Information Sheet

Requesting CIHI Data? What You Need to Know About CIHI's Privacy Audit Program

February 2020

Third-party recipients of CIHI data may be audited

Before you receive data from CIHI, you must sign our Non-Disclosure/Confidentiality Agreement, which sets out the terms and conditions under which CIHI will provide data to data recipients. One of the terms of the agreement is CIHI's right to conduct a privacy audit, which may include CIHI visiting any of the organizations legally bound by the agreement.

CIHI privacy audits focus on compliance with the agreement

CIHI privacy audits evaluate your organization's use and management of CIHI data, as well as your disclosure of research findings associated with that data. The audit process is designed to verify that data recipients are adhering to the terms and conditions in the signed agreement.

What you can learn from past CIHI compliance audits

Generally, our privacy audits have confirmed that third-party data recipients consistently treat CIHI data as required by the terms of the agreement. That being said, our audits have resulted in recommendations for corrective measures. Before requesting or receiving CIHI data, and throughout your project's life cycle,

1. Ensure that your organization meets or exceeds the specified minimum requirements for
   - Data security;
   - Encryption; and
   - Secure destruction.

   Review and understand the security-related obligations of the agreement. Most of these are described in the Information Security Form and the Secure Destruction Information Package that CIHI will give you. Engage your information technology staff as soon as possible to ensure you're complying with the agreement. And if you have any questions about the minimum requirements, ask your CIHI contact before you receive any data.

How to cite this document:
Canadian Institute for Health Information. *Requesting CIHI Data? What You Need to Know About CIHI's Privacy Audit Program*. Ottawa, ON: CIHI; 2020.

CIHI

2. Ensure that all individuals/organizations that will receive, store, access or use CIHI data have signed the agreement and are aware of their obligations. You and your organization — as the recipient organization — are accountable for the confidential CIHI data and the actions of other authorized persons who use that data. Maintain a record of access to CIHI data and remove access once it is no longer required.
3. Address CIHI's minimum requirements for publication of results and acknowledgments. The agreement lists our explicit requirements for reporting small cell sizes and facility-identifiable data, as well as language to be used when referencing CIHI data in your published work.

When projects involve multiple organizations, and even different departments within the same organization, there can be inconsistent and inappropriate data management practices. Developing data management procedures and plans, including checklists that cover the use of CIHI data, can reduce the risk. These procedures/plans are also valuable training resources for new project staff.

4. Implement processes to ensure that contract obligations are not affected in situations where there are role changes within the project team or team members are transitioning on or off the project.
5. Notify CIHI **before**
   - Transferring CIHI data to a new physical location or transmitting CIHI data under any circumstance not already described in the agreement (including the Information Security Form);
   - Adding new staff or organizations to your project that require access to CIHI data (i.e., anyone not already identified in the agreement); and
   - Changing the relationship between the principal individual/lead researcher and the recipient organization, making organizational changes (e.g., involving acquisitions or mergers) or transferring the research project (and data) to a different organization.

   You must also notify CIHI **immediately** if you discover that any person has breached, or may have breached, any term or condition of the agreement.

What will happen if you are selected for an audit

CIHI will formally notify you and your organization, in writing, that it intends to conduct an audit. We will outline the purpose and scope of the audit, as well as the process we'll follow. Audits may include extensive documentation reviews, interviews and a site visit. At the end of the process, we'll provide a report that identifies non-conformities and opportunities for improvement, as well as corrective measures where required.

Questions?

Your primary contact for any questions is the CIHI staff person who is assisting with your data request. Specific questions about CIHI's Privacy Audit Program can be directed to privacy@cihi.ca. You can visit cihi.ca to learn about accessing CIHI data and reports, or to make a data request.