grouper are the population grouping methodology, the SAS software that applies the grouping methodology and related documentation.
3. The POP Grouper development project started April 1, 2013, and was completed December 15, 2016. Maintenance and enhancement of the POP Grouper is ongoing.
4. The grouping methodology and software are designed to
   - Assist CIHI and its clients with monitoring population health, predicting health care utilization patterns, surveilling and monitoring diseases, and explaining variations in health care resource use;
   - Provide a foundation for funding models;
   - Allow comparisons of inputs across jurisdictions; and
   - Provide clients with a comprehensive basis for standardizing populations when conducting interjurisdictional analyses.
5. The development of the POP Grouper was carried out using 3 years of data from Ontario, Alberta and British Columbia. These 3 jurisdictions were chosen because they have relatively complete coverage in a wide spectrum of CIHI data holdings that contain data at the person level.
6. Beyond the 3 years of foundation data from Ontario, Alberta and B.C., the POP Grouper also links and uses personal health information from more recent years and from other jurisdictions. Data comes from existing internal CIHI sources as it is acquired by CIHI, in accordance with CIHI's policies and procedures for data access and use.

1 Introduction

The Canadian Institute for Health Information (CIHI) collects and analyzes information on health and health care in Canada. Its mandate is to deliver comparable and actionable information to accelerate improvements in health care, health system performance and population health across the continuum of care. CIHI obtains data from hospitals and other health care facilities, long-term care homes, regional health authorities, medical practitioners and governments. This data includes information about health services provided to individuals, the health professionals who provide those services and the cost of the health services.

2 Background

2.1

The richness of CIHI's clinical data holdings provides opportunities for population grouping that are unavailable to most jurisdictions internationally. Data sources for the POP Grouper are selected, in part, by the coverage of person-level health data across Canada and the ability to link data over time and across health sectors.

The POP Grouper uses data from the following existing sources of CIHI data:

- Insured Persons Repository (IPR);
- Patient-Level Physician Billing (PLPB) Repository;
- Discharge Abstract Database (DAD);
- National Ambulatory Care Reporting System (NACRS);
- Ontario Mental Health Reporting System (OMHRS);
- Home Care Reporting System (HCRS);
- Continuing Care Reporting System (CCRS);
- Primary Health Care — Alliance Data (PHC-Alliance);
- Integrated interRAI Reporting System — Long-Term Care (IRRS-LTC);
- Integrated interRAI Reporting System — Home Care (IRRS-HC);
- National Prescription Drug Utilization Information System (NPDUIS);
- Canadian Patient Cost Database (CPCD); and
- Canadian MIS Database (CMDB).

Maintaining and enhancing the POP Grouper, providing aggregated results from the POP Grouper to support CIHI's public reporting (e.g., in Your Health System) and providing the general use data (GUD) files from the POP Grouper to support CIHI's internal analytical work all require that the above data be linked at the person level over time and across various health sectors.

The key deliverables for the POP Grouper are the grouping methodology, as well as SAS software that applies the grouping methodology and related documentation (i.e., a licensing agreement, SAS grouping software, a methodology report and a software user guide). The first version of the POP Grouper (v1.0) was released in December 2016; subsequent versions are released as the methodology is enhanced and other improvements are made. Further information on the POP Grouper is available on CIHI's Case mix web page.

2.2 Data collection

The POP Grouper does not collect data. All of the data used in the POP Grouper comes directly from existing internal CIHI sources: IPR, PLPB, DAD, NACRS, OMHRS, HCRS, CCRS, PHC-Alliance, IRRS-LTC, IRRS-HC, NPDUIS, CPCD and CMDB. A separate PIA has been conducted for each internal data source used by the POP Grouper; each one is available on CIHI's website.

2.3 Access management and data flow for the POP Grouper

From the internal data stored in a CIHI production database, a copy of each internal CIHI data holding required for the POP Grouper is uploaded to CIHI's SAS analytical environment, where it is made available to approved CIHI staf for CIHI purpo

3 Privacy analysis

3.1 Privacy and Security Risk Management Program

Privacy and security risk management is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur. CIHI has implemented its *Privacy and Security Risk Management Framework* and the associated *Policy on Privacy and Security Risk Management*. CIHI's chief privacy officer and general counsel and chief information security officer, in collaboration with senior managers, are responsible for identifying, assessing, treating, monitoring and reviewing privacy and security risks.

Privacy and security risks may be identified from a variety of sources, including PIAs. Once identified, risks are entered into the Privacy and Security Risk Register and categorized as **high**, **medium** or **low**, based on the likelihood and impact of a risk event:

- **High:** High probability of risk occurring, and/or controls and strategies are not reliable or effective;
- **Medium:** Medium probability of risk occurring, and/or controls and strategies are somewhat reliable or effective; or
- **Low:** Low probability of risk occurring, and/or reliable, effective controls and strategies exist.

The likelihood and impact of the identified risk are used to create a risk score. The risk assessment score of low, medium or high defines the seriousness of a risk. A higher risk ranking indicates a more serious threat and a greater imperative for treatment. Once an initial risk treatment is applied, the residual risk (the new calculation of the likelihood and impact of the risk, given the treatment) is assessed and compared against CIHI's privacy and security risk tolerance statement, which indicates that CIHI's privacy and security risk tolerance is low. If the risk score for the residual risk is still greater than low, additional risk treatment is necessary until the risk is low or the untreated/residual risk is accepted by CIHI's Executive Committee on behalf of the corporation.

There were no privacy and security risks identified as a result of this PIA.

3.2 Authorities governing POP Grouper data

General

CIHI adheres to its *Privacy Policy, 2010* and to any applicable privacy legislation and/or legal agreements.

Privacy legislation

CIHI is a secondary data collector of health information, specifically for the planning and management of the health system, including statistical analysis and reporting. Data providers are responsible for meeting the statutory requirements in their respective jurisdictions, where applicable, at the time the data is collected.

The following provinces and territories have enacted health information–specific privacy legislation: Newfoundland and Labrador, Prince Edward Island, Nova Scotia, New Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, the Yukon and the Northwest Territories. Health information–specific privacy legislation authorizes facilities to disclose personal health information without patient consent for the purposes of health system use, provided that certain requirements are met. For example, CIHI is recognized as a prescribed entity under the *Personal Health Information Protection Act* of Ontario, so health information custodians in Ontario may disclose personal health information to CIHI without patient consent pursuant to Section 29 as permitted by Section 45(1) of the act.

In provinces and territories that do not currently have health information–specific privacy legislation in place, facilities are governed by public-sector legislation. This legislation authorizes facilities to disclose personal information for statistical purposes, without an individual's consent.

Agreements

At CIHI, POP Grouper data is governed by CIHI's *Privacy Policy, 2010*, by legislation in the jurisdictions and by data-sharing agreements with the provinces and territories. The data-sharing agreements set out the purpose, use, disclosure, retention and disposal requirements of personal health information provided to CIHI, as well as any subsequent disclosures that may be permitted. The agreements also describe the legislative authority under which personal health information is disclosed to CIHI.

3.3 Principle 1: Accountability for personal health information

As noted previously, all of the data required for the POP Grouper comes directly from existing internal CIHI sources, specifically the IPR, PLPB, DAD, NACRS, OMHRS, HCRS, CCRS, PHC-Alliance, IRRS-LTC, IRRS-HC, NPDUIS, CPCD and CMDB. With the exception of the CMDB, which does not collect personal health information or other personal information, the internal data sources required for the POP Grouper include an encrypted HCN (replacing the original HCN), Indigenous-identifiable data, facility-assigned identifiers, personal attributes and identifiers, patient demographic and geographic attributes, and detailed clinical and related health information. For additional information about the data, please consult the PIAs for the internal data sources required for the POP Grouper (available on CIHI's website).

3.5 Principle 3: Consent for the collection, use or disclosure of personal health information

CIHI is a secondary collector of data and does not have direct contact with patients. CIHI relies on data providers to abide by and meet their data collection, use and disclosure rules and responsibilities, including those related to consent and notification, as outlined in jurisdiction-applicable laws, regulations and policies.

3.6 Principle 4: Limiting collection of personal health information

CIHI is committed to the principle of data minimization. Under sections 1 and 2 of CIHI's *Privacy Policy, 2010*, CIHI collects from data providers only the information that is reasonably required for health system uses, including statistical analysis and reporting, in support of the management, evaluation or monitoring of the health care system.

The POP Grouper does not collect personal health information; however, the internal CIHI data sources required for POP Grouper purposes do (except for the CMDB, as noted in Section 3.4). CIHI limits its collection of personal health information to that which is necessary to support authorized data quality and analytical activities. A PIA for each internal CIHI data source required for the POP Grouper is available on CIHI's website.

3.7 Principle 5: Limiting use, disclosure and retention of personal health information

Limiting use

Clients

CIHI limits the use of POP Grouper data to authorized purposes, as described in Section 3.4. These include comparative analyses within and among jurisdictions; trend analyses to assess and monitor the impact of differences in policy, practices and service delivery; and production of statistics to support planning, management and quality improvement.

CIHI staff

CIHI staff are permitted to access and use data on a need-to-know basis only, including for data processing and quality management, producing statistics and data files, and conducting analyses. All CIHI staff are required to sign a confidentiality agreement at the commencement of employment, and they are subsequently required to renew their commitment to privacy yearly.

Staff access to CIHI's secure analytical environment is provided through CIHI's centralized data access process. This environment is a separate, secure space for analytical data files, including GUD files, where staff are required to conduct and store the outputs from their analytical work.

The process ensures that all requests for access, including access to the POP Grouper data, are traceable and authorized, in compliance with Section 10 of CIHI's *Privacy Policy, 2010*. Access to CIHI's secure analytical environment is subject to an annual audit to ensure that staff are accessing data on a need-to-know basis. Section 3.9 includes additional information about how the various procedural and technical measures are deployed to prevent unauthorized access and otherwise secure the POP Grouper data.

Data linkage

Data linkages are performed between the POP Grouper data and other CIHI data sources. While this potentially causes greater risk of identification of an individual, CIHI undertakes mitigating steps to reduce the risks.

Sections 14 to 31 of CIHI's *Privacy Policy, 2010* govern linkage of records of personal health information. Pursuant to this policy, CIHI permits the linkage of personal health information under certain circumstances. Data linkage within a single data holding for CIHI's own purposes is generally permitted. Data linkage across data holdings for CIHI's own purposes and all third-party requests for data linkage are subject to an internal review and approval process. When carrying out data linkages, CIHI will generally do so using consistently encrypted HCNs. The linked data remains subject to the use and disclosure provisions in the *Privacy Policy, 2010*.

Criteria for approval of data linkages are set out in sections 23 and 24 of CIHI's *Privacy Policy, 2010*, as follows:

Section 23 The individuals whose personal health information is used for data linkage have consented to the data linkage; or

Section 24 All of the following criteria are met:

a. The purpose of the data linkage is consistent with CIHI's mandate;
b. The public benefits of the linkage significantly offset any risks to the privacy of individuals;
c. The results of the data linkage will not be used for any purpose that would be detrimental to the individuals that the personal health information concerns;
d. The data linkage is for a time-limited specific project and the linked data will be subsequently destroyed in a manner consistent with sections 28 and 29; or
e. The data linkage is for purposes of an approved CIHI ongoing program of work where the linked data will be retained for as long as necessary to meet the identified purposes and, when no longer required, will be destroyed in a manner consistent with sections 28 and 29; and
f. The data linkage has demonstrable savings over other alternatives or is the only practical alternative.

Client linkage standard

CIHI has implemented a corporate-wide client linkage standard to be used for the linkage of records created in 2010–2011 or later, where the records include the following data elements: encrypted HCN, and the province/territory issued the HCN. For the linkage of records that do not satisfy these criteria, the linkage mechanism is determined on a case-by-case basis.

Destruction of linked data

Section 28 of CIHI's *Privacy Policy, 2010* sets out the requirement that CIHI will destroy personal health information and de-identifed data in a secure manner, using destruction methodologies appropriate to the format, media or device such that reconstruction is not reasonably foreseeable.

Section 29 of CIHI's *Privacy Policy, 2010* further requires that for time-limited specifc projects, the secure destruction of linked data will occur within 1 year after publication of the resulting analysis, or 3 years after the linkage, whichever is sooner, in a manner consistent with CIHI's *Destruction Standard*. For linked data resulting from an ongoing program of work, secure destruction will occur when the linked data is no longer required to meet the identifed purposes, in a manner consistent with CIHI's *Destruction Standard*. These requirements apply to data linkages both for CIHI's own purposes and for third-party data requests.

In April 2013, CIHI's Privacy, Confdentiality and Security team approved data linkage for the development of the POP Grouper methodology as an ongoing program of work. Since then, the linkage approval has been renewed every fscal year. In February 2023, the linkage approval was expanded to include CIHI's use of aggregate results from the POP Grouper for the purpose of supporting CIHI's analytical work, including public reporting and preparing record-level GUD fles.

Return of own data

This is not applicable for the POP Grouper.

Limiting disclosure

Third-party data requests

Data required for the POP Grouper is not accessible through CIHI's third-party data request program.

Public release

As part of its mandate, CIHI publicly releases aggregated data only in a manner designed to minimize any risk of re-identifcation and residual disclosure. This generally requires a minimum of 5 observations per cell in accordance with Section 33 of CIHI's *Privacy Policy, 2010*. Aggregated data generated from the POP Grouper is made available during CIHI demonstrations of the grouping methodology (e.g., meetings, conferences) and on CIHI's website (e.g., in information sheets, Your Health System and statistical reports produced by CIHI staf).

Limiting retention

Data required for the POP Grouper forms part of CIHI's data holdings and, consistent with its mandate and core functions, CIHI retains such information for as long as necessary to meet the identifed purposes.

3.8 Principle 6: Accuracy of personal health information

CIHI has a comprehensive data quality program. Any known data quality issues will be addressed by the data provider or documented in data limitations documentation, which CIHI makes available to all users.

Similar to other CIHI data holdings, the POP Grouper is subject to a data quality assessment on a regular basis, based on *CIHI's Information Quality Framework*. The process of completing the framework includes numerous activities to assess the various dimensions of quality, including the accuracy of POP Grouper data.

3.9 Principle 7: Safeguards for personal health information

CIHI's Privacy and Security Framework

CIHI has developed a *Privacy and Security Framework* to provide a comprehensive approach to enterprise privacy and security management. Based on best practices from across the public, private and health sectors, the framework is designed to coordinate CIHI's privacy and security policies and to provide an integrated view of the organization's information management practices. Key aspects of CIHI's system security with respect to the POP Grouper data are highlighted below.

System security

CIHI recognizes that information is secure only if it is secure throughout its entire life cycle: creation and collection, access, retention and storage, use, disclosure and destruction. Accordingly, CIHI has a comprehensive suite of policies that specify the necessary controls for the protection of information in both physical and electronic formats, up to and including robust encryption and secure destruction. This suite of policies and the associated standards, guidelines and operating procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.

System control and audit logs are an integral component of CIHI's Information Security Program. CIHI's system control and audit logs are immutable. Analysis at CIHI is generally conducted with the use of de-identified record-level data, where the HCN has been removed or encrypted upon first receipt. In exceptional instances, staff will require access to original HCNs. CIHI's internal *Privacy Policy and Procedures, 2010* sets out strict controls to ensure that access is approved at the appropriate level and in the appropriate circumstances, and that the principle of data minimization is adhered to at all times. CIHI logs access to data as follows:

- Access to HCNs and patient names (rarely collected) within CIHI's operational production databases;
- Access to data files containing personal health information extracted from CIHI's operational production databases and made available to the internal analytical community on an exceptional basis; and
- Changes to permissions in access to operational production databases.

CIHI's employees are made aware of the importance of maintaining the confidentiality of personal health information and other sensitive information through the mandatory Privacy and Security Training Program and through ongoing communications about CIHI's privacy and security policies and procedures. Employees attempting to access a CIHI information system must confirm, prior to each logon attempt, their understanding that they may not access or use the computer system without CIHI's express prior authority or in excess of that authority.

CIHI is committed to safeguarding its information technology ecosystem, securing its data holdings and protecting information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. Audits are an important component of CIHI's overall Information Security Program; they are intended to ensure that best practices are being followed and to assess compliance with all information security policies, procedures and practices implemented by CIHI. Audits are used to assess, among other things, the technical compliance of information-processing systems with best practices and published architectural and security standards; CIHI's ability to safeguard its information and information-processing systems against threats and vulnerabilities; and the overall security posture of CIHI's technical infrastructure, including networks, servers, firewalls, software and applications.

An important component of CIHI's Audit Program is regular third-party vulnerability assessments and penetration tests of its infrastructure and selected applications. All recommendations resulting from third-party audits are tracked in the Corporate Action Plan Master Log of Recommendations, and action is taken accordingly.

3.10 Principle 8: Openness about the management of personal health information

CIHI makes information available about its privacy policies, data practices and programs relating to the management of personal health information. Specifically, CIHI's *Privacy and Security Framework* and *Privacy Policy, 2010* are available to the public on cihi.ca.

3.11 Principle 9: Individual access to, and amendment of, personal health information

Personal health information held by CIHI is not used by CIHI to make any administrative or personal decisions affecting individuals. Requests from individuals seeking access to their personal health information will be processed in accordance with sections 60 to 63 of CIHI's *Privacy Policy, 2010*.

3.12 Principle 10: Complaints about CIHI's handling of personal health information

As set out in sections 64 and 65 of CIHI's *Privacy Policy, 2010*, questions, concerns or complaints about CIHI's handling of information are investigated by the chief privacy officer and general counsel, who may direct an inquiry or complaint to the Information and Privacy Commissioner of the jurisdiction of the person making the inquiry or complaint.

4 Conclusion

CIHI's assessment of the POP Grouper did not identify any privacy or security risks.

This PIA will be updated or renewed in compliance with CIHI's *Privacy Impact Assessment Policy*.

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca