Policy Governing Data for Sponsored Research

Document 222042

1 – Context and purpose

This policy describes the principles governing the collection, handling, use, and retention of data that is required to conduct *sponsored research*.

Data is the lifeblood of actuarial science. Having access to high-quality, comprehensive data from a variety of sources is essential for the CIA to fulfill its research mission and its responsibilities to members.

This policy is designed to:

- Inspire confidence in *data contributors* that the collection, handling, use, retention, and where applicable, destruction of *contributed data* follows best practices and complies with applicable laws; and
- Ensure that *research providers*, *research assistants*, *peer reviewers*, and any other persons or entities with access to *contributed data* are aware of their responsibilities in this regard.

This policy should be read in conjunction with the CIA *Policy Governing Research*. Unless otherwise indicated, terms such as *sponsored research*, *contributed research*, *core research*, *exploratory research*, and *research providers* have the same meanings as in that document.

2 – Scope

2.1 – Data covered by this policy

This policy covers all non-public data that is or has been collected in connection with *sponsored research*, as well as any data that is derived from this data. It also covers data that the CIA acquires under a licensing or similar agreement and has permission to distribute to CIA members, *research providers*, *research assistants*, or *peer reviewers* for research purposes.

This policy does not apply to data that is in the public domain or data that a CIA member or some other person or entity who is not acting as a representative of the CIA collects or acquires in connection with *contributed research*.

2.2 – Entities to which this policy applies

This policy applies to all persons or entities engaged in the collection, handling, use, or retention of data that is required for *sponsored research*. This includes, but is not limited to, *research providers*, *research assistants*, and *peer reviewers*.

Research assistants are persons or entities that support or work under the supervision of

research providers.

Peer reviewers are persons or entities that review the work of *research providers* for reasonability and, as appropriate, accuracy. *Peer reviewers* will have sufficient knowledge and experience to conduct such a review but need not have the same level of expertise as the *research providers* conducting the research.

Peer review is particularly important for initiatives such as the construction of a new mortality or morbidity table where the results can have a significant impact on actuarial practice standards and/or financial reporting.

3 – Sources and types of data

3.1 – Data contributors

Data contributors means

- Insurance companies, banks, or other financial institutions or financial services providers,
- Pension plans, pension plan administrators, or pension services providers,
- Commercial or non-profit enterprises or organizations,
- Governments or government agencies,
- Educational institutions,
- Consulting firms,
- Entities representing or acting on behalf of one of these entities, or
- Any other entities,

that provide *contributed data* to the CIA or to *research providers.*

3.2 – Contributed data

Contributed data means non-public data that *data contributors* provide to the CIA or *researcher providers* for the purpose of conducting *sponsored research*. This includes but is not limited to:

- Demographic, descriptive, and/or experience data on current, prospective, or former policyholders, account holders, pension plan members, or the like;
- Data on reserves, capital, solvency, and/or funded status;
- Data related to proprietary investment or risk management strategies; and
- Survey response data.

3.3 – Licensed data

Licensed data means data that the CIA acquires with or without a subscription from a commercial enterprise, non-profit organization, government agency, or similar entity and has permission to distribute to CIA members, *research providers*, *research assistants*, or *peer reviewers* for research purposes.

4 – Collection of contributed data for core research

CIA Head Office staff are responsible for collecting *contributed data* for *core research* and managing all aspects of the data collection process. This includes, but is not limited to:

- Determining the data to collect for each *core research* project based on the input of an advisory group established by the Research Council (see section 11 of the CIA *Policy Governing Research*), best practices, and applicable laws;
- Creating templates for *data contributors* to submit this data to the CIA;
- Preparing and distributing *data requests* to potential *data contributors;*
- Responding to inquiries from *data contributors* regarding these *data requests;*
- Maintaining the infrastructure necessary for *data contributors* to submit *contributed data* to the CIA; and
- Ensuring that the data submitted to the CIA adheres to CIA requirements (see section 4.2 – Data submissions).

4.1 – Data requests

Data requests are formal requests to companies, organizations, administrators, agencies, governments, or related entities to provide non-public data in their possession to the CIA for the purpose of *core research*.

Data requests should clearly identify the data that is being requested, why it is being requested, how it will be used, and the potential benefits for *data contributors*. *Data requests* should also include information on how the data will be stored and policies with respect to data retention and destruction (see section 7 – Retention of contributed data for core research). *Data requests* should be accompanied by templates for submitting the requested data and detailed instructions for completing these templates and submitting the data.

Data requests must disclose if *contributed data* or data that is derived from it will be shared with *research providers* who reside outside of Canada, the rationale for retaining *research providers* who reside outside of Canada, and the names and employers of the *research providers* with whom the data will be shared in this case (see section 6.6 – Sharing of data).

4.2 – Data submissions

Data submitted to the CIA in response to *data requests* must be in electronic form and in the format specified.

Data submitted to the CIA must not contain any information that could uniquely identify an individual, a policy or certificate holder, a pension plan member, or similar entity. Such information includes, but is not limited to, an entity's name, social insurance or tax identification number, and full postal address. However, data submitted to the CIA may contain general geographic information on the entity such as the first three digits of their postal code or the area code (NPA) and exchange (NXX) of their telephone number.

Data submitted to the CIA will be checked before it is stored on CIA servers or made accessible to *research providers*, *research assistants*, or *peer reviewers* to ensure that it meets these requirements. Any *contributed data* that does not meet these requirements will be promptly destroyed and the *data contributors* will be asked to resubmit the data in the appropriate form.

5 – Handling of contributed data for core research

5.1 – Storage of contributed data

Contributed data that is provided to the CIA will be stored on a secure server with controlled access.

5.2 – Access to contributed data

5.2.1 – Persons or entities with access

Only CIA staff, *research providers*, *research assistants*, and *peer reviewers* with authorization will be permitted to access *contributed data* that is in the CIA's possession.

A designated CIA staff member will determine who should have access to *contributed data* in the CIA's possession and any limitations on that access. In determining who should have access to *contributed data* in the CIA's possession, the designated CIA staff member will be guided by and adhere to the provisions of this policy concerning the sharing of data (see section 6.6 – Sharing of data).

Prior to being granted access to *contributed data*, *research providers*, *research assistants*, and *peer reviewers* will be required to sign a confidentiality agreement governing access to this data.

5.2.2 – Limitations on access

Persons or entities with access to *contributed data* may only access that data to the extent required for *core research*.

Research providers with access to *contributed data* will only have access to the *contributed data* that is needed to conduct the *core research* for which they have been retained and only for the period of their engagement.

Research assistants with access to *contributed data* will only have access to the *contributed data* that is needed to conduct the *core research* for which the *research providers* have been retained and only for the period that they support or work under the supervision of the retained *research providers.*

Peer reviewers with access to *contributed data* will only have access to the *contributed data* that is needed to conduct their review and only for the duration of the review.

5.2.3 – Responsibilities of persons with access

Persons or entities with access to *contributed data* in the CIA's possession must adhere to the provisions of this policy, the CIA *Privacy Policy*, and all applicable laws governing the handling, use, and retention of data that is not in the public domain including, but not limited to, privacy laws.

Persons or entities with access to *contributed data* must take all necessary precautions to ensure that persons or entities without authorization do not gain access to this data or any data derived from it.

Files containing *contributed data* or data derived from it that are in the possession of *research providers, research assistants*, or *peer reviewers* must be password-protected and stored in a secure location (see section 6.7 – Copying of data).

5.2.4 – Access log

The CIA will maintain a log of the dates and times that *contributed data* is accessed and the login identifications of the persons or entities that accessed the data.

5.2.5 – Revocation of access privileges

Any person or entity that does not adhere to the provisions of this policy or any associated confidentiality agreement will have their access to *contributed data* revoked.

6 – Use of contributed data for core research

6.1 – Possible uses of contributed data

Contributed data may be used in many ways including, but not limited to:

- Identifying patterns;
- Making inferences;
- Building models;
- Estimating parameters;
- Testing hypotheses;
- Estimating prediction errors;
- Determining rate indications;
- Conducting experience studies; and
- Performing peer reviews.

Contributed data may also be used to compare current observations against previous ones and/or identify trends over time.

6.2 – CIA use of contributed data

Contributed data that the CIA collects for *core research* may only be used for *core research*.

Subject to the limitations stated in section 6.6 – Sharing of data, *contributed data* that the CIA collects for one *core research* project may be used for other *core research* projects.

6.3 – Research provider use of contributed data

Research providers with access to *contributed data* may only use this data to conduct the *core research* for which they have been retained and only for the duration of their engagement. They may not use this data for any other purpose.

Except as noted in section 6.6 – Sharing of data, *research providers* may not share *contributed data* to which they have access with any other persons or entities.

6.4 – Research assistant use of contributed data

Research assistants with access to *contributed data* may only use this data to conduct the *core research* for which the *research providers* have been retained and only for the period that they support or work under the supervision of the retained *research providers.* They may not use this data for any other purpose, nor may they share it with any other persons or entities.

6.5 – Peer reviewer use of contributed data

Peer reviewers with access to *contributed data* may only use this data to review the *core*

research work they have been assigned. They may not use this data for any other purpose, nor may they share it with any other persons or entities.

6.6 – Sharing of data

Contributed data submitted to the CIA, including data derived from it, may only be shared in the circumstances described in this policy.

Contributed data submitted to the CIA must be reviewed by CIA Head Office staff before it is shared to ensure that it does not contain any information that could uniquely identify an individual, a policy or certificate holder, a pension plan member, or similar entity (see section 4.2 – Data submissions). Any such information, and any information not required to conduct *core research,* must be removed from the *contributed data* before it is shared with *research providers*, *research assistants*, or *peer reviewers*.

6.6.1 – Research providers residing within Canada

The CIA may share *contributed data* that it collects for *core research* with *research providers* retained to conduct *core research* provided that:

- The *research providers* and any *research assistants* that support them or work under their supervision reside within Canada;
- The *contributed data* and any data derived from it remains in Canada;
- Access privileges are provided to the *research providers* and, as applicable, *research assistants*, in accordance with the provisions of section 5.2 – Access to contributed data; and
- The *research providers* and *research assistants* adhere to all the provisions of this policy, including provisions regarding access to *contributed data* (section 5.2 – Access to contributed data), use of *contributed data* (section 6.3 – Research provider use of contributed data and section 6.4 – Research assistant use of contributed data), copying of *contributed data* (section 6.7 – Copying of data), and retention of *contributed data* (section 7.2 – Retention of contributed data by research providers, research assistants, and peer reviewers), and any associated confidentiality agreements.

Submission of *contributed data* to the CIA implies consent to share this data or data derived from it with *research providers* retained to conduct *core research* under these conditions.

Research providers with access to *contributed data* may only share this data or data derived from it with persons or entities that are part of the research group that has been approved by the CIA to conduct the research for which the *research providers* have been retained, and they may only share the data that is needed to conduct this research. They may not share *contributed data* or data that is derived from it with any other persons or entities or for any other purpose. Persons or entities with whom the *contributed data* or data derived from it is shared must sign a confidentiality agreement before gaining access to the data, and they must adhere to all provisions of this policy.

6.6.2 – Research providers residing outside of Canada

The CIA may not share *contributed data* that it collects for *core research,* or any data derived from it, with *research providers* residing outside of Canada unless:

- The *data request* distributed to *data contributors* explicitly stated that the

contributed data or data derived from it would be shared with *research providers* residing outside of Canada;
- The *data request* explained why it was necessary to retain *research providers* residing outside of Canada; and
- The *data request* disclosed the names and employers of the *research providers* with whom the data would be shared.

If these conditions and the conditions stated in section 6.6.1 – Research providers residing within Canada (other than the residency requirement) are met, then *contributed data* submitted to the CIA in response to this *data request* may be shared with the *research providers* identified in the *data request*.

Research providers residing outside of Canada may not share *contributed data* or any data derived from it with any persons or entities that are not explicitly identified in the *data request*.

6.6.3 – Peer reviewers

The CIA may share *contributed data* that it collects for *core research* with *peer reviewers* residing within Canada provided that:

- The *contributed data* and any data derived from it remains in Canada;
- Access privileges are provided to the *peer reviewers* in accordance with the provisions of section 5.2 – Access to contributed data; and
- The *peer reviewers* adhere to all the provisions of this policy, including provisions regarding access to *contributed data* (section 5.2 – Access to contributed data), use of *contributed data* (section 6.5 – Peer reviewer use of contributed data), copying of *contributed data* (section 6.7 – Copying of data), and retention of *contributed data* (section 7.2 – Retention of contributed data by research providers, research assistants, and peer reviewers), and any associated confidentiality agreements.

The CIA may not share *contributed data* that it collects with *peer reviewers* residing outside of Canada.

6.7 – Copying of data

Research providers, *research assistants*, *peer reviewers*, and any other entities with access to *contributed data* may not make a physical or electronic copy of any *contributed data* or data derived from it on any storage device or mechanism that is not explicitly approved by the CIA. Such devices or mechanisms include, but are not limited to, Dropbox, 1Box, OneDrive for Home, or any other cloud filesharing or file syncing service.

Prior written approval is required before *contributed data* or data derived from it may be stored on a storage device or mechanism that is different from the one provided by the CIA.

Under no circumstances will *research providers* or other entities residing outside of Canada be permitted to store *contributed data* or data derived from it on a storage device or mechanism that is not provided by the CIA. *Research providers* residing outside of Canada will only have access to *contributed data* through systems provided by the CIA and all data derived from this data will remain within CIA systems.

7 – Retention of contributed data for core research

7.1 – Retention of contributed data by the CIA

Contributed data that the CIA collects for *core research* should be retained for future *core research* to facilitate consistency checks, investigate questions that arise from exploratory analysis of the *contributed data*, and compare results over time. CIA staff will determine which *contributed data* should be retained and for how long (see section 4.1 – Data requests).

Contributed data in the CIA's possession will be reviewed periodically to determine whether it is still needed for *core research*. *Contributed data* that is no longer needed for *core research* will be destroyed in accordance with best practices.

7.2 – Retention of contributed data by research providers, research assistants, and peer reviewers

Except as noted in section 7.3 – Retention of files required to support analysis, *research providers, research assistants*, and *peer reviewers* with access to *contributed data* or data derived from it must destroy all files in their possession that contain *contributed data* or data derived from it at the conclusion of their engagement with the CIA. This includes any hard-copy documents containing *contributed data* or data derived from it.

Files containing *contributed data* or data derived from it must be destroyed using commercially available software that precludes any possible retrieval or restoration of the files and is specifically designed for this purpose. Simply deleting the files from a hard drive is insufficient. Hard-copy documents must be shredded using a commercial-grade shredder.

7.3 – Retention of files required to support analysis

Files and/or hard copies containing information or calculations needed to support the analysis of the *research providers* may be retained by the lead researcher but only to the extent required to satisfy relevant professional practice standards. All other files and/or hard copies must be destroyed.

Files that are retained must be password-protected using a secure password and stored on a secure device or mechanism that has been approved in writing by the CIA (see section 6.7 – Copying of data). Hard copies that are retained must be kept in a secure location.

8 – Contributed data for exploratory research

Research providers retained to conduct *exploratory research* and any *research assistants* that support them or work under their supervision must adhere to the provisions of this policy, the CIA *Privacy Policy*, and all applicable laws governing the collection, handling, use, and retention of data that is not in the public domain including, but not limited to, privacy laws.

8.1 – Collection of data

Unless otherwise agreed with the CIA, *research providers* retained to conduct *exploratory research* are responsible for collecting any data that is needed to conduct their research.

Requests for non-public data that *research providers* circulate to potential *data contributors* should contain the following information at a minimum:

- A precise description of the data being requested;

- An explanation of why the data is being requested, how it will be used, where it will be stored, and how participation in the study will benefit the *data contributors;*
- Information on who will have access to the data and what measures will be taken to ensure that unauthorized persons or entities do not obtain access; and
- Information on whether any of the data will be retained when the research is completed, what measures will be taken to ensure that retained data remains secure, and when and how the retained data will ultimately be destroyed (see section 8.4 – Retention of data).

Requests for non-public data that *research providers* circulate to potential *data contributors* may mention that the research is funded by the CIA but must make clear that the *research providers* are neither employees nor representatives of the CIA.

Only the data required to conduct the research for which the *research providers* have been retained may be collected.

Data that is collected should not contain any information that could uniquely identify an individual, a policy or certificate holder, a pension plan member, or similar entity; examples of such information include an entity's name, social insurance or tax identification number, and full postal address. However, general geographic information such as the first three digits of an individual's postal code may be collected.

8.2 – Handling of data

Research providers and *research assistants* should follow best practices when handling non-public data that has been collected for *exploratory research*. These practices include, but are not limited to:

- Storing the data on a password-protected hard drive or secure server with controlled access;
- Limiting access to those persons or entities conducting or supporting the *exploratory research* for which the *research providers* have been retained;
- Ensuring that persons or entities with access are aware of their responsibilities and sign a confidentiality agreement;
- Maintaining a log of who has access to the data and when the data is accessed, by whom, and for what purpose; and
- Promptly revoking access privileges when a person or entity no longer requires access to the data or is in violation of any provision of this policy.

8.3 – Use of Data

Research providers and *research assistants* should follow best practices when using non-public data that they have collected for *exploratory research*. These practices include, but are not limited to:

- Only using the data to conduct the *exploratory research* for which the *research providers* have been retained, unless otherwise disclosed to the *data contributors* prior to collection of the data; and
- Not sharing the data with persons or entities that are not part of the research group that is responsible for conducting the *exploratory research* for which the *research providers* have been retained, unless otherwise disclosed to the *data contributors*

prior to collection of the data.

Research providers must share data they use to conduct the *exploratory research* for which they have been retained with *peer reviewers* that the CIA assigns to review their work.

Peer reviewers with access to this data may only use it to review the work of the *research providers* and may not share it with any other persons or entities. Prior to obtaining access to the data, *peer reviewers* will be required to sign a confidentiality agreement.

8.4 – Retention of Data

Research providers should follow best practices regarding the retention of non-public data. These practices include, but are not limited to:

- Retaining only the data and working files needed to support the analysis and satisfy relevant professional practice standards;
- Password-protecting any retained files and storing them in a secure location; and
- Destroying all other files, whether electronic or hard-copy, using commercial-grade software and/or hardware specifically designed for this purpose.

Except as required to satisfy relevant professional practice standards, *peer reviewers* must destroy any non-public data that *research providers* or *research assistants* provide them upon completion of their review.

9 – Handling and use of licensed data

Licensed data may only be distributed to CIA members, *research providers*, *research assistants*, and *peer reviewers* to the extent permitted by the license governing it and only used in accordance with this license.

Upon expiry of the license, access to this *licensed data* must be revoked and, if required by the license, any *licensed data* in the CIA's possession destroyed.

10 – Oversight

CIA staff will report to the CIA Board each year on the collection, handling, use, and retention of *contributed data* that was in the CIA's possession during the year.

Exemptions

n/a

Escalation Procedures/Management of Non-compliance with this Policy

The Research Council is responsible for interpreting this policy and handling any conflicts or issues of non-compliance.

Definitions and Abbreviations

n/a

Associated Documents
Policy Governing Research
CIA *Privacy Policy*

References
n/a

Monitoring, Evaluation, and Review	
Approval date	March 31, 2022
Effective date	April 1, 2022
Approval authority	Board
Review owner	Research Council
Prior review and revision dates	N/A
Review cycle	Three years
Next review date	2025