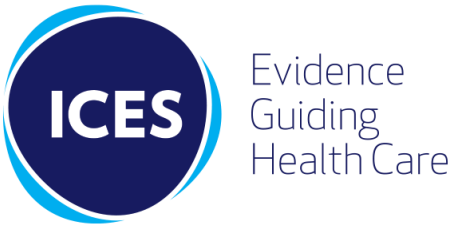


ICES Report

2014 Prescribed Entity Review

Institute for Clinical Evaluative Sciences
G1 06, 2075 Bayview Avenue
Toronto, Ontario M4N 3M5
www.ices.on.ca

Table of Contents

`

A. Introduction & Explanatory Note

This report has been prepared by the Institute for Clinical Evaluative Sciences (ICES) to support its request for continued approval of the Information and Privacy Commissioner of Ontario (IPC) under section 45(3) of Ontario's *Personal Health Information Protection Act* (PHIPA).

Our report demonstrates ICES' policies, procedures and practices to protect the privacy of individuals whose personal health information ICES collects under section 45(1) PHIPA. It does so from three perspectives. Section B details the existence and sufficiency of the documentation required by Appendices "A" and "B" of the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* (IPC Manual). This is followed, in Section C of our report, by an assessment of the effectiveness of those policies, procedures and practices according to the indicators defined in Appendix "C" of the IPC Manual. Finally, we affirm the accuracy and completeness of this information through the affidavit of ICES' Chief Executive Officer.

Our report shows that this has been a time of significant, positive change at ICES. Almost every policy and procedure reported is new or substantially improved since the time of our last report. For this reason, in certain areas work remains ongoing at the time of filing this report. ICES' Chief Privacy Officer has been charged with overseeing the completion of this important work, which is projected in all but one area by the end of 2014.

Prepared by Laura W. Davison and Kelley A. Ross.

B. Required Documentation

Part 1 – Privacy Documentation

1. Privacy Policy in Respect of its Status as a Prescribed Person or Prescribed Entity

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
	b. Privacy Information, Inquiries & Complaints Policy	Implemented
	c. Privacy Impact Assessment Policy	Implemented
	d. ICES PIA – New ICES Data Holding	Implemented
	e. ICES Project PIA Form	Approved
	f. Website privacy information	Implemented
Comments	Implementation of the new ICES Project PIA Form and an ICES data retention schedule is projected by December 31, 2014. In the meantime, a substantially similar version of the ICES Project PIA Form is in effect.	

DESCRIPTION

ICES' Privacy Policy establishes an overarching framework for ICES' collection, use and disclosure of personal health information, and ICES' approach to its protection.

Status under the Act

ICES Privacy Policy describes ICES' status as a prescribed entity under s. 45 of PHIPA. The policy declares ICES' commitment to protect personal health information in accordance with PHIPA and its regulation. In addition, the policy confirms that ICES implements the required privacy and security policies and procedures and that these are subject to review and approval by the Information and Privacy Commissioner of Ontario every three years. The policy also acknowledges ICES' responsibility for the handling of personal health information by its agents, and requires ICES to provide training to agents to enable their compliance.

Privacy & Security Accountability Framework

ICES' Privacy Policy articulates an accountability framework for ensuring compliance with the privacy and security policies and procedures ICES implements to maintain its designation as a prescribed entity. Under the framework, ICES' Chief Executive Officer:

- Has ultimate responsibility for ensuring compliance with PHIPA and its regulation and ICES' privacy and security policies and procedures as a prescribed entity;
- Must appoint a Chief Privacy Officer and a Senior Director, Data Platform, and delegate to them authority for day-to-day management of, respectively, privacy and security at ICES, including responsibility for putting in place policies and procedures to prevent, detect and respond to privacy and security breaches; and
- Is required to make an annual report of privacy breaches and complaints as well as privacy audits and privacy impact assessments to the Finance, Audit and Risk Committee of ICES' Board of Directors.

Collection of Personal Health Information

ICES' Privacy Policy identifies the purposes for which personal health information is collected, the types of personal health information collected and its sources. The policy also articulates ICES' commitment to ensuring collection is in accordance with PHIPA and its regulation, and limited to that which is reasonably necessary to, and avoided where other information will, serve the purpose. ICES' Privacy Impact Assessment Policy, which is referenced in the Privacy Policy, stipulates that a privacy impact assessment must be conducted by an ICES Privacy Officer prior to collection. Assessment of the amount and type of personal health information collected, which must be justified, is specifically provided for in templates used to conduct privacy impact assessments under that policy. The Privacy Policy requires the Chief Privacy Officer to ensure publication of a list of ICES data holdings on ICES' public website, together with a mechanism to allow individuals to request more detailed information. The list of specific ICES' data holdings is both very long and very dynamic, and for this reason the list itself does not form part of ICES' Privacy Policy.

Use of Personal Health Information

ICES' Privacy Policy identifies the purposes for which personal health information is used. Personal health information may be used for the purposes of health system analysis and evaluation and research conducted within ICES, and preparing information for disclosure to external researchers. In all cases, use must be in accordance with PHIPA and its regulation and, where applicable, research ethics board approvals. The policy clearly provides that

agents who conduct health system evaluation and research within ICES are permitted to use "coded" information only. Coded information is personal health information from which direct personal identifiers, such as names and health card numbers, have been either removed or replaced by a confidential ICES identifier or "code". The policy also stipulates that requests to use such information are subject to a privacy impact assessment conducted by an ICES Privacy Officer. The template developed for this purpose under ICES' Privacy Impact Assessment Policy is specifically designed to limit the information made available for these purposes to what is reasonably necessary and in the least sensitive form required. In contrast, the information prepared for use by external researchers must be de-identified prior to disclosure.

Disclosure of Personal Health Information

ICES' Privacy Policy limits disclosure of personal health information to disclosures to other prescribed entities and prescribed registries. Disclosures are made only as permitted by PHIPA and section 18(4) of its regulation and data sharing agreements, and verified through a privacy impact assessment. Conducted by ICES Privacy Officers, privacy impact assessments are designed to ensure that ICES discloses personal health information only where other information will not serve the purpose and discloses no more personal health information than is reasonably necessary. Disclosure of personal health information is not permitted in any other scenario. Instead, the policy permits disclosure of de-identified information only to external researchers and knowledge users and in publications. In each case, permission to disclose is subject to a determination the information presents a low risk of re-identification

Secure Retention, Transfer & Disposal of Records of Personal Health Information

ICES' Privacy Policy addresses the secure retention, transfer and disposal of personal health information in both paper and electronic format. Personal health information with direct personal identifiers is retained only temporarily. It is isolated in secure network folders and cabinets until data quality issues have been resolved and is then securely destroyed by an ICES-approved method such as cross-cut shredding for paper or secure wiping or physical destruction for media and devices. ICES also protects personal health information in transit. Protections include an encrypted file transfer system that is used for inbound and outbound electronic file transfers, and a requirement to remove direct personal identifiers before transferring paper.

Implementation of Administrative, Technical & Physical Safeguards

ICES' Privacy Policy outlines some of the administrative, technical and physical safeguards ICES implements to protect personal health information against theft, loss and authorized use and disclosure. The safeguards outlined include restrictions on access that protect personal health information against unauthorized copying, modification or disposal: agents who conduct health system and analysis and evaluation or health-related research are permitted to access coded information, and external researchers are permitted to access de-identified information, only.

Inquiries, Concerns & Complaints Related to Information Practices

ICES' Privacy Policy requires ICES to establish processes to allow individuals to make inquiries and complaints about ICES' privacy policies, procedures and practices as a prescribed entity and comply with PHIPA and its regulation. The Chief Privacy Officer is responsible for establishing and implementing procedures for the receipt and handling of privacy inquiries and complaints by ICES Privacy Officers. The Chief Privacy Officer is also required to ensure instructions, including contact information, are published on ICES' public website. The information published on ICES' public website must include instructions that inquiries, concerns and complaints about ICES' privacy practices may be addressed to the Chief Privacy Officer directly, both verbally and in writing, and a mailing address and other contact information to enable this. The website must also include a statement that individuals may direct complaints regarding ICES' compliance with its obligations as a prescribed entity to the Information and Privacy Commissioner of Ontario, and associated mailing address and contact information.

Transparency of Practices in Respect of Personal Health Information

ICES' Privacy Policy requires ICES to publish information about its privacy practices on its website and establish processes to allow individuals to obtain further information about its privacy policies, procedures and practices as a prescribed entity. ICES' Chief Privacy Officer is responsible for fulfillment of both requirements, which are also elaborated, under ICES' Privacy Information, Inquiries and Complaints Policy.

2. Policy & Procedures for Ongoing Review of Privacy Policies, Procedures & Practices

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Audit & Monitoring Policy	Implemented
	b. Privacy Monitoring Log & Report Forms Workbook	Implemented
	c. Policy Framework & Governance Policy	Implemented
	d. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Privacy Audit and Monitoring Policy provides for continuous monitoring of ICES' privacy policies and procedures. The purpose of monitoring is to detect when existing policies or procedures require amendment and when new policies and procedures are required to meet ICES' obligations as a prescribed entity.

The Chief Privacy Officer is responsible for putting in place a monitoring program to identify and address the implications of the following as they occur:

- Relevant regulatory changes and guidance, including any orders, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario under PHIPA and its regulation;
- Changes to relevant industry standards;
- Risks identified through privacy impact assessments;
- Deficiencies identified through audits;
- Inconsistencies between and among privacy and security policies, procedures and practices and between them and ICES' actual practices; and
- Investigations into privacy incidents and breaches and complaints about ICES' privacy practices.

The policy and associated procedures, which the Chief Privacy Officer is responsible for putting in place, provide for:

- Annual review of every privacy policy and all of its associated procedures against all of the above;
- Searches of relevant external websites and databases and of ICES' records to identify the changes, risks, deficiencies and inconsistencies listed above in support of the review;
- The procedure and timeframe for undertaking the review;
- The form, content and supporting evidence that must be generated to document the review;
- The procedure for identifying, and taking steps to address, any need to amend or supplement ICES' privacy policies, procedures and practices identified through the review; and
- Assignment of ICES Privacy Officers or qualified third parties to conduct the reviews.

ICES' Policy Framework and Governance Policy governs the revision, creation and communication of policies and procedures at ICES, including ICES' Privacy Audit and Monitoring Policy. In accordance with ICES' Policy Framework and Governance Policy, the Chief Privacy Officer is responsible for the creation, revision and communication of any changes to ICES' privacy policies and procedures, including ICES' Privacy Audit and Monitoring Policy. The Policy Framework and Governance Policy stipulates that changes must be communicated both to agents through ICES' intranet and to the public.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

3. Policy on the Transparency of Privacy Policies, Procedures & Practices

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
	b. Privacy Information, Inquiries & Complaints Policy	Implemented
	c. Privacy Statement	Implemented
	d. Website Privacy FAQ	Implemented

DESCRIPTION

ICES' Privacy Policy and Privacy Information, Inquiries and Complaints Policy require ICES to publish information about its data holdings and privacy policies, procedures and practices on its public website. Information that must be published on ICES' public website includes:

- ICES' Privacy Policy;
- Frequently asked questions related to ICES' privacy policies, procedures and practices;
- Documentation related to ICES' most recent review under s. 45(3) by the Information and Privacy Commissioner of Ontario;
- An overview of key administrative, technical and physical safeguards to protect privacy and prevent privacy breaches;
- A list of ICES' data holdings; and
- Instructions, including the title, mailing address and contact information, for making inquiries and complaints about ICES' privacy policies, procedures and practices and compliance with PHIPA and its regulation.

The Privacy Information, Inquiries and Complaints Policy requires publication of a brochure, which at a minimum must address:

- The types of personal health information in ICES data holdings and its sources;
- The purposes for which personal health information is collected;
- The purposes for which personal health information is used; and
- The circumstances under which ICES discloses personal health information.

Under the policies, ICES' Chief Privacy Officer is responsible for ICES' compliance with the above requirements.

4. Policy & Procedures for the Collection of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Collection of Personally Identifiable Information Policy	Implemented
	b. Collection of Personally Identifiable Information Procedures	Implemented
	c. Privacy Policy	Implemented
	d. ICES PIA Form – New ICES Data Holding	Implemented
	e. ICES Project PIA Form	Approved
	f. Privacy Audit & Monitoring Policy	Implemented
	g. Discipline & Corrective Action Policy	Implemented
	h. Privacy Incident Management Policy	Implemented
Comments	Implementation of the new ICES Project PIA Form is projected by December 31, 2014.	

	In the meantime, a substantially similar form is in effect.

DESCRIPTION

ICES' Privacy Policy identifies the purposes for which ICES collects personal health information, its nature, and from whom. Key collection purposes identified in the policy include health system analysis and evaluation, conducted by ICES independently or on behalf of policy-makers and health care providers, and research conducted by ICES scientists and others under the oversight of a research ethics board. Health information custodians like hospitals, other prescribed entities, prescribed registries and researchers are identified as the sources. All disclose personal health information to ICES.

ICES' Privacy Policy and Collection of Personally Identifiable Information Policy both articulate ICES' commitment to collect personal health information only in accordance with PHIPA and its regulation, to collect personal health information only where other information will not serve the purpose, and to collect no more personal health information than is reasonably necessary to meet the purpose.

Compliance with ICES' Privacy Policy and these procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

Review & Approval Process

The Collection of Personally Identifiable Information Policy stipulates that any agent who wishes to collect personal health information must ask ICES' Privacy Office to conduct a privacy impact assessment. Assessments, which are conducted by an ICES Privacy Officer in consultation with the requestor, must be completed to authorize the collection. The assessments are conducted against templates developed by ICES' Privacy Office under ICES' Privacy Impact Assessment Policy. The templates are designed to ensure that:

- Collection is permitted by PHIPA and its regulation;
- All conditions or restrictions in PHIPA and its regulation are satisfied;
- Other information, such as de-identified or aggregate information, will not serve the purpose; and
- No more personal health information is collected than is reasonably necessary for the identified purpose.

Conditions or Restrictions on Approval

ICES' privacy impact assessment templates, which are defined and mandatory, are the vehicle used to address and document each of the requirements listed above, and communicate the results. Requestors receive a copy of the completed assessment, which includes a decision to approve or deny collection as well as any conditions that must be met. These include requirements to establish a data sharing agreement prior to collection in all cases except where personal health information is being collected by an ICES Abstractor. In those cases, a data sharing agreement is not required if the responsible research ethics board has approved the collection and this is evidenced in writing. Both requirements are supported in the Collection of Personally Identifiable Information Procedures. The procedures define the process for obtaining approvals and establishing data sharing agreements. Where personal health information is being collected by an ICES Abstractor, responsibility for obtaining approvals rests with the project manager, who then initiates the collection process. In all other cases ICES' Data Partnership and Development staff is responsible. They alert ICES' Data Covenantors when agreements are in place and collection may therefore proceed.

Secure Retention, Transfer & Return or Disposal

The policy specifically requires that personal health information, once collected, be retained, transferred and returned or disposed of in accordance with ICES policies and procedures on these topics. Those policies are described in 2(5), 2(7) and 2(8) in Part 2 of Section B of this report.

5. List of Data Holdings Containing Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Data Dictionary	Implemented
DESCRIPTION		
ICES has developed and maintains an up-to-date list and brief description of ICES' data holdings, which is published on ICES' public website.		

6. Policy & Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES DSA (HIC)	Implemented
	b. ICES DSA (Researcher)	Implemented
	c. Collection of Personally Identifiable Information Procedures	Implemented
	d. Collection of Personally Identifiable Information Policy	Implemented
	e. Privacy Impact Assessment Policy	Implemented
	f. Privacy Audit & Monitoring Policy	Implemented
	g. Discipline & Corrective Action Policy	Implemented
	h. Privacy Incident Management Policy	Implemented
	i. ICES PIA Form – New ICES Data Holding	Implemented
	j. ICES Project PIA Form	Approved
Comments	Implementation of the ICES Project PIA Form is projected by December 31, 2014. In the meantime, a substantially similar form is in effect.	
DESCRIPTION		

ICES' Collection of Personally Identifiable Information Policy and associated procedures set out the requirements for generating, reviewing, amending and approving statements of purpose for data holdings containing personal health information. The policy requires ICES to generate a statement of purpose each time it collects information for inclusion as an ICES data holding. Statements of purpose must identify the purpose of the collection as well as the personal health information involved, its source, and the need for it.

Under the policy, any agent who wishes to collect personal health information for an ICES data holding must ask ICES' Privacy Office to conduct a privacy impact assessment. Assessments, which are conducted by an ICES Privacy Officer in consultation with, and signed off by, the requestor, are required to generate an approved statement of purpose. A member of ICES' Data Partnerships and Development team must then ensure that the approved statement of purpose is reviewed by the person or organization from whom the personal health information will be collected and incorporated into a data sharing agreement, which must be in place prior to collection. Under the policy, the statement of purpose must be amended, by repeating these procedures, prior to undertaking any activity that is inconsistent with the statement of purpose as approved.

The accuracy and currency of statements of purpose are verified on an ongoing basis as well as through annual audits. Permission to use any data holding is subject to review and approval by an ICES Privacy Officer. Conducted using an ICES Project PIA Form, the review must confirm that the proposed use is in accordance with the statement of purpose. Annual audits are conducted by an ICES Privacy Officer, and are required under ICES' Privacy Audit and Monitoring Policy. Where inaccuracies are discovered though an audit, these must be corrected by following the procedures for amendment described above.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or

procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

7. Statements of Purpose for Data Holdings Containing Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES DSA (HIC)	Implemented
	b. ICES DSA (Researcher)	Implemented
DESCRIPTION		
ICES generates a statement of purpose each time it collects personal health information for inclusion as an ICES data holding. Statements of purpose, are incorporated into, and form part of, data sharing agreements and research agreements with individuals and organizations who disclose personal health information to ICES. The statements of purpose identify the purpose of the data holding as well as the personal health information involved, its source, and the need for the information in relation to the identified purpose.		

8. Policy & Procedures for Limiting Agent Access to & Use of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Protection of ICES Data Policy	Implemented
	b. Contracts Database	Implemented
	c. ICES Confidentiality Agreement (General)	Implemented
	d. ICES Confidentiality Agreement (Data Covenantor)	Implemented
	e. ICES Confidentiality Agreement (Abstractor)	Implemented
	f. ICES Collaborating Researcher NDA	Implemented
	g. ICES Project PIA Form	Approved
	h. Privacy Impact Assessment Policy	Implemented
	i. ICES PIA – New Data Holding Form	Implemented
	j. Termination of Employment/Resignation & Discharge Policy	Implemented
	k. Termination of Employment, Resignation & Discharge Procedures	Implemented
	l. Management of Data Covenantors Procedure	Implemented
	m. Abstractor Onboarding & Offboarding Procedure	Implemented
	n. ICES Controlled Use Data Log	Implemented
	o. Log of ICES Abstractors	Implemented
	p. ICES Project PIA Log	Implemented
	q. Privacy Incident Management Policy	Implemented
	r. Discipline & Corrective Action Policy	Implemented

	s. Privacy Audit & Monitoring Policy	Implemented
Comments	Implementation of the new ICES Project PIA Form and of a required software upgrade is projected by December 31, 2014. In the meantime, a substantially similar version of the ICES Project PIA Form is in effect. Note, certain information identified in this Report as being captured in the Contracts Database will be captured in ICES' Integrated Data Log until October 31, 2014.	

DESCRIPTION

ICES' Protection of ICES Data Policy limits access to and use of personal health information by agents on a need-to-know basis. The policy ensures that agents access and use the least identifiable information and the minimum amount required for their role.

Under the policy, only ICES Data Covenantors and ICES Abstractors are permitted to handle personal health information with direct personal identifiers. These are the agents responsible for collecting personal health information at ICES. Agents who conduct health system analysis and evaluation, and link information in ICES data holdings for those purposes, are permitted to access "coded" information only. Coded information is personal health information from which direct personal identifiers, such as names and health card numbers, have been removed or replaced with a confidential code by an ICES Data Covenantor.

The extent of access to coded information is then subject to access levels and permissions, which are based on need. ICES analytic staff, who create project datasets, require and therefore have access to ICES data holdings; others on the project team are permitted to access and use project datasets only, subject to their assigned level of access and approval to participate in the project. For example, an epidemiologist may have access to a version of a project dataset that contains year of birth and the first three digits of the postal code; those variables will not be present in the version used by the investigator. Analytic staff are responsible for making these adjustments to the project datasets they create. And, under the policy, investigators who are not ICES scientists - called ICES collaborating researchers – are permitted to receive aggregate data only.

All agents are prohibited from accessing and using personal health information if other information, such as de-identified or aggregate information, will serve the purpose, and using more personal health information than is necessary for the purpose. Agents are also prohibited from using coded or other information, alone or in combination, to identify any individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. This prohibition is reinforced through ICES' confidentiality and non-disclosure agreements and conditions enforced through the ICES Project PIA Form, which is used to request and document approval to conduct projects at ICES.

<u>Review & Approval Process</u>

Under the Protection of ICES Data Policy, permission to access or use personal health information is subject to a privacy impact assessment. Privacy impact assessments are conducted by ICES Privacy Officers under ICES' Privacy Impact Assessment Policy.

Permission for an ICES Data Covenantor to collect and use personal health information for the purposes of establishing or maintaining an ICES data holding is provided in an ICES PIA Form – New Data Holding. The process for requesting a privacy impact assessment in this scenario and the requirements that must be satisfied are set out in Part 1(4) of Section B of this report.

All other permissions to access and use personal health information for purposes other than research are provided in the ICES Project PIA Form. Submitted to ICES' Privacy Office by the principal investigator for the project, the ICES Project PIA Form defines the requirements and documentation that must be satisfied in requesting, reviewing and determining whether, and on what basis, permission to use personal health information is granted. To approve, the ICES Privacy Officer must be satisfied that:

- The request to access and use personal health information is permitted by PHIPA and its regulation;
- The project objectives cannot reasonably be accomplished without the personal health information;
- The project objectives cannot be accomplished with de-identified and/or aggregate information; and
- No more personal health information will be accessed and used than is necessary to achieve the objectives of the project.

These determinations are supported by a warranty from the principal investigator, which has been confirmed by their program leader, that the personal health information is relevant and required. Further, in all cases permission is granted subject to the condition that a more granular dataset creation plan must be established jointly by the principal investigator and ICES analytic staff prior to creation of the project dataset, and align to the project objectives approved in the ICES Project PIA Form.

Once finalized, the ICES' Privacy Office Administrator sends the approved ICES Project PIA Form to the principal investigator for the project and uploads a copy to a network folder, where it is accessible to ICES' Data Covenantors and analytic staff.

Conditions & Restrictions on Approval

Again, the Protection of ICES Data Policy establishes the purposes for, and conditions under, which each category of ICES agent is permitted to access and use personal health information. Under the policy, permission for access and use personal health information is for, and for as long as required for, those purposes.

An imminent software upgrade will allow ICES Data Quality and Information Management team to translate end dates in privacy impact assessments into automatic expiries. In the meantime, this is reinforced by provisions in confidentiality agreements, which must be signed by every agent under ICES' Privacy Awareness and Training Policy. By signing, agents agree to access and use personal health information only:

- As necessary for their role;
- If other information will not serve the purpose; and
- To the extent reasonably necessary for the purpose.

The agreements also require agents to acknowledge and agree that they are not permitted to disclose personal health information. (The exception is ICES Data Covenantors, who are responsible for disclosures, subject to the policies and procedures described in Part 1(12) of Part B of this report.)

Notification & Termination of Access & Use

Procedures are in place to provide notification and terminate access and use when an agent is no longer employed by ICES or requires access. ICES' Termination of Employment/Resignation and Discharge Policy and procedures address notification and termination of access and use of personal health information at the end of employment. Under the procedures, employees are required to notify their supervisor in writing of their intention to resign. Within 24 hours of receipt, the supervisor is required to forward the written notice to a member of ICES' Human Resources staff, who is required to create a ticket that notifies ICES' Information Systems Department and ICES' Facility Manager one week before the departure. The ticket alerts those groups of the need to secure computer files and terminate access to ICES systems and facilities, and the timeframe for doing so. There are distinct procedures that govern the process for terminating access when an ICES Data Covenantor transitions to a different role or an ICES Abstractor's assignment concludes. The Management of Data Covenantors Procedures require the immediate supervisor to submit a request form to the Director of ICES Data Quality and Information Management, who must then send a ticket that instructs ICES' Information Systems to remove access. Under the Abstractor Onboarding and Offboarding Procedures, the research co-ordinator responsible for the ICES Abstractor sends the ticket, triggering removal of access and recovery of any IT equipment.

Secure Retention & Disposal

Under the Protection of ICES Data Policy all permission to access or use personal health information is subject to the policies and procedures governing secure retention and disposal that are described in 2(5) and 2(8) in Part 2 of Section B of this report.

Tracking Approved Access to & Use of Personal Health Information

ICES tracks approved access to and use of personal health information. Four logs are maintained. The Director of ICES' Data Quality and Information Management maintains the ICES Controlled Use Data Log, which lists approved ICES Data Covenantors. ICES' Data Quality and Information Management staff maintain the Contracts Database, which tracks actual access and use of personal health information by ICES Data Covenantors. The Director of ICES' Research Practice maintains a log of ICES Abstractors, which identifies abstractors and the scope, purpose and duration of their approval to access personal health information. Finally, the Privacy Office Administrator maintains the ICES Project PIA Log, which captures the names of all agents authorized to access and use personal health information for specific projects.

Compliance, Audit & Enforcement

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

9. Log of Agents Granted Approval to Access & Use Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Contracts Database	Implemented
	b. Privacy Awareness Log	Implemented
	c. ICES Abstractor Log	Implemented
	d. ICES Project PIA Log	Implemented
	e. DQIM Data Disclosure Log	Implemented

DESCRIPTION

ICES maintains logs of agents granted approval to access and use personal health information. Together the logs capture:

- Agent name;
- Data holding;
- Type of access and use;
- Start date; and
- End date.

Please note, the DQIM Data Disclosure Log captures date of disclosure instead of start and end dates.

10. Policy & Procedures for the Use of Personal Health Information for Research

APPLICATION		
Fully applicable ☐	Qualified application (*explain*) ICES' Privacy Policy permits the use of personal health information for research. Part1(10) therefore applies to ICES only up to the bolded sub-heading on page 31.	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
	b. Privacy Incident Management Policy	Implemented
	c. Discipline & Corrective Action Policy	Implemented
	d. Privacy Audit & Monitoring Policy	Implemented
	e. Research Ethics Review Policy	Implemented
	f. Protection of ICES Data Policy	Implemented
	g. Privacy Impact Assessment Policy	Implemented
	h. ICES Project PIA Form	Approved
	i. Privacy Awareness Policy	Implemented
	j. ICES Confidentiality Agreement (General)	Implemented
	k. ICES Confidentiality Agreement (Data Covenantor)	Implemented
	l. ICES Confidentiality Agreement (Abstractor)	Implemented
	m. ICES Collaborating Researcher NDA	Implemented
	n. ICES Project PIA Log	Implemented
Comments	Implementation of the new ICES Project PIA Form is projected by December 31, 2014. In the meantime, a substantially similar version of this form is in effect.	

DESCRIPTION

ICES' Privacy Policy identifies two scenarios in which personal health information may be used for research purposes. Personal health information may be used for research conducted by ICES and for the purposes of continuing research commenced outside ICES. In both cases, this is subject to the general principle, also articulated in the policy, that ICES does not use personal health information if other information will serve the purpose or use more personal health information than is necessary for the purpose.

Compliance with the privacy policy is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy, in accordance with ICES' Privacy Incident Management Policy. Violations, including breach, are subject to a range of disciplinary actions, including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

Circumstances in which use of Personal Health Information is Permitted

ICES Research Ethics Review Policy stipulates that ICES must obtain approval of its board of record, the Research Ethics Board of Sunnybrook Health Sciences Centre, prior to commencing any ICES research. Use of personal health information for the purposes of externally approved research must have the approval of the research ethics board that approved the research. These requirements are reinforced through the ICES Project PIA Form, which is used to request and document approval to conduct research in both scenarios.

Distinction between the Use of Personal Health Information for Research & Other Purposes

Both the Privacy Policy and the Research Ethics Review Policy explicitly distinguish between use of personal health information for research purposes and for the purposes of section 45 of PHIPA. This is reinforced in the ICES Project PIA Form. This is the form used to request and document permission to use personal health information for any project at ICES. Submitted to ICES' Privacy Office by the principal investigator for the project, the form must be reviewed and approved by an ICES Privacy Officer. To do so, the ICES Privacy Officer must identify and record on the form:

- Whether the use will be for a section 45 purpose or for research;
- Whether or not research ethics board approval is required; and
- Where research ethics board approval is required, identify any deficiencies in that approval, which need to be addressed in order for the project to proceed.

Review & Approval Process

Under the Protection of ICES Data Policy, permission to access or use personal health information for any project is subject to a privacy impact assessment. Privacy impact assessments are conducted by ICES Privacy Officers under ICES' Privacy Impact Assessment Policy, using the ICES Project PIA Form.

Submitted to ICES' Privacy Office by the principal investigator for the project, the ICES Project PIA Form defines the requirements and documentation that must be satisfied in requesting, reviewing and determining whether, and on what basis, permission to use personal health information for a research purpose is granted. To approve, the ICES Privacy Officer must be satisfied that:

- The request to access and use personal health information is permitted by PHIPA and its regulation;
- The proposed use of personal health information is reflected in a written research plan, which has been approved by a research ethics board in accordance with PHIPA and its regulation;
- A copy of the research ethics board approval is appended to the ICES Project PIA Form;
- The personal health information to be used is consistent with what has been approved;
- The research objectives cannot be accomplished with de-identified and/or aggregate information; and
- No more personal health information will be accessed and used than is necessary to achieve the research objectives.

These determinations are supported by a warranty from the principal investigator, which has been confirmed by their program leader, that the personal health information is relevant and required. Further, in all cases permission is granted subject to the condition that a more granular dataset creation plan must be established jointly by the principal investigator and ICES analytic staff prior to creation of the project dataset, and align to the research objectives approved in the ICES Project PIA Form.

Once finalized, the ICES' Privacy Office Administrator sends the approved ICES Project PIA Form to the principal investigator for the project and uploads a copy to a network folder, where it is accessible to ICES' Data Covenantors and analytic staff.

Conditions or Restrictions on the Approval

The ICES Project PIA Form is designed to ensure compliance with the requirements of section 44(6) (a) through (f) of PHIPA. It does so as follows. First, to approve, the ICES Privacy Officer is required to verify compliance with:

- Any conditions specified in the written research plan; and
- Any data sharing agreement governing personal health information disclosed to ICES for the research.

Second, in submitting an ICES Project PIA Form for approval, the principal investigator has already formally accepted that the research will be subject to the terms and conditions identified on the form. They stipulate that:

- Personal health information may be used only for the approved research objectives;
- Results must not be published in any form that could reasonably enable re-identification of any individual;
- Personal health information must not be disclosed except as required by law;
- No individual may be contacted; and
- Agents report breaches and suspected breaches to an ICES Privacy Officer at the first reasonable opportunity.

ICES' Privacy Incident Management Policy and procedures, in turn, require ICES to notify the person or organization who disclosed the information to ICES. Although the principal investigator has overarching responsibility for conduct of research, it should be noted that the same conditions are imposed through confidentiality agreements that are signed by every agent who participates.

Secure Retention, Return or Disposal

Personal health information used for research at ICES remains in ICES' custody and control at all times, subject to ICES' policies and procedures for secure retention, return and disposal described in 2(5) and 2(8) of Part 2 of Section B of this report. To the extent these are inconsistent with what has been approved by a research ethics board, that inconsistency will be identified and addressed as part of the ICES Privacy Officer's review and approval.

Where research involves ICES' collection of personal health information for the research, ICES' Collection of Personally Identifiable Information Policy and procedures will apply. They require establishment of a data sharing agreement, and use of an ICES template that will provide for destruction to be carried out by an ICES Data Covenantor. All ICES data sharing agreement templates also stipulate that the ICES Data Covenantor generate a signed destruction certificate that identifies the ICES Data Covenantor, the records of personal health information destroyed, and the date, time and method of destruction used, and deliver this to a contact identified in the agreement. Where de-identification or aggregation is required to comply with a research ethics board's approval, this will be carried out subject to ICES' policies and procedures described at 2(24) of Part B of this report.

ICES' compliance with all of the above is subject to an annual audit conducted by an ICES Privacy Officer under ICES' Privacy Audit and Monitoring Policy.

Tracking Approved Uses of Personal Health Information for Research

ICES uses the ICES Project PIA Log to track approved access to and use of personal health information for research The log is maintained by the Privacy Office Administrator, who is also responsible for creating and maintaining a file on the ICES network for every project, including research projects. They include the ICES Project PIA Form that approved conduct of the research with supporting research plans and approvals. ICES' Data Quality and Information Management team, who are responsible for all data destruction at ICES, maintain a separate log that captures creation of certificates of destruction.

11. Log of Approved Uses of Personal Health Information for Research

APPLICATION		
Not applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Project PIA Log	Implemented
	b. Contracts Database	Implemented
Comments	ICES will implement additional logging to manage obligations to return data (which are extremely rare), and to track the date personal health information was provided. This will impact a number of systems, so we plan to complete this no later than December 31, 2014.	

DESCRIPTION

The ICES Project PIA log, which is maintained by the Privacy Office Administrator, captures:

- The name of the research study;
- The principal investigator for the research study, to whom approval is granted;

- The date of the decision of the research ethics board that approved the written research plan;
- The date ICES approved use of personal health information for the research study;
- The nature of the personal health information approved for use; and
- The projected end date for the research study.

For any personal health information collected for the research study, the Contracts Database maintained by ICES' Data Covenantors captures:

- The planned destruction date; and
- The actual destruction date.

12. Policy & Procedures for Disclosure of Personal Health Information for Purposes Other Than Research

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
	b. Privacy Impact Assessment Policy	Implemented
	c. Privacy Incident Management Policy	Implemented
	d. Privacy Audit & Monitoring Policy	Implemented
	e. Discipline & Corrective Action Policy	Implemented
	f. ICES Project PIA Form	Approved
	g. ICES PIA Form – ICES Data Disclosure	Implemented
	h. Re-identification Risk Assessment Procedure	Planned
Comments	Implementation of the new ICES Project PIA Form is projected by December 31, 2014. In the meantime, a substantially similar version of the form is in effect. The procedure for creating documented risk assessments of reports and publications will be defined and implemented in the same timeframe.	

DESCRIPTION

ICES' Privacy Policy authorizes disclosure of personal health information to other prescribed organizations for their prescribed purposes, as permitted by PHIPA and its regulation and data sharing agreements. The policy does not authorize disclosure of personal health information in any other scenario. Disclosure is authorized only where other information will not serve the purpose, and only to the extent reasonably necessary to meet the purpose.

Compliance with ICES' Privacy Policy is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

Review & Approval Process

ICES' Privacy Policy stipulates that disclosures must undergo, and be approved through, a privacy impact assessment. Assessments are conducted by an ICES Privacy Officer under ICES' Privacy Impact Assessment Policy. Under that policy, ICES Data Partnerships and Development must submit a Request for Data Disclosure PIA Form to ICES' Privacy Office. This is the prompt for an ICES Privacy Officer to initiate an ICES PIA Form – ICES Data Disclosure to document its assessment and any approval and associated conditions and instructions. Once the ICES Privacy Officer is satisfied all conditions and restrictions have been satisfied, the completed form is communicated to ICES Data Partnerships and Development for action.

Requirements for disclosure that are enforced through the ICES PIA Form – ICES Data Disclosure include:

- The disclosure is permitted by PHIPA and its regulation;
- All conditions and restrictions under PHIPA and its regulation are satisfied;

- Other information, such as de-identified or aggregate information, will not serve the purpose; and
- No more personal health information will be disclosed than is reasonably necessary for the identified purpose.

Conditions & Restrictions on the Approval

Where disclosure is authorized, the ICES PIA Form – ICES Data Disclosure stipulates that a data sharing agreement is required and includes a section with instructions on this topic for ICES' Data Partnerships and Development. ICES' Data Partnerships and Development is responsible for ensuring a data sharing agreement is put in place prior to the disclosure, in accordance with ICES' policies and procedures described in Parts 1(16) and 1(17) of Section B of our report.

ICES' Privacy Policy authorizes disclosure of de-identified information only to knowledge users, such as policy-makers. It does so with the caveat that the information must first be assessed as creating no discernible risk of re-identification. Responsibility for making, documenting, communicating and retaining such assessments is being addressed and will be defined and implemented no later than December 31, 2014.

Secure Transfer, Return or Disposal

The topics secure transfer and secure return or disposal are both addressed in the ICES PIA Form – ICES Data Disclosure. The completed form provides instructions for how each of these topics must be addressed in the data sharing agreement that governs the disclosure, which must be in compliance with ICES' Secure Transfer, Retention and Destruction of ICES Data Policy. This includes the timeframe for return or destruction, including return or destruction in the context of termination of the data sharing agreement, and related enforcement mechanisms. ICES' Data Partnerships and Development department is responsible for administration of data sharing agreements, including enforcement of these required elements.

Compliance

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

13. Policy & Procedures for Disclosure of Personal Health Information for Research Purposes & the Execution of Research Agreements

APPLICATION		
Fully applicable ☐	Qualified application (*explain*) ICES' Privacy Policy does not permit disclosure of personal health information for research. Part 1(13) therefore applies to ICES only from the bolded sub-heading on page 39 of the IPC Manual. Please note, the procedures will be replaced by similar procedures, which are under development for the new ICES Data and Analytic Services Division (ICES DAS).	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
	b. CD-Link PIA Form	Implemented
	c. CD-Link Proposal Review & Approval Standard Operating Procedure (SOP)	Implemented
	d. CD-Link SOP – Dataset De-identification	Implemented
	e. CD-Link Data User Agreement	Implemented

DESCRIPTION

ICES' Privacy Policy does not permit disclosure of personal health information to researchers. Disclosure of de-identified information only is permitted under the policy.

Review & Approval Process

Procedures are in place, and roles and responsibilities defined, for the review and approval of requests to disclose to

external researchers. This is enabled by the CD-Link PIA Form, which ensures consistent handling and documentation of approvals against clear criteria. Criteria for approval include demonstration that each variable of the personal health information involved is necessary for the purposes of the identified research objectives and a determination the researcher's plan for securing the data is appropriate. Researchers who wish to receive data under the program are required to complete a CD-Link PIA Form and submit it to ICES for review and approval by an ICES Privacy Officer. The CD-Link PIA Form is used by ICES' Privacy Office to document its assessment and any approval and associated conditions and instructions. Once the responsible ICES Privacy Officer is satisfied all conditions and restrictions have been satisfied, the completed form is communicated to the CD-Link program co-ordinator, who communicates the result to the researcher.

The procedures are then in place that require an ICES analyst to review any CD-Link dataset prior to disclosure to verify it does not identify any person and could not foreseeably be used to do so.

Conditions or Restrictions on the Approval

The procedures require that a data use agreement be put in place with the researcher prior to disclosure. The agreement specifically prohibits any attempt to re-identify any individual represented in a CD-Link dataset, which is de-identified. It also stipulates that the dataset may be disclosed to the researcher only after the researcher provides evidence of research ethics board approval for the research that meets the requirements of PHIPA and its regulation. The agreements and approvals are tracked by the program co-ordinator.

14. Template Research Agreement

APPLICATION		
Not applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
DESCRIPTION		
ICES' Privacy Policy does not permit disclosure of personal health information to researchers. This requirement is therefore not applicable to ICES.		

15. Log of Research Agreements

APPLICATION		
Not applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented
DESCRIPTION		
ICES' Privacy Policy does not permit disclosure of personal health information to researchers. This requirement is therefore not applicable to ICES.		

16. Policy & Procedures for the Execution of Data Sharing Agreements

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Impact Assessment Policy	Implemented
	b. ICES PIA Form – ICES Data Disclosure	Implemented
	c. ICES PIA Form – New Data Holding	Implemented

	d. ICES Project PIA Form	Approved
	e. Request for New Data Holding PIA Form	Implemented
	f. Request for ICES Data Disclose PIA Form	Implemented
	a. Privacy Audit & Monitoring Policy	Implemented
	g. Discipline & Corrective Action Policy	Implemented
	h. Privacy Incident Management Policy	Implemented
	i. Contracts Database	Implemented
Comments	Implementation of the new ICES Project PIA Form is projected by December 31, 2014. In the meantime, a substantially similar version of this form is in effect.	

DESCRIPTION

ICES has developed policies and procedures to identify the circumstances under which, and the processes to be followed, to put in place data sharing agreements.

ICES' Privacy Impact Assessment Policy stipulates that no personal health information may be collected or disclosed unless approved through a privacy impact assessment. Assessments are guided by forms, which define the circumstances under which a data sharing agreement is required. In the case of disclosures for purposes other than research, a data sharing agreement is always required.

The forms, which must be completed and approved by an ICES Privacy Officer, set out the requirements that must be satisfied and the process to be followed in relation to data sharing agreements. For example, the ICES Project PIA Form is used to assess requests to collect personal health information for a specific project. Once complete, that form identifies the correct legal authority for the collection and corresponding data sharing agreement template, and gathers content required to complete the template. Collectively ICES' privacy impact assessment forms ensure that ICES enters into data sharing agreements:

- To disclose personal health information for purposes other than research only where the disclosure has been approved in accordance with ICES' policies and procedures described in Part 1(12) of Section B of this report; and
- To collect personal health information for purposes other than research only where the collection has been approved in accordance with ICES' policies and procedures described in Part 1(4) of Section B of this report.

The forms include a section for data sharing agreement instructions and approvals, which are provided by ICES' Privacy Office. Responsibility for initiation is specified on the forms, and varies by scenario. Where collection is for the purposes of a single project, the form is initiated by the principal investigator. In all other cases, including requests to disclose, ICES Data Partnerships and Development are required to submit the appropriate request for PIA form to ICES' Privacy Office, who then initiate the corresponding privacy impact assessment form. Once approved, the Privacy Office Administrator or responsible ICES Privacy Officer alerts ICES Data Partnerships and Development, who are responsible for ensuring data sharing agreements are executed in accordance with the approvals and instructions documented on the form. The forms also stipulate that, once executed, ICES Data Partnerships and Development reflect this in a log, which they are required to maintain.

Compliance with the policy and its procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

17. Template Data Sharing Agreement

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES DSA (HIC)	Implemented
	b. ICES DSA (Researcher)	Implemented
Comments	ICES undertakes to initiate review and revision, as required, of its umbrella data sharing	

	agreements with prescribed entities and persons no later than October 31, 2014.

DESCRIPTION

ICES has established template data sharing agreements for use when a data sharing agreement is required under its policies and procedures. The templates address the matters set out below.

General Provisions

The templates describe ICES' status as a prescribed entity under PHIPA and the duties and responsibilities arising from that status. They specify the precise nature of any personal health information subject to the agreement and provide a definition of personal health information that is consistent with PHIPA and its regulation. The templates also identify the party that is collecting and party that is disclosing under the agreements.

Purposes of Collection, Use & Disclosure

The templates identify the purposes for which personal health information is being collected and will be used under the agreements. In identifying these purposes, the templates explicitly state that direct personal identifiers, such as names and personal health numbers, will be removed or replaced with a confidential code and only linked with other similarly coded information. In addition, the agreements describe the nature and source of that other information, how linkage will be conducted and why it is required for the identified purpose.

The templates also contain an acknowledgement that any personal health information being collected is, and is no more than is, reasonably necessary for the purpose, and that other information, such as de-identified or aggregate information, will not serve the purpose. The templates stipulate that any personal health information may be disclosed only where required by law. They further stipulate that all collection, use or disclosure of any personal health information that is subject to the agreements must comply with PHIPA and its regulation, and set out the authority for each collection, use and disclosure contemplated.

Secure Transfer

The templates require secure transfer of any personal health information, and set out the manner, contact and procedure for transfer. This information is captured in an appendix, which must be completed by ICES Data Partnership and Development staff, who are responsible for establishing data sharing agreements. This permits selection of the ICES-approved method for secure transfer that is most appropriate in each case. In the majority of cases, the method selected will be use of an ICES-managed encrypted channel.

Secure Retention

The templates stipulate that ICES is permitted to retain personal health information with direct personal identifiers only as long as required for ICES analysts, who created linked datasets for projects, to detect and resolve data quality issues. They also specify the retention method. Physical media must be retained in locked rooms or cabinets, and information saved on ICES systems must be isolated from the ICES network and accessible by ICES Data Covenantors only. Both methods of retention comply with ICES' policies governing secure retention. In addition, the templates include a specific provision requiring ICES to take steps to protect any personal health information against theft, loss and unauthorized use or disclosure, and a range of supporting safeguards. The most important of these is the stipulation that scientists and analytic staff will have access to information without direct personal identifiers only and on condition they make no attempt to re-identify any person.

Secure Return or Disposal

The templates stipulate that ICES securely destroy the personal health information with direct personal identifiers after the coded information, which is derived from it, has been delivered to ICES' analytic staff for linking. The templates provide a definition of secure destruction and identify the precise methods that may be used, which must not fall short of industry standards and relevant IPC orders. The templates specify that destruction must be carried out within 6 months of delivery to ICES' analytic staff, and a destruction certificate provided 5 business days after that. Destruction certificates must be delivered to the general contact for notice, who is identified in the agreement, and identify the records of personal health information disposed of and the date, time, location and method of destruction used, and bear the name and signature of the ICES Data Covenantor who carries out the destruction.

Notification

The templates require that notification be provided at the first reasonable opportunity if the agreement has been breached or personal health information subject to the agreement has, or is suspected to have, been stolen, lost or accessed by unauthorized persons. The process and contact for notice are defined, which must be provided in writing.

Consequences of Breach & Monitoring Compliance

The templates outline the consequences of breach of the agreements, which include a right of immediate termination in the event of a privacy breach. To enable compliance, the templates specifically require that any ICES Data Covenantor who handles the personal health information must be familiar with, and agree to uphold, the terms and

conditions of the agreement and that this be confirmed in a confidentiality agreement. ICES discloses personal health information in very limited circumstances. Rarity combined with the complexity and particularity of those data partnerships do not lend themselves to creation or use of a specific template. ICES acknowledges that the requirements in this subsection are applicable in these cases, and undertakes to ensure any future data sharing agreements comply with the above requirements.

18. Log of Data Sharing Agreements

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Contracts Database	Implemented
	b. ICES Project PIA Log	Implemented
	c. DQIM Data Disclosure Log	Implemented
	d. ICES PIA – Data Disclosure Form	Implemented

DESCRIPTION

ICES has developed and maintains a log of executed data sharing agreements. Information captured in the log includes:

- Name of the person or organization from whom the personal health information was collected or to whom the personal health information was disclosed;
- Date agreement executed;
- Nature of the personal health information;
- Retention end-date, or required destruction date, for the personal health information;
- Agreement termination date; and
- Date on which personal health information has been securely returned or destroyed.

The remaining required elements are captured through other vehicles developed and maintained by ICES:

- The ICES Project PIA Log contains the date the collection was approved;
- The ICES PIA – Data Disclosure Form contains the date the disclosure was approved;
- The Contracts Database contains the collection date and the date of return or destruction;
- The Contracts Database contains the date destruction certificates are provided; and
- The DQIM Data Disclosure Log contains the dates of all disclosures.

19. Policy & Procedures for Executing Agreements with Third Party Service Providers in Respect of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Privacy Impact Assessment Policy	Implemented
	b. ICES PIA – Service Provider Form	Implemented

DESCRIPTION

ICES' Privacy Impact Assessment Policy stipulates that a privacy impact assessment be conducted prior to establishing any service relationship involving personal health information. Responsibility for requesting a privacy impact assessment rests with the agent who wishes to establish the service relationship. The ICES PIA – Service Provider Form, which is used to conduct privacy impact assessments in this scenario, requires that a service level agreement be put in place prior to permitting access to personal health information by a third party service provider.

ICES' Privacy Office is responsible for the conduct of privacy impact assessments. Privacy impact assessments are conducted by ICES Privacy Officers using the ICES PIA – Service Provider Form. Completion of that form

results in:

- Acceptance of responsibility by the requestor to ensure a service level agreement is put in place by ICES' Procurement Manager;
- Compliance of all service level agreements with the template described in Part 1(20) of this report;
- A determination by the responsible ICES Privacy Officer that personal health information is provided to any third party service provider only where other information, such as de-identified or aggregate information, will not serve the purpose, and no more personal health information is provided than is reasonably necessary to meet the purpose;
- Acceptance of responsibility by the requestor for ensuring compliance with service provider obligations to return or destroy, and provide a certificate of destruction for, any personal health information in the event of termination, and referring cases of non-compliance to the Chief Privacy Officer for action after 30 days; and
- Responsibility of ICES' Procurement Manager to ensure any service level agreement is logged in, and a copy uploaded to, ICES' Contracts Database.

Compliance with the policy and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

20. Template Agreement for All Third Party Service Providers

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Privacy Impact Assessment Policy	Implemented
	b. ICES PIA – Service Provider Form	Implemented

DESCRIPTION

ICES' Privacy Impact Assessment Policy stipulates that a privacy impact assessment be conducted by an ICES Privacy Officer prior to establishing any service relationship involving personal health information. The ICES PIA – Service Provider Form, which is used to conduct privacy impact assessments in this scenario, requires that a service level agreement be put in place in all cases and defines minimum content for such agreements. The minimum content includes:

- A description of ICES' prescribed status and its associated duties under PHIPA and its regulation;
- Whether or not the service provider will act as ICES' agent, and if yes, an agreement to comply with PHIPA and provisions in the agreement related to the collection, access, use, disclosure, secure transfer, retention and destruction of personal health information;
- The precise nature of the personal health information the service provider will be permitted to access or use and a definition of personal health information that is consistent with PHIPA and its regulation;
- The identity of the party that is collecting or disclosing personal health information;
- An obligation of the service provider to deliver services in a professional manner, in accordance with industry standards and practices and by properly trained agents of the service provider;
- Prohibition against access, use and disclosure of personal health information except as necessary to provide the agreed services and permitted by the agreement or as required by law;
- Purposes of authorized access, use and disclosure of any personal health information and related limitations and conditions as well as authority under PHIPA and its regulation;
- Prohibition against use and disclosure where other information will serve the purpose or in excess of that which is reasonably necessary;
- General and specific obligations to protect information against theft, loss and unauthorized use, disclosure, copying, modification or disposal;
- An obligation and specific method to make agents who will have access to records of personal health

information aware of and agree to comply with the obligations in the agreement;
- Where subcontracting is permitted, service provider's duty to enter into an equivalent agreement with the subcontractor and provide advance notice of subcontracting and a copy of the agreement to ICES;
- Where relevant, whether the information will be returned or destroyed following termination of the agreement, the associated timeframe and specific manner, which must comply with ICES' policies and procedures reported in Part 2(7) of Section B of this report;
- Consequences of breach, duty to notify at the first reasonable opportunity and associated process and timelines, including manner and contact for notice and containment requirements; and
- Where appropriate taking in account the information and the service, right of audit and associated mechanics, including notice.

Where the service provider is acting as an electronic service provider that is not an agent of ICES:

- Prohibition against disclosure except as required by law.

Where the service involves transfer:

- Secure transfer method, procedure, timeframes, conditions and recipients, which meet the requirements of ICES' own policies and procedures for secure transfer;
- Service provider's obligation to maintain an inventory of transfers, inbound and outbound;
- Service provider's obligation to provide certificates of receipt, with date and time and mode of transfer; and
- Overarching responsibility of the service provider to maintain security during transfer.

Where the service involves retention:

- Service provider's obligation to maintain an inventory of, and track, records of personal health information being retained;
- Secure retention method (by medium); and
- Overarching responsibility of the service provider to maintain security over retained records.

Where the service includes destruction:

- A definition of secure disposal that is consistent with PHIPA and its regulation;
- Destruction method (by medium) and security, which is consistent with PHIPA and its regulation and relevant orders, guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner;
- Service provider's obligation to provide certificates of destruction that specify records destroyed, date, time, method and responsible agent (including signature), the timeframe for doing so and ICES recipient;
- Timeframes and triggers for destruction (including termination); and
- Right of ICES to witness destruction.

Where disposal is the primary service provided, in addition to the requirements above:

- Timeframe within which destruction must be carried out;
- Precise destruction method for each medium involved;
- Conditions surrounding destruction;
- Service provider's obligation to maintain an inventory of, and track, records of personal health information being destroyed; and
- Persons responsible for ensuring destruction is secure.

21. Log of Agreements with Third Party Service Providers

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Contracts Database	Implemented

DESCRIPTION
ICES has defined and maintains a log of agreements with third party service providers. Information captured in the log includes: • Service provider name; • Service description; • Effective date; • Date the personal health information was transferred/provided; • Nature of the personal health information provided/accessed; • Termination date; • Whether the personal health information will be returned or destroyed; and • Date information returned/certificate date.

22. Policy & Procedures for the Linkage of Records of Personal Health Information

APPLICATION		
Not applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Protection of ICES Data Policy	Implemented
	b. Privacy Impact Assessment Policy	Implemented
	c. ICES Project PIA Form	Approved
	a. ICES Project PIA Review Procedure	Implemented
	d. CD-Link PIA Form	Implemented
	e. CD-Link SOP – Proposal Review & Approval	Implemented
	f. Privacy Incident Management Policy	Implemented
	g. Privacy Audit & Monitoring Policy	Implemented
	h. Linking Procedure	Planned
Comments	Implementation of the new ICES Project PIA Form is projected by December 31, 2014. In the meantime a substantially similar version of the form is in effect. Development and implementation of a linking procedure is planned for the same timeframe.	

ICES' Protection of ICES Data Policy permits linkages of personal health information, and identifies the purposes for and circumstances under which this is permitted. Linkages of personal health information are permitted for the purposes of creating project datasets to support the conduct of projects and research that have been reviewed and approved in accordance with ICES policies and procedures.

The mechanism for approval for project and research, and associated linkages, is a privacy impact assessment. Criteria for approval include whether:

- In the case of research only, it will be conducted at ICES or externally;
- The project or research will be conducted by ICES and only involve linkages of personal health information from ICES' data holdings;
- The project or research will be conducted at ICES and involve linkage with records of personal health information collected from external sources;
- In the case of research conducted externally, the research will involve linkages of personal health information from ICES' data holdings; and
- In the case of research conducted externally, the research will involve linkages of personal health information from ICES' data holdings with records of personal health information collected from external sources for the purposes of the research.

<u>Review & Approval Process</u>

Again, permission to link personal health information is subject to a privacy impact assessment. Privacy impact assessments are conducted by ICES Privacy Officers under ICES' Privacy Impact Assessment Policy.

The ICES Project PIA Form is used to request linkages of personal health information for projects and research conducted within ICES. The CD-Link PIA Form is used where the request is for research to be conducted outside ICES. Submitted to ICES' Privacy Office by the principal investigator, these forms define the requirements and documentation that must be satisfied in requesting, reviewing and determining whether, and on what basis,

permission for linkages of personal health information is granted.

To approve, the ICES Privacy Officer must be satisfied that the requested linkages are:

- Permitted by PHIPA and its regulation;
- Permitted by data sharing agreements and research ethics board approvals applicable to the request; and
- Relevant and reasonably necessary for accomplishment of the stated objectives.

Once finalized, ICES' Privacy Office Administrator sends an approved ICES Project PIA Form to the principal investigator for the project and uploads a copy to a network folder, where it is accessible to analytic staff, who perform linkages. The Privacy Office Administrator forwards an approved CD-Link PIA Form to the CD-Link program co-ordinator, who communicates it to analytic staff once an agreement with the researcher is in place.

Conditions & Restrictions on Approval

Under ICES' Protection of ICES Data Policy linked records of personal health information must be de-identified prior to disclosure to an external researcher. Linkages for projects and research conducted within ICES are subject to ICES' policies and procedures described at Parts 1(8), 1(10) and 1(24) of Section B of this report.

Process for the Linkage of Records of Personal Health Information

The Protection of ICES Data Policy stipulates that linking records of personal health information is the responsibility of ICES analytic staff. Historically, the linking process has been regarded as an exercise of professional skill and judgment. ICES acknowledges that a procedure is required to be fully compliant with this section of the Manual, and so commits to capturing this activity in a procedure and implementing this by December 31, 2014.

Secure Retention & Disposal

Under the Protection of ICES Data Policy, until and unless they are de-identified in accordance with ICES' policy and procedures, all linked records of personal health information are subject to the policies and procedures governing secure retention and disposal described in 2(5) and 2(8) in Part 2 of Section B of this report.

Compliance, Audit & Enforcement

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

Tracking Approved Linkages of Personal Health Information

ICES uses the ICES Project PIA log to track all approved linkages of personal health information. Maintained by the Privacy Office Administrator, the log captures the name of the principal investigator of the associated project or research, who requested the linkages, the date the linkages were approved, and the nature of the personal health information linked.

23. Log of Approved Linkages of Records of Personal Health Information

APPLICATION		
Not applicable ☐	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Project PIA Log	Implemented
DESCRIPTION		

ICES has developed and maintains a log of approved linkages of personal health information. Information captured in the log includes:

- Requestor name;
- Approval date; and
- Description of the personal health information approved for linking.

24. Policy & Procedures with Respect to De-Identification & Aggregation

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Protection of ICES Data Policy	Implemented
	b. CD-Link SOP – Dataset De-identification	Implemented
	c. CD-Link Data User Agreement	Implemented
	d. Privacy Incident Management Policy	Implemented
	e. Privacy Audit & Monitoring Policy	Implemented
	f. Creation of Summary Data Procedure	Planned
Comments	Development and implementation of the Creation of Summary Data Procedure is planned for no later than December 31, 2014.	

DESCRIPTION

ICES' Protection of ICES Data Policy stipulates that personal health information may not be used or disclosed if other information, namely de-identified or aggregate information, will serve the identified purpose. It also identifies the following specific scenarios in which de-identified information only may be used or disclosed:

- Incorporation of results into publications and reports; and
- Disclosure for research conducted outside ICES.

Investigators who are not ICES scientists are permitted to collaborate on ICES projects, but may use aggregate information only (in ICES' policies, referred to as "summary" information).

ICES' Protection of ICES Data Policy addresses the topic of cell sizes of less than five – or small cells. The policy, which takes into account restrictions in data sharing agreements as well as research plans, prohibits inclusion of small cells in any report or publication of the results of any ICES project or any research, whether conducted at ICES or by an external researcher.

The policy contains definitions of de-identified information, aggregate - "summary"- information and small cells. All have regard to, and are consistent with, the meaning of "identifying information" in section 4(2) of PHIPA.

ICES has a procedure that defines the information that must be removed, encrypted and/or truncated in order to constitute de-identified information. It also specifically provides for review of the resulting information prior to disclosure. The review, which is performed and documented by an ICES analyst, is conducted against specific criteria identified in the procedure, which are designed to ensure no individual is identified and it is not reasonably foreseeable in the circumstances the information could be used, either alone or in combination with other information, to identify an individual. Currently articulated in the CD-Link procedure identified above, the procedure is being augmented to include specific consideration of the type of directly and indirectly identifying information available and expanded to support research in any area, not just cancer. In addition, it is being adapted to reinforce ICES' long-standing practice of reviewing reports and publications prior to release. These, along with a procedure for the creation of aggregate – "summary" – information, will all be defined and implemented to comply with the requirements of this section on or by December 31, 2014.

External researchers who receive de-identified information from ICES are required to sign confidentiality agreements that prohibit them from using the information, alone or in combination, to identify any individual. This includes attempting to decrypt information that is encrypted, attempting to identify an individual based on unencrypted information and attempting to identify an individual based on prior knowledge. The agreements provide that ICES may terminate access to the information in the event of any violation of this condition by a researcher.

Compliance with the policy and any procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

25. Privacy Impact Assessment Policy & Procedures

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Impact Assessment Policy	Implemented
	b. Privacy Impact Assessments Log	Implemented
	c. ICES PIA Form – New ICES Data Holding	Implemented
	d. ICES PIA Form – General	Implemented
	e. ICES PIA Form – ICES Data Disclosure	Implemented
	f. ICES PIA Form – Third Party Research	Implemented
	g. ICES PIA Form – Service Provider	Implemented
	h. ICES Project PIA Form	Approved
	i. Privacy Audit & Monitoring Policy	Implemented
	j. Privacy Audit Log & Report Forms Workbook	Implemented
	k. Policy Framework & Governance Policy	Implemented
	l. Privacy Incident Management Policy	Implemented
	m. Discipline & Corrective Action Policy	Implemented
Comments	Implementation of the new ICES Project PIA Form is projected by December 31, 2014. In the meantime, a substantially similar version of this form is in effect.	

DESCRIPTION

ICES' Privacy Impact Assessment Policy identifies the circumstances under which privacy impact assessments must be conducted. Under the policy, a privacy impact assessment is required before the implementation of any change that will substantially affect the collection, use or handling of personal health information by or on behalf of ICES. There are no exceptions. The policy provides an illustrative list of triggers, which include:

- Proposed establishment of a new data holding;
- Establishing or changing a service relationship that involves personal health information; and
- Introducing or substantially changing a business process, information system or technology that involves personal health information.

The policy stipulates that privacy impact assessments are to be conducted prior to implementation of the change. They must be initiated at the conceptual design stage and then reviewed and amended, as necessary, at both the detailed design and pre-implementation stages. Under the policy, responsibility for requesting a privacy impact assessment rests with the person responsible for the data holding, process, system or service relationship involved. That person must contact ICES' Privacy Office to request a privacy impact assessment before proceeding. The Chief Privacy Officer has distributed day-to-day responsibility for the conduct of privacy impact assessments across the Privacy Office, and this is communicated on the privacy page of the ICES intranet. For example, a particular Privacy Officer is responsible for assessing new data holdings and is identified as the first point of contact for requesting a privacy impact assessment in that scenario. When a request for a privacy impact assessment is received, the designated ICES Privacy Officer is then responsible for conducting, reviewing and/or amending the privacy impact assessment, with oversight by the Chief Privacy Officer and support from an ICES Security Officer, as required.

ICES has created a suite of forms to guide privacy impact assessments. Tailored according to scenario, the forms address:

- The data holding, information system, technology or program at issue;
- The nature and type of personal health information involved and its sources;
- The purpose and rationale for collection, use or disclosure;
- The flow of personal health information;
- Legal authority for each collection, use and disclosure of personal health information;
- Limitations imposed on collection, use and disclosure;
- Whether or not personal health information will be linked to other information;
- Retention period;
- Secure manner in which the personal health information will be retained, transferred and disposed of;
- Administrative, technical and physical safeguards, including functionality for logging access, use,

modification and disclosure of personal health information and functionality for auditing to detect unauthorized use or disclosure;
- Privacy risks and mitigation strategies; and
- Recommendations arising from privacy impact assessments and associated responsibilities of agents, including compliance oversight and timelines.

ICES has established a log of privacy impact assessments, which captures the following:

- Responsible Privacy Officer;
- The timeframe within which a particular privacy impact assessment needs to be completed;
- Privacy impact assessments that have been completed;
- Privacy Impact assessments that have been initiated but not completed; and
- Privacy impact assessments that were evaluated and determined not required and why.

The privacy impact assessment forms all include instructions to Privacy Officers to reflect assessments and their status in the Privacy Impact Assessments Log. Privacy impact assessments may be marked as closed only after the Privacy Officer is satisfied all recommendations have been addressed.

Implementation and effectiveness of the Privacy Impact Assessment Policy and associated forms is subject to audit under ICES' Privacy Audit and Monitoring Policy. Under that policy, the Chief Privacy Office is required to establish an audit schedule that includes an audit of the Privacy Impact Assessment Policy and associated procedures each year. This would include testing to verify the quality and continued accuracy of specific privacy impact assessments as well as completion rates. The privacy audit procedures, which are defined in the Privacy Audit Log and Report Forms Workbook, provide, in turn, for correction of deficiencies detected through an audit.

Compliance with the policy and its procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

26. Log of Privacy Impact Assessments

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Impact Assessments Log	Implemented

DESCRIPTION

ICES has defined and implemented a log of privacy impact assessments. Information captured in the log includes:

- Privacy impact assessments that have been completed;
- Privacy Impact assessments that have been initiated but not completed;
- Privacy impact assessments that were evaluated and determined not required and why;
- The associated data holding, information system, technology, program or process;
- Target date for completion;
- Actual date of completion;
- The ICES Privacy Officer responsible for determining whether or not a privacy impact assessment is required and, if so, completing or ensuring the completion of the privacy impact assessment; and
- Existence and status of any recommendations.

The log includes a Recommendations tracking sheet, which captures for each recommendation:

- The associated privacy impact assessment;
- The agents responsible for addressing the recommendation;
- The manner in which it has been agreed that each recommendation will be addressed; and

- The date as of which the recommendation was or is expected to be addressed.

27. Policy & Procedures in Respect of Privacy Audits

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Audit & Monitoring Policy	Implemented
	b. Privacy Audit Log & Report Forms Workbook	Implemented

DESCRIPTION

ICES' Privacy Audit & Monitoring Policy identifies the purpose and frequency of privacy audits. Under the policy, ICES must conduct an audit to test compliance with each of its privacy policies and their associated procedures every year. This includes a requirement to audit ICES' policies and procedures governing agent access and use of personal health information described at Part 1(8) of Section B of this report. The Chief Privacy Officer has overall responsibility for implementation of the policy. This specifically includes responsibility for the appointment and oversight of appropriately skilled agents to conduct audits and establishment of an audit schedule.

The ICES Privacy Audit and Report Forms Workbook is designed to hold report forms to guide audits. Report forms will be tailored by audit type, but will consistently address the following:

- The nature (e.g. document reviews, interviews) and scope of the audit;
- Responsible auditor;
- Selection criteria;
- Audit findings;
- Recommendations;
- Remedial action and associated responsibilities, timing and status; and
- Whether or not notice will be provided.

A report form for an audit of ICES' Privacy Awareness Policy and procedures has been created as a proof of concept. Additional report forms will be devised after the design of this first report form is tested and as ICES' program of privacy audits is rolled out over time.

Topics common to all privacy audits are addressed on the general Instructions page for auditors at the front of the ICES Privacy Audit Log and Report Forms Workbook. These topics include:

- The process, form and content for giving notice of a planned audit;
- Content and responsibility for maintaining audit files;
- Location of audit files;
- Responsibility for making and communicating audit findings and recommendations, and the timing, manner and content of those communications;
- Responsibility and a timeline for establishing and carrying out action plans to address recommendations;
- Responsibility and a timeline for monitoring the implementation and effectiveness of action plans;
- Approval and reporting of audit findings, which include a requirement to report high risk findings to ICES' Chief Executive Officer; and
- Timing and required documentation for closure of audit files.

The Instructions sheet also addresses maintenance of the Privacy Audit Log, including storage location of the log and audit files and auditors' responsibility for:

- Maintenance of the log;
- Communicating and tracking recommendations that arise from privacy audits;
- Documentation of audits.

Agents who conduct audits have a duty to report any breaches or suspected breaches detected at the first reasonable opportunity under ICES' Privacy Incident Management Policy.

28. Log of Privacy Audits

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Audit Log & Report Forms Workbook	Implemented

DESCRIPTION

ICES has defined a log of privacy audits that have been completed. Information captured in the log includes:

- The nature and type of privacy audit conducted;
- The date the privacy audit was completed;
- Agent responsible for completing the privacy audit;
- Recommendations arising from the privacy audit;
- Agent responsibile for addressing each recommendation;
- The date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

29. Policy & Procedures for Privacy Breach Management

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Incident Management Policy	Implemented
	b. Privacy Incident Log & Report Forms Workbook	Implemented
	c. Privacy Audit & Monitoring Policy	Implemented
	d. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Privacy Incident Management Policy and associated procedures address the process to be followed for the identification, reporting, containment, notification, investigation and remediation of privacy breaches. The definition of privacy breach encompasses any collection, use, disclosure, copying, modification, disposal, loss, theft or other act or failure to act, involving personal health information, or information derived from it such as de-identified information, that makes personal health information subject to unauthorized copying, modification or disposal or that is not in accordance with:

- PHIPA or its regulation;
- ICES' privacy or policies as a prescribed entity; or
- Any data sharing or other agreement governing ICES' handling of the personal health information.

Under the policy, every agent is required to report such events to an ICES Privacy Officer at the first reasonable opportunity. Events are considered detected and reportable, and subject to this policy and its associated procedures, once suspected. This includes events reported and handled initially as information security breaches.

Agents who detect or suspect a privacy breach are required to report it to the ICES Privacy Officer at the ICES location most closely associated with the breach. They are required to do so immediately. The policy stipulates that contact is to be made verbally, wherever practicable, and otherwise by email. In the absence of an ICES Privacy Officer, reports should be made to ICES' Chief Privacy Officer. The identity and contact information for ICES Privacy Officers as well as the Chief Privacy Officer is provided, and accessible to all agents, on the privacy page of ICES' intranet. The ICES Privacy Officer creates an entry for the report on the Privacy Incidents Log and establishes a file on the secure Privacy folder on the ICES network.

Under the procedures, an ICES Privacy Officer is then required to launch a Privacy Breach Report Form and commence an investigation. The Form, which guides the investigation and must be completed, captures the date of

the report, the nature and extent of the personal health information involved and the determination whether or not a breach has, in fact, occurred. Where it has, the investigating Privacy Officer is required to report this immediately to the Chief Privacy Officer, who must notify ICES' Chief Executive Officer. Whether that report is provided verbally or in writing depends on the complexity of the facts to be relayed, and is decided by the Chief Privacy Officer. The information provided to the Chief Executive Officer includes the nature and extent of the personal health information involved, containment measures and the identity of any parties who must be notified and a plan for how notice will be given. This is subject to the general requirement that notice to those parties should be given at the earliest reasonable opportunity.

The procedures stipulate that breaches, including suspected breaches, be immediately contained by the responsible ICES Privacy Officer. The procedures specify the approach and objectives for containment. At a minimum, the ICES Privacy Officer must determine whether or not the breach resulted in copies of personal health information being made, and if so, to ensure and document their secure return or destruction. Where records are destroyed, the date, time and method of destruction must be captured. Containment must also prevent further unauthorized access, use or disclosure of the personal health information or other personal health information. The nature of the containment measures taken and who is responsible for taking them must be documented on the Privacy Breach Report Form, and sent to the Chief Privacy Officer for review and approval.

Where an investigation indicates there has been a privacy breach involving personal health information, the procedures require ICES to notify the person or organization that disclosed that personal health information to ICES. The ICES Privacy Officer responsible for handling the breach is required to prepare a written notification plan for review by the Chief Privacy Officer. The plan must take into account any particular arrangements relevant to notification contained in the data sharing agreement. It must also identify the appropriate ICES agent to deliver the notice and its format, the nature of the personal health information at issue, the measures that have been, and will be, implemented to contain the breach, including investigation and remediation. Once approved, the Chief Privacy Officer is required to inform ICES' Chief Executive Officer of the notification plan, and ensure it is carried out and addresses all of the information identified in the plan.

Where requested by an organization, ICES may agree to notify third parties or individuals on their behalf, but only with the approval of ICES' Chief Privacy Officer and Chief Executive Officer.

Under the procedures, the responsible ICES Privacy Officer is required to commence an investigation once a breach has been contained. The objective is to gain a more precise understanding of the breach, including the personal health information involved, and identify the root cause(s) and measures to address them. The ICES Privacy Officer is empowered to make whatever inquiries are reasonably required to achieve these objectives, which can include document review, interviews and physical inspections. All must be reflected in the Privacy Breach Report Form and supported by documentation, which must be saved to the incident file.

The ICES Privacy Officer is responsible for communicating recommendations and working with agents to finalize action plans to address them, consulting with the Chief Privacy Officer as necessary. The ICES Privacy Officer then reflects what has been agreed in a written plan, which is sent to the agent. This includes the names of those responsible as well as the timeline, which cannot exceed 45 days unless approved by the Chief Privacy Officer. It is the responsibility of the agents identified on the plan to assign others, as required, to carry it out; the ICES Privacy Officer monitors to ensure compliance with the agreed timeline and reflects this in the Privacy Incidents Log. Where relevant, an ICES Security Officer will be involved in developing, or carrying out, action plans.

Once all remedial action and notification are complete, the ICES Privacy Officer ensures all supporting documentation is saved to the file, updates the Privacy Breach Report Form and sends a link to the Chief Privacy Officer to request approval to close the file. The Form, which is reviewed and endorsed by the Chief Privacy Officer, captures all the key facts associated with the breach, including recommendations and their status. Once approval is received, the ICES Privacy Officer reflects this in the Privacy Incidents Log, which is maintained to track all breaches and associated recommendations and timelines.

Compliance with the policy and its procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

30. Log of Privacy Breaches

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Incident Log	Implemented
DESCRIPTION		

ICES maintains a log of privacy breaches, which captures:

- The date of the privacy breach;
- The date the privacy breach was identified or suspected;
- Whether the privacy breach was internal or external;
- The nature of the personal health information involved and the nature and extent of the privacy breach;
- The date the privacy breach was contained and the nature of the containment measures;
- The date the health information custodian or other person or organization that disclosed the information was notified;
- The date investigation of the privacy breach was completed;
- The agent responsible for conducting the investigation;
- Recommendations arising from the investigation;
- The date each recommendation was, or is expected to be, addressed;
- Responsibility for addressing recommendations; and
- The manner in which each recommendation was, or is expected to be, addressed.

31. Policy & Procedures for Privacy Inquiries & Complaints

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Information, Inquiries & Complaints Policy	Implemented
	b. Privacy Inquiries & Privacy Complaints Log	Implemented
	c. Privacy Inquiry Report Form	Implemented
	d. Privacy Complaint Report Form	Implemented
	e. Privacy Inquiry & Privacy Complaints Procedures	Implemented
	f. Privacy Complaint Response 1 Template 1 A	Implemented
	g. Privacy Complaint Response 1 Template 1 B	Implemented
	h. Privacy Complaint Response 2 Template	Implemented
	i. Privacy Complaint Form	Implemented
DESCRIPTION		

ICES' Privacy Information, Inquiries and Complaints Policy in combination with the Privacy Inquiries and Privacy Complaints Procedures, Privacy Inquiries and Privacy Complaints Log, Privacy Inquiry Report Form, Privacy Complaint Report Form and letter templates address the process to be followed in the receiving, documenting, tracking and responding to privacy inquiries and complaints.

Privacy Inquiries

Under the policy, privacy inquiry is defined and includes inquiries about ICES' compliance with PHIPA and its regulation and the policies, procedures and practices ICES implements as a prescribed entity. The policy requires the Chief Privacy Officer to ensure that ICES' public website informs the public of their right to make a privacy inquiry to ICES, and provides a title, mailing address and format(s) for contacting ICES to enable this.

The policy requires the Chief Privacy Officer to establish procedures for the receipt, handling and documentation of privacy inquiries. The Privacy Inquiry and Complaints Procedures and associated log and report form have been devised for this purpose. Together they define the process for receiving and responding to privacy inquiries at ICES.

Topics they address include:

- Responsibility for receipt and response;
- Documentation that is required to be completed and provided;
- Required content of the documentation;
- The format and content of response to privacy inquiries; and
- Roles and responsibilities of the Chief Privacy Officer, ICES Privacy Officers and ICES' Security Office.

All of the procedures, including documentation, are carried out or co-ordinated by ICES Privacy Officers with oversight by ICES' Chief Privacy Officer.

Privacy Complaints

Under the policy, a privacy complaint is defined and includes concerns or complaints about ICES' compliance with PHIPA and its regulation and the policies, procedures and practices ICES implements as a prescribed entity. The policy requires the Chief Privacy Officer to ensure that ICES' public website informs the public of their right to make a privacy complaint to ICES or the Information and Privacy Commissioner of Ontario. Under the policy, the information on ICES' public website must include a title and mailing address for contacting both ICES and the IPC, as well as format(s) for communicating privacy complaints to ICES.

The policy also requires the Chief Privacy Officer to establish procedures for the handling and documentation of privacy complaints. The Privacy Inquiry and Complaints Procedures and associated log and report form have been devised for this purpose. Together they define the process for receiving and responding to privacy complaints at ICES. Topics they address include:

- Responsibility for receipt and response;
- Documentation that is required to be completed and provided;
- Required content of the documentation;
- The nature of information that must be requested from complainants; and
- Roles and responsibilities of the Chief Privacy Officer, ICES Privacy Officers and ICES' Security Office.

Except for notification and approvals, which are the responsibility ICES' Chief Privacy Officer, all of the procedures outlined here are either carried out or co-ordinated by an ICES Privacy Officer.

The procedures require a determination to be made whether or not a privacy complaint will be investigated and identify the agent responsible, timeline, process and criteria for doing so, and related documentation. Where the determination is that the privacy complaint does not warrant investigation, the procedures stipulate that a letter be sent to the complainant to acknowledge the complaint and advise them of the decision not to investigate. The template that has been developed for use in this scenario also advises complainants of their right to complain to the Information and Privacy Commissioner of Ontario and provides contact information to enable this. Where the determination is that investigation is warranted, the procedures stipulate that a letter be sent to the complainant to acknowledge the complaint, advise them of the decision to investigate and describe the investigation process, including the process for requesting further information from the complainant, the projected timeframe, and the nature of the documentation the complainant will be provided upon completion of the investigation. The procedures identify the agents responsible for sending these letters and associated timelines.

The procedures identify the agent responsible for investigating privacy complaints, as well as the process for planning and carrying out investigations. This includes a discussion of how investigations and associated findings must be documented and the content of that documentation, as well as responsibility for its creation, communication and approval. The procedures also define the process for addressing recommendations that arise from the investigations, with associated responsibilities, timelines and requirements for documentation. Also addressed is the topic of notification, with associated responsibilities, content requirements and timelines. This includes criteria for the notification of ICES' Chief Executive Officer and third parties, as well a template letter to complainants that speaks to investigative findings and recommendations, if any, as well as the right to complain to the Information and Privacy Commissioner of Ontario, with contact information to enable this.

The Privacy Information, Inquiries and Complaints Policy requires the Chief Privacy Officer to define procedures to track privacy complaints. The Privacy Inquiries and Privacy Complaints Log, Privacy Inquiries and Privacy Complaints Procedures, and Privacy Complaint Form have been designed, and work together to address logging, creation and retention of documentation, as well as responsibility for oversight and timely closure of recommendations.

Compliance & Enforcement

Compliance with the policy and its procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject

to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

32. Log of Privacy Complaints

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Information, Inquiries & Complaints Policy	Implemented
	b. Privacy Inquiries & Privacy Complaints Log	Implemented
	c. Privacy Complaint Report	Implemented

DESCRIPTION

ICES maintains a log of privacy complaints received, which captures the following:

- Date received and type of complaint;
- Decision whether or not to investigate and the date this decision is made;
- Date the complainant is advised of the decision whether or not to investigate;
- Investigator name;
- Date of investigation commencement and completion;
- Whether or not the investigation revealed deficiencies in ICES' processes;
- Status of remedial action; and
- Date the complainant is advised of the investigation findings and any remediation.

The information in the Privacy Complaints Log is supplemented by the more detailed Privacy Complaint Report, which is created for each privacy complaint ICES receives. Information captured in the Privacy Complaint Report includes:

- Specific deficiencies and recommendations identified by the investigation;
- Agent responsible for addressing each recommendation;
- Timeline for addressing each recommendation; and
- Manner in which each recommendation will be addressed.

Part 2 – Security Documentation

1. Information Security Policy

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Framework & Governance Policy	Implemented
	b. Security Incident Management Policy	Implemented
	c. Security Audit Policy	Implemented
	d. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Security Framework and Governance Policy establishes an overarching framework, and responsibility, for information security at ICES. Requirements of the policy specifically include:

- Establishment of an information security program that consists of administrative, technical and physical safeguards aligned with established industry standards and practices, and that has sufficient documentary requirements to allow independent verification;
- Ensuring that ICES takes reasonable steps to protect personal health information against theft, loss and unauthorized use or disclosure and protect records of personal health information against unauthorized copying, modification or disposal;
- Conduct of organization-wide threat and risk assessments of all information assets, including personal health information, and project specific threat and risk assessments; and
- Establishment of a documented methodology for assessing and remediating threats and risks and prioritizing their remediation.

The policy requires ICES' information security program to consist of control objectives and security policies, procedures and practices that address:

- Ongoing review of security policies and procedures;
- Information security training and awareness for all ICES staff;
- Physical security;
- Secure retention, transfer and disposal of records containing personal health information, including information contained on mobile devices, remote access and security of information at rest;
- Access control and authorization, including business requirements, user access management, user responsibilities, network access control, operating system access control and application and information access control;
- Systems acquisition, development and maintenance, including the security requirements of information systems, correct processing in applications, cryptographic controls, security of system files, security in development and support procedures and technical vulnerability management;
- Monitoring, including maintenance and review of system control and audit logs and security audits;
- Network security, including patch management and change management;
- Acceptable use of information technology;
- Back-up and recovery;
- Security breach management; and
- Protection against malicious and mobile code.

The policy stipulates that the information security infrastructure provide for:

- The transmission of personal health information over authenticated, encrypted and secure connections;
- Security-hardened servers, firewalls and secure segregation of services within ICES' network;
- Anti-virus, anti-spam and anti-spyware measures;
- Intrusion detection and prevention systems;
- Privacy and security enhancing technologies; and
- Mandatory system-wide password-protected screen savers after a defined period of inactivity.

The policy also provides for continuous assessment and verification of ICES' information security program in order to deal with threats and risks to data holdings containing personal health information. ICES relies on its

security audit program for such continuous assessment and verification. The program consists of assessments of the effectiveness of the administrative, technical and physical safeguards ICES has implemented. Specifically, audits assess compliance with ICES' security policies, procedures and practices, including those governing access to and use of personal health information, and include vulnerability assessments and penetration testing of ICES' information systems conducted by independent auditors.

ICES' Chief Executive Officer is ultimately accountable for ensuring the security of information at ICES and that agents comply with the security policies, procedures and practices. The Senior Director, Data Platform has been delegated authority to approve and oversee the information security program. The Security Lead has been delegated authority to develop and implement the information security program, which includes implementation of administrative, technical and physical safeguards. The Senior Director, Corporate Services has been delegated authority to approve and oversee the physical security of ICES' premises. The Facilities Manager has been delegated authority to develop and implement the physical security program.

Compliance with the above policy and its procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

2. Policy & Procedures for Ongoing Review of Security Policies, Procedures & Practices

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Framework & Governance Policy	Implemented
	b. Security Audit Policy	Implemented
	c. Security Audit SOP	Implemented
	d. Security Audit Log	Implemented
	e. Policy Framework & Governance Policy	Implemented
	f. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Security Audit Policy and associated procedures provide for continuous monitoring of ICES' security policies and procedures. Matters addressed in the policy and procedures include frequency, timeframe and the procedures for conduct of reviews, which must be conducted at least annually. Ongoing monitoring is the joint responsibility of ICES' Senior Director, Data Platform and the Security Lead. Required audit activities specifically include monitoring for continued alignment of ICES' security policies, procedures and practices against:

- Applicable IPC orders, guidelines, fact sheets and best practices;
- Evolving industry security standards and best practices;
- Technological advancements;
- Amendments to PHIPA and its regulation;
- Recommendations arising from privacy and security audits;
- Recommendations arising from threat-risk assessments and privacy impact assessments;
- Recommendations resulting from investigations into privacy or security breaches; and
- Consistency of security policies and procedures with actual ICES practices and with ICES' privacy policies and procedures.

ICES' Policy Framework and Governance Policy governs revision, creation, communication and implementation of policies and procedures at ICES and changes to them. The policy specifically addresses:

- The procedure and responsibility for amending or drafting policies and procedures as a result of the review, and obtaining approval;
- The procedure and responsibly for internal communication of amended or new policies, including the method and nature of communication;
- The procedure and responsibility for reviewing and amending any external communication materials as a

result of the amended or new policies.

At ICES each policy and procedure has a designated "owner", who is responsible for ensuring the ongoing maintenance of the policy or procedure, and a designated "authority", who is responsible for overseeing formal review of the policy or procedure and approving amendments. The Senior Director, Data Platform is the authority for security policies and procedures. New or amended security policies and procedures that affect general ICES operations or require broader communication must undergo review and approval by ICES faculty members and ICES' Operations Committee before final approval by the Senior Director, Data Platform. Communication of amended or new security policies or procedures is the responsibility of the Senior Director, Data Platform.

Compliance with the above policies and procedures is mandatory for all agents. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

3. Policy & Procedures for Ensuring Physical Security of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Physical Security Policy	Implemented
	b. ICES-Central Physical Security SOP	Implemented
	c. ICES-Central Visitor SOP - Electronic Access Badge	Implemented
	d. ICES-Central Visitor SOP - Non-Electronic Access Badge	Implemented
	e. Visitors Sign In/Out Sheet	Implemented
	f. Visitors Policy	Implemented
	g. Keyscan Vantage Access Control System	Implemented
	h. Track-IT System	Implemented
	i. Onboarding System	Implemented
	j. Key Sign In Log	Implemented
	k. Security Audit Policy	Implemented
	l. Security Incident Management Policy	Implemented
	m. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES has defined a policy and associated procedures to address the physical safeguards required to protect personal health information against theft, loss and unauthorized use or disclosure and protect records of personal health information against unauthorized copying, modification or disposal.

Physical safeguards provided for under ICES' Physical Security Policy include controlled access to premises and locations where records of personal health information are retained, such as locked, restricted and/or monitored access. In addition, the policy provides for the creation of security zones, with progressive levels of security and the highest level preserved for locations where personal health information is held.

Compliance with the policy and its procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

Access by Agent

The policy and procedures identify the various agents responsible for receiving, reviewing, granting and terminating access by agents to ICES' premises and to locations within the premises where records of personal health

information are retained, including the levels of access that may be granted, which are outlined in the policy and procedures. The various responsible agents include supervisors, the Security Lead, the Director, Data Quality and Information Management and the Facilities Manager. The policy and procedures also address:

- Criteria for determining level of access, based on the "need-to-know" principle;
- Time-limited access, where appropriate; and
- Provisioning of identification cards, access cards and/or keys by the Facilities Manager.

Required documentation and communication of the above is also identified in the procedures. Supervisors must submit a Track-IT ticket to the Facilities Manager requesting an agent's access and supply any required confirmations of approval. The Facilities Manager will issue an identification card or access card programmed to allow access only to authorized locations within ICES' premises and for the required timeframe. The Facilities Manager must deliver the identification card or access card and/or keys to the agent in person.

Theft, Loss & Misplacement of Identification Cards, Access Cards & Keys

The policy and procedures set out the requirements and the process to be followed in the event of theft, loss and misplacement of identification cards, access cards and/or keys. The procedures require agents to notify ICES' Security Lead or the Facilities Manager at the first reasonable opportunity by email and must specify when and where the identification card, access card and/or keys were lost or misplaced. The Security Lead or Facilities Manager, as applicable, must immediately deactivate any electronic identification card or access cards. The Facilities Manager will issue a temporary or replacement identification card or access card and/or keys and must log the agent's name, card and/or key number, the date issued and the timeframe for return in the key log and/or card holder database, which are maintained and retained by the Facilities Manager. Where an agent fails to return an identification card or access card and/or keys, the Facilities Manager must contact the agent immediately to ensure they are returned, and for any electronic identification card or access card not returned, must also ensure it is deactivated.

Termination of Employment, Contractual or Other Relationship

The procedures require agents and their supervisors to notify a Human Resources Associate of the termination of the agent's employment, contractual or other relationship, and identify the procedure to be followed in terminating access. This includes a requirement that identification cards, access cards and/or keys be returned on the date of termination, at which time access to the premises must be terminated by the Facilities Manager. The timeline for terminating access, although not explicit, is by implication immediate. Termination includes deactivation of any electronic identification cards or access cards, and ensuring keys have been returned.

Notification When Access is No Longer Required

The procedures outline the process to be followed when an agent no longer requires access to locations within ICES that contain personal health information, including a requirement that agents and their supervisors notify the Facilities Manager. Notification, the nature and format of which is specified in the procedures, must be provided on or before the date that access is no longer required. The Facilities Manager must immediately reprogram the electronic identification card or access card to terminate access to the restricted locations, and ensure all applicable keys issued to the agent are returned.

Audit of Agents with Access to the Premises

ICES requires the conduct of audits of agents with access to ICES' premises and to locations within the premises where records of personal health information are retained, in accordance with ICES' Security Audit Policy and Security Audit SOP (Standard Operating Procedure). The purpose of the audit is to ensure that agents continue to have an employment, contractual or other relationship with ICES and continue to require the same level of access.

Under the SOP, an ICES Security Officer must review ICES' physical access logs and consult with agents' supervisors to confirm the agents continue to require access. The ICES Security Officer is required to notify the Facilities Manager of any required modifications to an agent's access. Audits of access must be conducted annually. An ICES Security Officer is responsible for ensuring compliance with ICES' Security Audit Policy and Security Audit SOP.

Tracking & Retention of Documentation Related to Access to the Premises

The procedures identify systems used to log access approvals and changes, and assign responsibility to ICES' Facilities Manager and, where applicable, ICES' receptionist for the management of those systems. Documentation related to the receipt, review, approval and termination of access to ICES' premises and locations within the premises are stored in the Facilities Manager's electronic or paper files.

Visitors

ICES' Visitors Policy and associated procedures identify the agents responsible and the process to be followed in identifying, screening and supervising visitors. Each visitor has a designated host who, where applicable, must

inform ICES' receptionist in advance of the visitor's arrival. The receptionist notifies the host when the visitor has arrived at ICES. Visitors are required to complete the visitors log, recording their name, date and time of arrival, the agent(s) with whom they are meeting and the date and time of departure. Where a visitor requires an electronic access card or identification card with special access privileges, the host must complete a Track-IT ticket requesting that the Facilities Manager issue the card. The Visitors Policy specifies the identification that must be worn by visitors at all times.

The procedures address the duties of agents responsible for identifying, screening and supervising visitors. At a minimum, the host must ensure the visitor is accompanied at all times, wears the identification card issued to him/her and returns it upon departure. The host and ICES' receptionist are jointly responsible for ensuring the visitor completes the visitors log upon arrival and departure. Where it is discovered that a visitor has failed to complete the log, ICES' receptionist must contact the host to obtain the necessary information. Where a visitor has failed to return the identification card or access card, ICES' receptionist must contact the host, who must, in turn, follow up with the visitor to ensure the card is returned. If the card is lost or missing, ICES' receptionist must notify the Facilities Manager, who is required to deactivate any electronic card.

The procedures require that ICES' receptionist retain the visitors log in the receptionist's office and that the Facilities Manager retain other documentation related to the identification, screening or supervision of visitors in his/her office in a designated file.

4. Log of Agents with Access to the Premises of the Prescribed Person or Prescribed Entity

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES-Central Physical Security SOP	Implemented
	b. Onboarding System	Implemented
	c. Keyscan Vantage Access Control System	Implemented
	d. Track-IT System	Implemented
	e. Visitors Sign In/Out Sheet	Implemented
	f. ICES-Central Visitors SOP - Non Electronic Badge	Implemented
	g. ICES-Central Visitors SOP - Electronic Access Badge	Implemented
	h. Visitors Policy	Implemented
	i. Termination of Employment/Resignation & Discharge Procedure	Implemented
	j. Security Audit Policy	Implemented
	k. Security Audit SOP	Implemented

DESCRIPTION

ICES has defined procedures that address the requirement to maintain a log of agents granted approval to access the premises and the level of access granted. The required logs can be generated from the systems and processes identified above, and include:

- Agent's name;
- Level and nature of access;
- Locations within the premises to which access is granted;
- Date(s) access was granted;
- Date(s) identification cards, access cards or keys were provided, associated identification numbers and date(s) returned; and
- Date of next audit.

The systems and processes are subject to audit by an ICES Security Officer under ICES' Security Audit Policy and associated procedures.

5. Policy & Procedures for Secure Retention of Records of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Data Management Policy	Implemented
	b. ICES Data Management Standard	Implemented
	c. Data Backup Policy	Implemented
	d. Destruction of ICES Data SOP	Implemented
	e. Privacy Impact Assessment Policy	Implemented
	f. ICES PIA Form - Service Provider	Implemented
	g. Security Incident Management Policy	Implemented
	h. Security Audit Policy	Implemented
	i. Discipline & Corrective Action Policy	Implemented
Comments	ICES undertakes to create a records retention schedule. Implementation is projected for no later than December 31, 2014.	

DESCRIPTION

ICES has developed policies and procedures that collectively satisfy the requirements with respect to the secure retention of records of personal health information in paper and electronic format.

The ICES Data Management Policy mandates that records of personal health information in both paper and electronic format be retained for only as long as necessary to fulfill the purposes for which they were collected. The policy requires that records of personal health information collected for research not be retained for longer than specified in the research plan approved by a research ethics board, and that records of personal health information collected pursuant to a data sharing agreement not be retained for longer than set out in the agreement. The policy provides for the establishment of a records retention schedule to monitor and manage retention of personal health information in accordance with research plans and data sharing agreements.

The policy stipulates that records of personal health information must be retained in a secure manner and assigns overall responsibility to the ICES' Director, Data Quality and Information Management. The policy and the ICES Data Management Standard identify the precise methods by which records of personal health information in paper and electronic format must be securely retained. Records of personal health information on paper must be stored in locked rooms and cabinets. Records of personal health information in electronic format on ICES systems must be stored on a server isolated from the ICES network. Records of personal health information on mobile media must be encrypted and stored in locked rooms and safes.

The policy requires agents to take reasonable steps to ensure records of personal health information are protected against theft, loss and unauthorized use, disclosure, copying, modification or disposal. The detail of the policy and supporting standard, compliance with which is mandatory, effectively defines the reasonable steps, which include use of locked rooms, cabinets and safes, segregated servers with access controls and encryption of mobile media. As well, under the standard personal health information with direct personal identifiers is retained only temporarily until data quality issues have been resolved and is then securely destroyed by an ICES-approved method.

<u>Retention by a Third Party Service Provider</u>

ICES' Privacy Impact Assessment Policy addresses the selection and management of any third party service provider contracted to retain records of personal health information on ICES' behalf (e.g. for backup purposes). The policy stipulates that a privacy impact assessment must be conducted prior to establishing any such service relationship. The ICES PIA Form - Service Provider, completion of which is the responsibility of an ICES Privacy Officer, has been defined for this purpose. The form is designed to:

- Address the circumstances under which and the purposes for which records of personal health information will be transferred to a third party for secure retention;
- Establish and detail an appropriately secure procedure and method for the transfer of records of personal health information to the third party and the retrieval of records from the third party, which meet the requirements of ICES' own policies and procedures for secure transfer;
- Identify conditions for transfer and retrieval; and
- Ensure the services are appropriately documented in a service level agreement that meets or exceeds appropriate mandatory privacy content, which must be reviewed and approved by an ICES Privacy Officer prior to transfer.

The ICES Data Management Policy addresses the documentation that must be maintained in relation to the transfer of records of personal health information to a third party service provider for retention. In particular, the agent responsible for ensuring the secure transfer, either the Director, Information Technology (IT) or delegate, is required to document the date, time and mode of transfer, and maintain a repository of written confirmations received from the third party service provider upon receipt of the records as well as a detailed inventory of the personal health information being securely retained by or retrieved from the third party service provider.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

6. Policy & Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Protecting Personal Health Information on Mobile Devices Policy	Implemented
	b. Security Audit Policy	Implemented
	c. Discipline & Corrective Action Policy	Implemented
	d. Security Incident Management Policy	Implemented
	e. Privacy Impact Assessment Policy	Implemented
	f. ICES Project PIA Form	Approved
	g. ICES Project PIA Review Procedure	Implemented
	h. Password Policy	Implemented
	i. Mobile Device Policy	Implemented
	j. ICES Data Management Policy	Implemented
	k. ICES Data Management Standard	Implemented
	l. Access to ICES Data Policy	Implemented
	m. Remote Access Policy	Implemented
	n. Discipline & Corrective Action Policy	Implemented
Comments	Implementation of the new ICES Project PIA Form is projected for no later than December 31, 2014. In the meantime, a substantially similar version of this form is in effect.	

DESCRIPTION

ICES has developed policies and procedures to identify whether and in what circumstances ICES permits the retention of records of personal health information on mobile devices. The term "mobile device" is defined in ICES' Protecting Personal Health Information on Mobile Devices Policy. Compliance with the policies and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

ICES' Protection of Personal Health Information on Mobile Devices Policy authorizes collection and retention on mobile devices subject to approval through a privacy impact assessment. Conducted by an ICES Privacy Officer under ICES' Privacy Impact Assessment Policy, privacy impact assessments are guided by, and documented through, an ICES Project PIA Form. The agent requesting to collect or retain records of personal health information on a mobile device must submit an ICES Project PIA Form, the required content of which is defined in the form, to an

ICES Privacy Officer. The ICES Privacy Officer must review the ICES Project PIA Form, taking into account the criteria for approving or denying the request, including ensuring that other information - namely de-identified and/or aggregate information - will not serve the purpose and no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose. The ICES Privacy Officer must indicate approval by signing a copy of the ICES Project PIA Form and returning it by email to the agent.

ICES' Protecting Personal Health Information on Mobile Devices Policy and Mobile Device Policy establish conditions and restrictions on retention, which include:

- Retention of de-identified or aggregate information only if it will serve the purpose;
- De-identification to the fullest extent possible;
- A prohibition against retaining more personal health information on a mobile device than is reasonably necessary for the identified purpose;
- Use of encryption and complex passwords in accordance with ICES' Password Policy, and responsibility of assigned IT staff for encryption;
- Password-protected screen savers and responsibility for enabling them;
- Shortest possible retention period;
- Second layer of encryption and different complex password at the file level; and
- Ensuring the use of the personal health information subject to assessment has already been approved pursuant to ICES' Privacy Impact Assessment Policy and supporting procedures.

ICES' Protecting Personal Health Information on Mobile Devices Policy requires agents to retain personal health information on the mobile device in compliance with ICES' policies and procedures relating to secure retention of records of personal health information and securely delete the information in accordance with the process and timeframe set out in the policies and procedures. This policy and the ICES Data Management Policy both address steps and measures to protect personal health information on mobile devices against theft, loss and unauthorized use, disclosure, copying, modification or disposal.

Remote access to personal health information is prohibited under ICES' Remote Access Policy.

7. Policy & Procedures for Secure Transfer of Records of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Data Management Policy	Implemented
	b. ICES Data Management Standard	Implemented
	c. Secure Transfer of Personal Health Information SOP	Implemented
	d. Contracts Database	Implemented
	e. DQIM Data Disclosure Log	Implemented
	f. Security Incident Management Policy	Implemented
	g. Security Audit Policy	Implemented
	h. Discipline & Corrective Action Policy	Implemented
Comments	The process, conditions, roles and responsibilities, and required documentation for secure transfer of personal health information on paper and by email are currently set out in ICES' primary data collection training modules. Development of a formal procedure to manage paper and email transfers, compliance with which will be mandatory for all agents and subject to annual audit, is planned, with a projected implementation date of no later than December 31, 2014.	
DESCRIPTION		
ICES has developed policies and procedures that collectively address the secure transfer of personal health information in paper and electronic format. The ICES Data Management Policy requires personal health information to be transferred in a secure manner, and the ICES Data Management Standard and the Secure Transfer of Personal Health Information SOP set out the secure methods of transferring records of personal health information in paper and electronic format that have been approved by ICES. The policy specifically requires agents to use only approved methods of transferring records of personal health information and prohibits all other methods. The standard and SOP outline the approved methods and associated procedures.		

Electronic File & Mobile Media Transfers

The standard and SOP authorize transmission of records of personal health information through a secure and encrypted electronic file transfer system or encrypted mobile media. The standard and SOP outline the conditions for transfer. These include conduct and approval of a privacy impact assessment by an ICES Privacy Officer that documents authority for the transfer of records. The SOP assigns responsibility to an ICES Data Covenantor for ensuring the records of personal health information are securely transferred. In the case of inbound transfers, ICES' receptionist is permitted to receive mobile media transferred to ICES by courier, but upon receipt, the media must be retrieved by an ICES Data Covenantor and stored in a secure data safe.

The SOP identifies the documentation that must be completed in relation to the secure transfer. For each inbound transfer an ICES Data Convenantor must update the Contracts Database, recording the date and mode of transfer and the recipient of the records of personal health information. The Contracts Database also contains the nature of personal health information transferred to ICES. For each outbound transfer, the ICES Data Covenantor must update the DQIM Data Disclosure Log, recording the date and mode transfer, the recipient of the records and the nature of the personal health information transferred. The ICES Data Covenantor is required to file confirmations of receipt.

Paper & Email Transfers

The standard permits the transfer of records of personal health information by email or by paper only in the context of a specific type of ICES activity called "primary data collection". The procedures, conditions, roles and responsibilities and required documentation for paper and email transfers are set out in ICES' primary data collection training modules. Paper, which is only ever transferred from data custodians to ICES and never from ICES to them, must be sent by courier and any direct personal identifiers must be removed prior to transfer. Records sent by email must not contain direct personal identifiers and must be retained in a password-protected file. Paper and email transfers are permitted subject to conduct and approval of a privacy impact assessment by an ICES Privacy Officer. The assigned ICES research coordinator or ICES Abstractor, as applicable, is responsible for ensuring the records are securely transferred. Confirmations of receipt by email are required in the case of email transfers.

The SOP together with the ICES Data Management Policy and the ICES Data Management Standard outline the administrative, technical and physical safeguards that must be implemented in transferring records of personal health information through each of the approved methods. The policy requires that the approved methods of secure transfer and associated procedures and safeguards be consistent with IPC orders, including Order HO-004 and Order HO-007; IPC guidelines, fact sheets and best practices, and evolving privacy and security standards and best practices.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

8. Policy & Procedures for Secure Disposal of Records of Personal Health Information

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Data Management Policy	Implemented
	b. ICES Data Management Standard	Implemented
	c. Destruction of ICES Data SOP	Implemented
	d. Information Media Destruction SOP	Draft
	e. Privacy Impact Assessment Policy	Implemented
	f. ICES PIA Form – Service Provider	Implemented
	g. Security Audit Policy	Implemented
	h. Privacy Audit & Monitoring Policy	Implemented
	i. Security Incident Management Policy	Implemented
	j. Privacy Incident Management Policy	Implemented
	k. Discipline & Corrective Action Policy	Implemented

Comments	Implementation of the Information Media Destruction SOP is projected by October 31, 2014.

DESCRIPTION

The ICES Data Management Policy and related procedures address the secure disposal of records of personal health information in both paper and electronic format. The policy requires records of personal health information to be disposed of in a secure manner that is consistent with the definition in PHIPA and its regulation. The policy states that secure disposal means that records are disposed of in such a manner that their reconstruction is not reasonably foreseeable in the circumstances.

The ICES Data Management Standard, Information Media Destruction SOP and Destruction of ICES Data SOP identify the precise methods for the secure disposal of records of personal health information in paper and electronic format, including various media. Records on paper must be disposed of by crosscut shredding or deposited into approved shredding bins for secure disposal by a third party service provider. Mobile devices or media must be wiped using secure overwrite utility software. Unserviceable mobile media must be physically destroyed by burning platters, degaussing or shredding to prevent reconstruction. Records on ICES servers must be permanently deleted. The policy requires that these secure disposal methods be consistent with PHIPA and its regulation, with IPC orders, including Order H0-001 and Order HO-006, and with IPC guidelines, fact sheets and best practices, including *Fact Sheet 10: Secure Destruction of Personal Information.*

The standard and the two SOPs address the secure retention of records of personal health information pending their secure disposal. Records intended for disposal must be physically segregated from records intended for recycling, stored in designated areas, and retained in clearly marked cabinets, safes or bins. Records on paper, if not shredded by ICES staff, must be stored in designated bins distributed throughout ICES' premises until they are securely disposed of by a third party service provider. Shredding bins are clearly marked, opaque and locked and their contents cannot be accessed by ICES staff. ICES' Facilities Manager is responsible for ensuring the security of paper bins pending secure disposal of their contents. Mobile media intended for disposal must be clearly marked and stored in a locked room in a clearly marked safe until they are securely disposed of. ICES' IT Service Lead is responsible for ensuring the media is securely retained pending its secure disposal.

<u>Disposal by a Designated ICES Agent, Not a Third Party Service Provider</u>

Under the Destruction of ICES Data SOP, where a designated ICES agent, and not a third party service provider, is responsible for disposal of records of personal health information, the disposal must be carried out or coordinated by an ICES Data Convenator or assigned IT staff. The circumstances under which disposal is performed by an ICES Data Convenantor include physical destruction of CD-Rs and removal of electronic records on laptops and ICES systems. When records are contained on mobile media or devices other than CD-Rs or laptops, an ICES Data Convernator must submit a Track-IT ticket to request disposal by assigned IT staff. Specific responsibilities of ICES Data Covenantors and IT staff with respect to secure disposal, including tracking of destruction dates and storage of certificates of destruction, are detailed in the Destruction of ICES Data SOP and Information Media Destruction SOP.

Under the ICES Data Management Standard, personal health information with direct personal identifiers is retained only temporarily until data quality issues have been resolved and is then securely destroyed by an ICES-approved method.

The SOPs require ICES Data Convenantors to provide certificates of destruction to the data custodian no later than a specified time following the secure disposal. The certificates of destruction are required to:

- Identify the records of personal health information to be securely disposed of;
- Confirm the secure disposal of the records of personal health information;
- Set out the date, time and method of secure disposal employed; and
- Bear the name and signature of the agent(s) who performed the secure disposal.

<u>Disposal by a Third Party Service Provider</u>

ICES' Privacy Impact Assessment Policy addresses the selection and management of any third party service provider contracted to securely dispose of records of personal health information on ICES' behalf. The policy stipulates that a privacy impact assessment must be conducted prior to establishing any such service relationship. The ICES PIA Form - Service Provider, completion of which is the responsibility of an ICES Privacy Officer, has been defined for this purpose. The form is designed to:

- Establish and detail an appropriately secure procedure and method for the transfer of records of personal health information to the third party service provider, which meet the requirements of ICES' own policies and procedures for secure transfer;
- Identify conditions for transfer; and
- Ensure the services are appropriately documented in a service level agreement that meets or exceeds appropriate mandatory privacy content, and which must be reviewed and approved by an ICES Privacy Officer prior to transfer.

The ICES Data Management Policy addresses the documentation that must be maintained in relation to the transfer of records of personal health information to a third party service for secure disposal. In particular, the agent responsible for ensuring the secure transfer, either the Director IT or delegate in the case of personal health information on mobile media or the Facilities Manager in the case of personal health information on paper, is required to document the date, time and mode of transfer, and maintain a repository of written confirmations received from the third party upon receipt of the records and a detailed inventory of the personal health information transferred for secure disposal.

Currently at ICES secure disposal of paper and mobile media by a third party service provider is done onsite only and transfer is not required. For disposal of paper the Information Media Destruction SOP requires ICES' receptionist to track the date the third party service provider was onsite to perform the disposal and the date the certificate of destruction was received. The receptionist must provide the certificate of destruction to the Facilities Manager for storage in the Manager's office. For disposal of mobile media, the IT Service Lead is responsible for tracking and filing copies of certificates of destruction on a restricted electronic folder. Where a third party service provider does not provide a certificate of destruction within the required timeframe, the Facilities Manager or IT Service Lead, as applicable, must follow up to ensure the certificate is provided.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

9. Policy & Procedures Relating to Passwords

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Password Policy	Implemented
	b. Security Incident Management Policy	Implemented
	c. Security Audit Policy	Implemented
	d. Discipline & Corrective Action Policy	Implemented
Comments	Temporary passwords for UNIX accounts, through which agents access data for analysis, will soon be programmed to expire immediately after first account login in accordance with ICES' Password Policy. This will be achieved through a systems upgrade projected for no later than December 31, 2014.	

DESCRIPTION

ICES' Password Policy addresses passwords for authentication and access to information systems, technologies, equipment, resources, applications and programs. The policy applies to all agents who access computing systems operated by ICES, including any default user account on systems or software owned, licensed or managed by ICES, whether such access is from an ICES-owned or personal computer.

The policy is consistent with orders, guidelines, fact sheets and best practices issued by the IPC, and industry standards. The policy defines:

- Minimum and maximum password length;
- Password composition, which must be a combination of upper and lower case letters, numbers and alphanumeric characters;
- Restrictions on re-use of prior passwords;
- Timed automated expiry and frequency of password change;
- Consequences following a defined number of failed login attempts, including account lockout;
- Imposition of system-wide password-protected screen saver after a defined period of inactivity; and
- Administrative, technical and physical safeguarding rules for agents to maintain confidentiality of passwords, including specific requirements to keep passwords private and secure, change passwords immediately if suspected they have become known to others, and to refrain from writing down, displaying, concealing,

hinting at, providing, sharing or otherwise making passwords known to others.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

10. Policy & Procedure for Maintaining & Reviewing System Control & Audit Logs

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. System Control & Audit Log Policy	Implemented
	b. System Control & Audit Log SOP	Implemented
	c. System Control & Audit Log Standard	Implemented
	d. Security Audit SOP	Implemented
	e. Security Audit Policy	Implemented
	f. Privacy Incident Management Policy	Implemented
	g. Security Incident Management Policy	Implemented
	h. Discipline & Corrective Action Policy	Implemented
Comments	ICES' information systems will soon be configured to log automatically access to personal health information and related actions identified below. This will be achieved through a systems upgrade with a projected implementation date of no later than December 31, 2014.	

DESCRIPTION

ICES' System Control and Audit Log Policy provides for the creation, maintenance and ongoing review of system control and audit logs that are aligned with industry standards over time and commensurate with the amount and sensitivity of the personal health information maintained, the number and nature of agents with access, and the associated risks.

ICES' System Control and Audit Log SOP requires ICES' information systems involving personal health information, including technologies, applications and programs, to be configured to log access, use, modification and disclosure. The types of events that require auditing and the nature and scope of the information to be captured in the system control and audit logs are set out in ICES' System Control and Audit Log Standard. These logs are required to contain the date and time personal health information is accessed and access is disconnected, as well as the user and computer identifiers, type of action performed such as retrieval, creation or deletion, date and time of the action, and any changes to values. Under the SOP, the Security Lead, or an ICES Security Officer assigned by the Security Lead, is responsible for ensuring required audits are conducted and the required information is captured in these logs, including its nature and scope.

The immutability of these logs is ensured through provisions in ICES' System Control and Audit Log Policy and reinforced by the SOP, which also identifies the procedures for ensuring logs are protected from unauthorized access and assigns responsibility for protecting logs to the System/Database Administrator. The SOP requires the System/Database Administrator to retain these logs and identifies their location and the retention period. Review of these logs by the Security Lead, or an ICES Security Officer assigned by the Security Lead, as well as by the System Information and Event Management Administrator and under what circumstances, and the review frequency and process are also defined in the policy and SOP. These designated reviewers of logs are required to provide notification, at the first reasonable opportunity, of any privacy incidents or breaches under ICES' Privacy Incident Management Policy or security incidents or breaches under ICES' Security Incident Management Policy. The relationship between the SOP and ICES' Privacy Incident Management Policy and ICES' Security Incident Management Policy is identified in the SOP.

ICES' System Control and Audit Log SOP assigns responsibility to the Security Lead, or an ICES Security Officer assigned by the Security Lead, for addressing findings within specified timelines and monitoring to ensure the findings have been addressed, and identifies related documentary requirements. Also addressed in the SOP is how

findings will be communicated by the applicable ICES Security Officer to the Manager or Director of IT and the timeframes for communication. The SOP assigns responsibility to the Security Lead, or an ICES Security Officer assigned by the Security Lead, for tracking the findings using the Security Incidents Log and monitoring to ensure the findings and any remediation steps have been addressed.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources, in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

11. Policy & Procedures for Patch Management

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Patch Management Policy	Implemented
	b. Information Technology Change Management SOP	Implemented
	c. Security Incident Management Policy	Implemented
	d. Security Audit Policy	Implemented
	e. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Patch Management Policy addresses the implementation of patch management at ICES. Under the policy, ICES' IT Manager must assign responsibility to specific IT staff for monitoring the availability of patches and related patch management tasks. The policy identifies the frequency of monitoring and the associated procedure that must be followed. The policy requires assigned IT staff to determine whether and when to implement a patch, based upon criteria that are set out in the policy, and further identifies the process that must be followed in this regard. When it is determined a patch should not be implemented, the policy requires the assigned IT staff to document a description of the patch, the date it became available, the severity level, the information system to which the patch relates and the rationale for not implementing the patch. When it is determined a patch should be implemented, the policy identifies the priority and required timeframe for implementation based upon the severity level of the patch. The process for patch implementation is set out in ICES' Information Technology Change Management SOP, which identifies the agent responsible for implementation (i.e. the assigned Change Implementer), the circumstances in which patches must be tested, the timeframe for testing and the required documentation and responsibility for testing.

The policy and SOP address the documentation that is required to be maintained with respect to patches that have been implemented and assigns responsibility for its maintenance to the designated IT staff. Minimum documentation content includes a description of the patch and its severity level, the date it became available, the system to which the patch relates, implementation date, agent responsible for implementation, test date, agents responsible for testing, and the test results.

Compliance with the above policy and its procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

12. Policy & Procedures Related to Change Management

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Information Technology Change Management Policy	Implemented
	b. Information Technology Change Management SOP	Implemented
	c. Change Request Form	Implemented
	d. Security Incident Management Policy	Implemented
	e. Security Audit Policy	Implemented
	f. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Information Technology Change Management Policy and associated procedures address the receipt, review and approval or denial of requests to change the operational environment of ICES.

The policy and procedures address:

- The request process, requirements and associated roles and responsibilities;
- Receipt, review and approval or denial of change requests by an established Change Advisory Board comprised of agents from ICES' Information Technology, ICES' Security Office and ICES' Privacy Office;
- The documentation that must be completed (i.e. a Change Request Form) by the requestor and submitted to the Change Advisory Board for review and approval;
- Minimum documentation content requirements, which are defined in the Change Request Form, including the requestor's name, the change requested, the date the change was requested, the rationale/need for the change, the impact and, where applicable, the rationale for a decision not to implement the change;
- Criteria and process for determining whether to approve or deny requests;
- The manner in which decisions must be documented, and the method and format for communicating decisions to the requestor;
- Responsibility of the change manager and Change Advisory Board for prioritizing and determining timelines for implementation of approved changes, and associated documentation;
- The process and responsibility of the change implementer for implementing approved changes, and associated documentation;
- Responsibility of the change manager for maintaining and updating documentation of changes that have been implemented, including a description of the change requested, the requestor's name, the change requested, the date the change was requested, the change priority, the date the change was implemented, responsibility of the change implementer for implementation, the date the change was tested, responsibility of the change implementer for testing, and the test results; and
- The circumstances in which changes must be tested by the change implementer and associated time frame, procedures and documentation.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

13. Policy & Procedures for Back-Up & Recovery of Records of Personal Health Information

APPLICATION	
Fully applicable ☒	Qualified application (*explain*)

EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Data Backup Policy	Implemented
	b. Privacy Impact Assessment Policy	Implemented
	c. ICES Data Management Policy	Implemented
	d. ICES Data Management Standard	Implemented
	e. ICES PIA Form – Service Provider	Implemented
	f. Privacy Audit and Monitoring Policy	Implemented
	g. Privacy Incident Management Policy	Implemented

DESCRIPTION

ICES' Data Backup Policy addresses the backup and recovery of records of personal health information. The policy specifically addresses:

- Types of backup storage devices used;
- Frequency with which personal health information is backed up;
- Process and requirements for backup and recovery;
- The need for the availability of backed-up records and the circumstances under which backed-up records will be made available;
- Testing of backups and recovery procedures, and testing frequency and process;
- Required documentation for backup, recovery and testing, the contents of which are defined in the applicable document or log;
- Requirement to ensure backup storage devices are securely retained in a restricted area within ICES and timeframe for retention;
- Responsibility for all of the above, which is assigned to ICES' Director, IT and designated system administrators.

The policy is required to be in compliance with ICES' policies and procedures for the secure retention of records of personal health information, including the ICES Data Management Policy and the ICES Data Management Standard.

Retention by a Third Party Service Provider

ICES' Privacy Impact Assessment Policy addresses the selection and management of any third party service provider contracted to retain records of personal health information on ICES' behalf. This includes any third party service provider contracted to retain backed-up records. The policy stipulates that a privacy impact assessment must be conducted prior to establishing any such service relationship. The ICES PIA Form - Service Provider, completion of which is the responsibility of an ICES Privacy Officer, has been defined for this purpose. The form is designed to:

- Establish and detail an appropriately secure procedure and method for the transfer of backed-up records of personal health information to the third party service provider and the retrieval of records from the third party service provider, which meet the requirements of ICES' own policies and procedures for secure transfer;
- Identify conditions for transfer and retrieval; and
- Require that a written agreement be executed with the third party service provider that meets or exceeds appropriate mandatory privacy content, and which must be reviewed and approved by an ICES Privacy Officer prior to transfer.

The ICES Data Management Policy addresses the documentation that must be maintained in relation to the transfer of backed-up records of personal health information to a third party service provider for retention. In particular, the agent responsible for ensuring the secure transfer - namely the Director, IT or delegate, as applicable - is required to document the date, time and mode of transfer and maintain a repository of written confirmations received from the third party service provider upon receipt of the records and a detailed inventory of the personal health information being securely retained by, or retrieved from, the third party service provider.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are

subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

14. Policy & Procedures on the Acceptable Use of Technology

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Acceptable Use Policy	Implemented
	b. Information Technology Change Management Policy	Implemented
	c. Information Technology Change Management SOP	Implemented
	d. Track-IT System	Implemented
	e. Personnel IT Equipment Request Form	Implemented
	f. Security Incident Management Policy	Implemented
	g. Security Audit Policy	Implemented
	h. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Acceptable Use Policy outlines the acceptable use of ICES' information systems. The policy applies whether or not equipment involved is owned, leased or operated by ICES.

The policy defines uses that are permitted, uses that are prohibited and uses that are subject to prior approval. The policy does not detail the process for making or approving a request for any standard equipment, applications or programs. Requests for any of these are simply handled, and documented, through ICES' IT ticket system. The requestor must complete a Personnel IT Equipment Request Form, obtain the signature of his/her supervisor and, where applicable, the signatures of the Director of Finance and the relevant Senior Director, and submit the form through a Track-IT ticket to ICES' HelpDesk for processing by the assigned IT staff. The form requires, among other details, justification for the need of the equipment, application or program.

If the equipment, application or program falls outside of ICES' standard list, the process for making and approving a request is set out in ICES' Information Technology Change Management SOP. The requestor is required to complete a Change Request Form, the required details of which are defined in the form. This form must be reviewed by a designated Change Advisory Board consisting of agents from ICES' Information Technology, ICES' Security Office and ICES' Privacy Office. The SOP identifies the criteria for approving or denying the request, as well as how decisions by the Change Advisory Board must be documented, including the reasons for the decision and any conditions on approval with which the requestor must comply, and how those decisions must be communicated to the requestor.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

15. Policy & Procedures In Respect of Security Audits

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Audit Policy	Implemented
	b. Security Audit SOP	Implemented
	c. Security Audit Log	Implemented
	d. Threat Risk Assessment Log	Implemented
	e. Security Risk Assessment Log	Implemented
	f. Security Incident Management Policy	Implemented
	g. Privacy Incident Management Policy	Implemented

DESCRIPTION

ICES' Security Audit Policy and associated procedures identify the purpose and types of security audits that are required to be conducted. The types of security audits provided for include audits to assess compliance with ICES' security policies, procedures and practices, threat and risk assessments, security reviews, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs. The policy and ICES' Security Audit SOP identify the roles of agents delegated day-to-day authority to manage ICES' security program. Under the policy and SOP, ICES' Security Lead or designate, the Manager, IT and the Senior Director, Data Platform are each responsible for the management of different audit requirements.

For each type of security audit, the policies and procedures identify:

- Nature (e.g. document reviews) and scope of audit;
- Criteria for selecting subject matter of audit (where applicable);
- Responsibility of ICES' Security Lead or a ICES Security Officer assigned by the Security Lead for conduct of audit;
- Frequency or circumstances for conduct of audit;
- Audit process;
- Notification (where relevant to the audit type), including its nature and content and to whom notification must be provided;
- Documentation that must be completed in undertaking and at the conclusion of the audit, its content and recipients; and
- The audit schedule.

The procedures also address:

- Handling of audit recommendations and ensuring they are addressed within an established timeline;
- Communication of audit findings, including recommendations, to whom, including ICES' Chief Executive Officer, and the format and timeframe for communication;
- Maintenance of a log to track recommendations and timelines for addressing them;
- Retention and location of supporting documentation; and
- Responsibility of ICES' Security Lead or a Security Officer assigned by the Security Lead for carrying out all of the above.

Agents of ICES, including any auditor, have a duty to notify, at the first reasonable opportunity, an ICES Security Officer of any detected or suspected security breach under ICES' Security Incident Management Policy and an ICES Privacy Officer of any detected or suspected privacy breach under ICES' Privacy Incident Management Policy.

16. Log of Security Audits

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Audit Log	Implemented
	b. Threat Risk Assessment Log	Implemented
	c. Security Risk Assessment Log	Implemented

DESCRIPTION

ICES has developed logs of security audits and assessments that capture:

- Nature and type of audit;
- Completion date;
- Responsible auditor;
- Recommendations arising from the audit;
- Agent responsible for addressing the recommendations;
- Date each recommendation was or is expected to be addressed; and
- The manner in which each recommendation was or is expected to be addressed.

17. Policy & Procedures for Information Security Breach Management

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Incident Management Policy	Implemented
	b. Security Incident Management SOP	Implemented
	c. Security Incident Report Template	Implemented
	d. Security Incident Log	Implemented
	e. Privacy Incident Management Policy	Implemented
	f. Privacy Incident Management Procedure	Implemented

DESCRIPTION

ICES' Security Incident Management Policy and associated procedures address the identification, reporting, containment, notification, investigation and remediation of information security breaches. The meaning of information security breach is defined in the policy and includes a contravention of ICES' security policies.

The policy imposes a mandatory requirement for agents to provide notification, in writing or verbally, of any actual or suspected security breach at the first reasonable opportunity. Under the policy an agent must report actual or suspected beaches to ICES' Security Lead (the Incident Response Leader) or ICES HelpDesk, but at ICES' Satellite Sites, to the local ICES Privacy Officer. Contact information is identified, as is the timeframe for notification and the required information. Also addressed is the documentation that must be completed for notification, the content of which is defined in a report template, and responsibility of the Security Lead for its generation, and the recipient.

ICES' Security Incident Management SOP requires that the Security Lead or Director, IT determine whether a security breach has occurred and the extent of the breach. Under the SOP, notification of the Chief Privacy Officer is required when a security breach is suspected to involve personal health information, or when it is suspected that a breach reported as a security breach is instead, or is also, a privacy breach. The Chief Privacy Officer shall confirm whether a privacy breach has occurred. The policy and SOP address the circumstances under which the Senior Director, Data Platform is required to notify the Chief Executive Officer, the timeframe for and method of reporting and the required information to be reported.

The SOP addresses the requirement for immediate containment and assigns responsibility to the Security Lead. Also addressed is the process for containment, including the documentation that must be completed, its content and responsibility of the Security Lead for its generation. The SOP outlines reasonable steps to protect against further similar security breaches. The SOP defines the process to be followed by the Security Lead for reviewing the

containment measures implemented and determining if further measures are needed, and identifies the documentation to be completed, its content and the recipients.

ICES' Privacy Incident Management Policy requires that ICES fulfill any notification obligations, at the first reasonable opportunity, when personal health information provided by a third party is or is believed to be stolen, lost or accessed by unauthorized persons. The Chief Privacy Officer is responsible for determining the content of the notice and how and by whom it will be made. At a minimum, where notice is required, it must address the nature of the information involved, the extent of the incident or breach, and the measures that have been or will be taken to contain it, including investigation and remediation. The Chief Privacy Officer is responsible for evaluating whether and how to notify other parties and give notice. At a minimum, notice is given whenever required pursuant to the agreement with the health information custodian or other organization.

The SOP identifies the process that must be followed by the Security Lead in investigating security breaches, and the nature and scope of the investigations. The SOP further specifies the role of the Security Lead, and the Chief Privacy Officer, who are the agents that have been delegated day-to-day authority to manage the security and privacy programs, respectively. Also addressed is the documentation that must be completed, its content, responsibility of the Security Lead for its generation, and the recipients. The SOP makes the Security Lead responsible for assigning other agents to address any recommendations, establishing timelines and monitoring to ensure the recommendations are implemented. The SOP identifies the related documentation that must be completed by the Security Lead, its content and the recipients. The SOP addresses the method required to communicate the findings of investigations, including any recommendations and their status, responsibility of the Security Lead or Director, IT for communicating findings, as well as communication timelines and to whom findings must be communicated, including the Senior Director, Data Platform and Chief Executive Officer.

The SOP requires that a log of security breaches be maintained and assigns responsibility to the Security Lead for its maintenance and for tracking the implementation of recommendations. The Security Lead is also responsible for compiling documentation related to identification, reporting, containment, notification, investigation and remediation of security breaches, and for retaining the documentation in a designated folder.

Compliance with the above policies and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policies or procedures in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources, in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

18. Log of Information Security Breaches

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Incident Log	Implemented
DESCRIPTION		

ICES has defined a log, which captures:

- Date of the information security breach;
- Date the breach was identified or suspected;
- Nature of the personal health information, if any, involved;
- Nature and extent of the information security breach;
- Containment date and measures;
- Date of any notifications to the health information custodian or other organization;
- Investigation complete date;
- Investigator name; and
- Resulting recommendations and action plans with responsible agents and date each recommendation was addressed.

Part 3 – Human Resources Documentation

1. Policy & Procedures for Privacy Training & Awareness

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Awareness Policy	Implemented
	b. Privacy Awareness Procedures	Implemented
	c. Privacy Awareness Log	Implemented
	d. Privacy Awareness Attendance Sheet	Implemented
	e. Privacy Awareness Requirements Table	Implemented
	f. Privacy Consultation Log	Implemented
	g. Privacy Audit & Monitoring Policy	Implemented
	h. Discipline & Corrective Action	Implemented
	i. Privacy Incident Management Policy	Implemented
Comments	To this point, awareness activities have been ongoing but have not included training per se. This will very shortly change. ICES is actively developing an e-learning module, which will be mandatory for all agents and renewed annually. Procedures to support the new e-learning requirements, including tracking, required documentation, and associated roles and responsibilities are also being developed with a projected implementation timeline of early 2015.	

DESCRIPTION

ICES' Privacy Awareness Policy requires agents to comply with requirements established by the Chief Privacy Officer to create and sustain awareness of ICES' privacy policies and procedures. At a minimum, these requirements must include completion of initial privacy orientation prior to receiving access to personal health information as well as participation in ongoing privacy awareness initiatives, including annual privacy training, which are devised by the Chief Privacy Officer to meet the objectives of the policy.

Associated procedures assign responsibility to an ICES Privacy Officer for delivering initial privacy orientation. Responsibility for notifying ICES' Privacy Office Administrator to schedule orientation depends on the role of the incoming agent and is set out in ICES' Privacy Awareness Requirements Table, which is published and available for ongoing reference within ICES on the ICES intranet. Notification must be provided by email at the commencement of the agent's employment or contractual relationship with ICES.

The content of the initial privacy orientation is prescribed. Under the policy, the initial orientation must address:

- ICES' responsibilities arising from its designation under s. 45(3) of PHIPA;
- Types and sources of personal health information collected by ICES;
- Purposes for which ICES collects personal health information, and associated legal authorities and obligations;
- Limits on access to and use of personal health information at ICES;
- Responsibility and the procedure for handling privacy inquiries and complaints;
- Responsibility and the procedure for handling requests to disclose personal health information;
- An overview of ICES' key privacy policies and procedures, as well as administrative, technical and physical safeguards to protect personal health information against theft, loss and unauthorized use, copying, modification or disposal, and agents' role and responsibilities in upholding them;
- An overview of ICES' Privacy Incident Management Policy and the duties and responsibilities of agents in identifying, reporting, containing and participating in the investigation and remediation of privacy incidents and breaches (Duties include a mandatory requirement to provide notification of privacy incidents at the first reasonable opportunity and to comply with any instructions to facilitate their containment, investigation and remediation.);
- Consequences of breach;
- A description of ICES' privacy program and its management; and
- An overview of the applicable ICES Confidentiality Agreement, its purpose and key provisions.

The procedures require that the ICES Privacy Officer assigned to deliver privacy orientation verify attendance on the Privacy Awareness Attendance Sheet, the required content of which is defined in the attendance sheet, and then forward the attendance sheet to the Privacy Office Administrator. Referring to the attendance sheet, the Privacy

Office Administrator records attendance in the Privacy Awareness Log, the ongoing maintenance of which is specifically required by the policy and procedure. The Privacy Office Administrator is responsible for filing the attendance sheet. Where the attendance sheet shows an agent failed to attend privacy orientation, the Privacy Office Administrator must, on the same day, follow up with the agent to reschedule orientation.

To this point, privacy awareness activities have been ongoing but have not included training per se. This will very shortly change. ICES is actively developing an e-learning module, which will be mandatory for all agents and renewed annually. Procedures to support the new e-learning requirements, including tracking and associated roles and responsibilities are also being developed.

The policy also stipulates that ICES' privacy awareness program include role-based information and training and mechanisms to sustain awareness and communicate significant changes. Significant changes include introduction of new privacy policies and procedures and changes to them arising from the results of privacy impact assessments, privacy audits and monitoring, and privacy inquiries and complaints. The policy provides that mechanisms to sustain awareness will include awareness initiatives, which may be delivered as required by the assigned Privacy Officer at ICES staff meetings or by other means, and may include testing.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

2. Log of Attendance at Initial Privacy Orientation & Ongoing Privacy Training

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Awareness Log	Implemented
Comments	Historically, ICES has not tracked attendance of ongoing training. We have now established and implemented a policy that requires this.	
DESCRIPTION		
ICES has developed and maintains a Privacy Awareness Log to track attendance at initial privacy orientation. The log includes the individual's name and attendance date. Use of the log is required under ICES' Privacy Awareness Procedures. To this point, ongoing awareness activities have been carried out and have been tracked. But, because they have not to date included training per se, this has not taken the form of attendance tracking specifically. This will very shortly change when privacy e-learning is launched. That program, which will be mandatory for all agents and subject to annual renewal, will include tracking to monitor and enforce compliance.		

3. Policy & Procedures for Security Training & Awareness

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Training & Awareness Policy	Implemented
	b. Security Training - Content Management SOP	Implemented
	c. Security Training - Delivery Method SOP	Implemented
	d. Initial Security Orientation Attendance Sheet	Implemented
	e. Security Training & Awareness Log	Implemented

	f. Discipline & Corrective Action Policy	Implemented
	g. Security Audit Policy	Implemented
	h. Security Audit SOP	Implemented
	i. Security Incident Management Policy	Implemented

DESCRIPTION

ICES' Security Training and Awareness Policy and associated procedures require agents to attend initial security orientation prior to receiving access to personal health information, and to attend ongoing security training on an annual basis.

Procedures are defined to support the delivery of security orientation and ongoing security training. The procedures assign responsibility to ICES' Security Lead for preparing and delivering security orientation and ongoing security training. The procedures require a Human Resources Associate or an agent's supervisor, as applicable, to notify ICES' Security Lead to schedule orientation for new agents and affiliated persons. Notification must be provided by email at the commencement of the agent's employment or contractual relationship with ICES.

The procedures specify the standard information to be included in security orientation:

- An overview of ICES' key security policies and procedures, and agents' role and responsibilities in upholding them;
- Consequences of breach of the security policies and procedures;
- A description of ICES' security program, including key activities of the program and the agents that have been delegated day-to-day authority to manage the security program;
- ICES' administrative, technical and physical safeguards for protecting information against theft, loss and unauthorized use, disclosure, copying, modification or disposal;
- The duties and responsibilities of agents in upholding the administrative, technical and physical safeguards; and
- An explanation of ICES' policy and procedures for managing security breaches, and agents' duties and responsibilities in identifying, reporting, containing and participating in the investigation and remediation of information security breaches. (Duties include a mandatory requirement to provide notification of actual or suspected security breaches at the first reasonable opportunity and to comply with any instructions to facilitate their containment, investigation and remediation.)

Under the procedures, ongoing security training includes role-based training, and will address new security policies and procedures and recommendations from the results of privacy impact assessments, security breach investigations, and security audits including threat risk assessments, security reviews or assessments, vulnerability assessments, penetration testing, ethical hacks and reviews of system control and audit logs.

The procedures require that the Security Lead verify attendance at initial orientation on the Security Orientation Attendance Sheet, recording the agent's name and date orientation was delivered. Referring to the attendance sheet, the Security Lead must record attendance in the Security Training Attendance Log, and then forward a copy of the attendance sheet to ICES Helpdesk, where IT staff are required to confirm an agent attended security orientation prior to issuing access to ICES systems. Where an agent fails to attend security orientation, the Security Lead must follow up with the agent on the same day to reschedule orientation. The procedures also require the Security Lead to track completion of annual security training in the Security Training Attendance Log, recording the agent's name and the date training was completed. The procedures require agents to complete annual security training before a specified date, and for any agents who fail to do so, the Security Lead must notify ICES Helpdesk to remove their access to ICES systems until they have completed training. The Security Lead is responsible for retaining the documentation and log used for tracking attendance at initial security orientation and ongoing security training in a designated electronic folder.

The procedures identify other mechanisms to increase security awareness, including monthly security tips prepared by the Security Lead and disseminated through ICES staff communications.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Security Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Security Officer and an audit schedule established under ICES' Security Audit Policy.

4. Log of Attendance at Initial Security Orientation & Ongoing Security Training

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Initial Security Orientation Attendance Sheet	Approved
	b. Security Training & Awareness Log	Approved
DESCRIPTION		
ICES requires that a log be maintained to track completion of initial security orientation and ongoing security training. The log identifies the agent's name and the dates initial orientation and ongoing security training were completed.		

5. Policy & Procedures for the Execution of Confidentiality Agreements by Agents

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Awareness Policy	Implemented
	b. Privacy Awareness Procedures	Implemented
	c. Privacy Awareness Log	Implemented
	d. Privacy Awareness Requirements Table	Implemented
	e. Privacy Awareness Attendance Sheet	Implemented
	f. Privacy Audit & Monitoring Policy	Implemented
	g. Discipline & Corrective Action Policy	Implemented
DESCRIPTION		

ICES' Privacy Awareness Policy requires agents to sign a confidentiality agreement prior to being given access to data including personal health information and annually thereafter. Associated procedures and responsibilities are defined to support the execution of agreements. Under the procedures, a designated ICES agent must notify the Privacy Office Administrator to schedule privacy orientation and ensure an agreement is signed. Responsibility for providing notification depends on the role of the incoming agent and is set out in ICES' Privacy Awareness Requirements Table, which is published and available for ongoing reference within ICES on the ICES intranet. Notification, whether provided by ICES' Lead Program Administrator, a principal investigator or other delegated person or through ICES' onboarding system, must be provided by email at the commencement of the agent's employment or contractual relationship with ICES. Under the procedures, the ICES Privacy Officer assigned to deliver initial privacy orientation must, at the time, obtain a signed agreement. The ICES Privacy Officer must provide the signed agreement to the Privacy Officer Administrator, who is responsible for filing the agreement and tracking it in the Privacy Awareness Log. Where an agent fails to attend orientation and sign an agreement, the Privacy Office Administrator must, on the same day, contact the agent to reschedule orientation. An ICES Privacy Officer is required to obtain a signed agreement at the time of delivering orientation.

The procedures set out the specified time each year when the Privacy Office Administrator must send out confidentiality agreement renewal notifications and the process to be followed where an agent fails to renew his/her agreement by the specified deadline.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources, in consultation with ICES' Chief Privacy Officer under ICES' Discipline and Corrective Action Policy. Compliance is subject to annual audit by an ICES Privacy Officer and an audit schedule established under ICES' Privacy Audit and Monitoring Policy.

6. Template Confidentiality Agreement with Agents

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Confidentiality Agreement (General)	Implemented
	b. ICES Confidentiality Agreement (Data Covenantor)	Implemented
	c. ICES Confidentiality Agreement (Abstractor)	Implemented
	d. ICES Collaborating Researcher NDA	Implemented

DESCRIPTION

ICES has defined a suite of template confidentiality agreements, which are required for all agents under ICES' Privacy Awareness Policy.

General Provisions

The templates describe ICES' status as a prescribed entity under PHIPA and its duties and responsibilities arising from that status. The templates state that the individuals executing the agreements are agents of ICES and outline the responsibilities that arise from this. These specifically include agents' duty to comply with PHIPA and its regulation in relation to ICES and the terms of the confidentiality agreement and any amendments to it. Agents are also required to agree to read and comply with the privacy and security policies and procedures ICES has implemented as a prescribed entity and any amendments to them. They include a definition of personal health information that is consistent with PHIPA and its regulation.

Obligations with Respect to Collection, Use and Disclosure of Personal Health Information

The templates identify the purposes for which agents are permitted to collect, use and disclose personal health information on behalf of ICES and any associated conditions, limitations and restrictions. For example, ICES Abstractors are required to use any ICES equipment issued to them and abide by ICES instructions when they collect personal health information. ICES Data Covenantors, who collect and destroy personal health information, must do so in accordance with data sharing agreements. All versions prohibit agents from using personal health information except in accordance with the agreement or as required by law, more personal health information than is reasonably required to, or any personal information if other information will, serve the purpose. (Disclosure is permitted only in the template for ICES Data Covenantors.)

Termination of the Contractual or Employment Relationship

The templates stipulate that agents must return all property of ICES, including records of personal health information, and all identification cards, access cards and/or keys, by the end of the last day of their relationship with ICES. In all cases, in accordance with ICES' Termination of Employment/Resignation and Discharge Policy, the templates stipulate that these be personally delivered to the agent's ICES supervisor.

Notification

In accordance with ICES' Privacy Incident Management Policy and ICES' Security Incident Management Policy, the templates require agents to notify ICES immediately of any breach or suspected breach of the agreement or ICES' privacy and security policies and procedures, by the agent or any other party.

Consequences of Breach and Monitoring Compliance

The templates explicitly provide that failure to comply is grounds for discipline and may lead to termination of the agent's relationship with ICES. All reserve a right of audit by ICES, which agents must formally acknowledge. They acknowledge that ICES may request and inspect equipment used by them, logs and documents of any kind generated as result of their activities, and make such other inquiries as are reasonably required to confirm the agent's compliance with the agreement.

7. Log of Executed Confidentiality Agreements with Agents

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Awareness Log	Implemented

DESCRIPTION

ICES has defined a log to track the execution of all confidentiality agreements. Under ICES' Privacy Office Awareness and Training Procedures, maintenance of the log is required and is the responsibility of the Privacy Office Administrator. Information captured in the log includes:

- Agent name;
- Date their employment or contractual relationship commenced;
- Date initial agreement was signed; and
- Except for ICES Abstractors, date their annual renewal was signed.

ICES Abstractors are engaged, and are required to sign an ICES confidentiality agreement, on a short-term, project-by-project basis. Those agreements are therefore not subject to annual renewal.

8. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Privacy Program

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Detailed Position Description – Chief Privacy Officer	Implemented
	b. Privacy Audit and Monitoring Policy	Implemented
	c. Privacy Impact Assessment Policy	Implemented

DESCRIPTION

ICES has developed a job description for the position of Chief Privacy Officer. The job description gives the CPO authority to manage ICES' privacy program, reporting directly to ICES' Chief Executive Officer. The job description sets out the more detailed responsibilities and obligations of the CPO, which include:

- Developing, implementing, reviewing and amending privacy policies, procedures and practices;
- Ensuring compliance with the privacy policies, procedures and practices implemented;
- Ensuring transparency of the privacy policies, procedures and practices implemented;
- Facilitating compliance with PHIPA and its regulation;
- Ensuring employees and agents are aware of PHIPA and its regulation and their duties under it;
- Ensuring employees and agents are aware of, and appropriately informed of their duties under, the privacy policies, procedures and practices implemented by ICES in support of its designation as a prescribed entity;
- Directing, delivering and ensuring the delivery of the initial privacy orientation and ongoing privacy training, and fostering a culture of privacy;
- Receiving, documenting, tracking and investigating, remediating and responding to privacy complaints in accordance with IPC requirements;
- Receiving and responding to privacy inquiries in accordance with IPC requirements;
- Receiving, documenting, tracking, investigating and remediating privacy breaches and suspected privacy breaches in accordance with IPC requirements; and
- Conducting privacy audits in accordance with IPC requirements.

9. Job Description for the Position(s) Delegated Day-to-Day Authority to Manage the Security Program

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Position Description – Security Lead	Implemented
	b. ICES Position Description – Security Analyst	Implemented
	c. Security Incident Management Policy	Implemented
	d. Security Training & Awareness Policy	Implemented

DESCRIPTION

ICES has developed job descriptions for the positions delegated day-to-day authority to manage the security program. Both the Security Lead and Security Analyst report to ICES' Senior Director, Data Platform, who, in turn, reports to the Chief Executive Officer. The combined obligations and responsibilities of the Security Lead and Security Analyst include:

- Responding to security incidents; and
- Performing auditing activities.

Although not explicitly stated in the job description, the Security Lead:

- Develops and implements security policies and procedures, and ensures compliance with them; and
- Provides security awareness under ICES' Security Training and Awareness Policy, which includes building awareness of security policies and procedures and individuals' obligations arising from them, and delivering initial and ongoing security training.

10. Policy & Procedures for Termination or Cessation of the Employment or Contractual Relationship

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Termination of Employment/Resignation & Discharge Policy	Implemented
	b. Termination of Employment/Resignation & Discharge Procedure	Implemented
	c. Policy Framework & Governance Policy	Implemented
	d. Discipline & Corrective Action Policy	Implemented

DESCRIPTION

ICES' Termination of Employment/Resignation and Discharge Policy and associated procedures require agents to provide written notice of resignation to their supervisor before a specified time and their supervisors to, in turn, notify a Human Resources Associate.

The procedures require agents to securely return in person all ICES property to their supervisors on the termination date. ICES property is defined as including identification cards, access cards, and/or keys and copies of data including personal health information. The supervisor must, in turn, provide any property consisting of identification cards, access cards, and/or keys to ICES' Facilities Manager, who is required to maintain a record of items returned. The supervisor must provide any property consisting of mobile media or devices, which may contain copies of personal health information, to designated IT staff, who are required to maintain a record of items returned. If any property is not returned on the termination date, the procedures require a Human Resources Associate to take steps by the end of the day to engage the agent and obtain the property.

Under the procedures, one week prior to the agent's date of termination, a Human Resources Associate must (1)

submit a Track-IT ticket instructing designated IT staff to cut off access to ICES-controlled information systems on the agent's termination date; and (2) submit another Track-IT ticket instructing the Facilities Manager to terminate physical access to ICES on the agent's termination date. The procedures further require designated IT staff and the Facilities Manager to document the termination of access.

Compliance with the above policy and procedures is mandatory for all agents. Agents must notify an ICES Security Officer and/or an ICES Privacy Officer at the first reasonable opportunity if they breach, or believe there has been a breach of, the policy or procedures, in accordance with ICES' Security Incident Management Policy and/or ICES' Privacy Incident Management Policy. Violations including breach are subject to a range of disciplinary actions including warning, temporary or permanent loss of access privileges, legal sanctions and termination of employment or contract with ICES. Disciplinary actions are enforced by ICES' Manager of Human Resources in consultation with the Senior Director, Data Platform under ICES' Discipline and Corrective Action Policy. Compliance is subject to audit by a Human Resources Associate under ICES' Discipline and Corrective Action Policy.

11. Policy & Procedures for Discipline & Corrective Action

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Discipline & Corrective Action Policy	Implemented
	b. Discipline & Corrective Action Procedures	Implemented

DESCRIPTION

ICES' Discipline and Corrective Action Policy addresses discipline and corrective action with respect to agent misconduct generally and the associated procedures address misconduct involving personal health information specifically. In cases of misconduct involving personal health information, the procedures assign responsibility to the agent's supervisor, the Manager, Human Resources and the Chief Privacy Officer for conducting investigations. The procedures identify the documentation that must be completed by the Manager, Human Resources or the assigned Human Resources Associate, and its contents. Results of the investigation must be provided to the agent who has committed the misconduct, where applicable.

The types of discipline and corrective action that may be imposed and the factors that must be considered in determining the appropriate discipline and corrective action are set out in the policy and procedures. Under the procedures, the Manager, Human Resources, in consultation with the Chief Privacy Officer, must determine the appropriate type of discipline or corrective action to be imposed, up to and including termination. The procedures require the Manager, Human Resources or the assigned Human Resources Associate to document and file details related to the misconduct and the discipline imposed or corrective action taken.

Part 4 – Organizational & Other Documentation

1. Privacy Governance & Accountability Framework

APPLICATION	
Fully applicable ☒	Qualified application (*explain*)

EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Privacy Policy	Implemented

DESCRIPTION

ICES' Privacy Policy includes the following provisions to enable compliance with PHIPA and its regulation and compliance with ICES' privacy policies, procedures and practices addressed in this report. These include:

- Ultimate accountability of ICES' Chief Executive Officer;
- Identification of the Chief Privacy Officer as the position with day-to-day responsibility for privacy, who reports to and is overseen by the Chief Executive Officer;
- Identification of the role of, and requirement to appoint, privacy officers at ICES' main location and each ICES expansion site, who manage privacy under the oversight of ICES' Chief Privacy Officer;
- The oversight role of the Finance, Audit and Risk Committee of ICES' Board of Directors in relation to the privacy program; and
- The requirement that ICES' Chief Executive Officer report privacy breaches and privacy complaints to the Finance, Audit and Risk Committee, and submit to that committee each year a written update that addresses initiatives undertaken by the privacy program, including privacy training, the development and implementation of privacy policies and procedures, and privacy audits and privacy impact assessments and resulting recommendations and their status.

This policy stipulates that the policy, including the description of ICES' privacy governance and accountability framework it contains, must be published on the ICES intranet and addressed in privacy training, which is mandatory for all agents of ICES.

2. Security Governance & Accountability Framework

APPLICATION	
Fully applicable ☒	Qualified application (*explain*)

EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Security Framework & Governance Policy	Implemented

DESCRIPTION

ICES' Security Framework and Governance Policy ensures compliance with ICES' security policies, procedures and practices and with PHIPA and its regulation. Under the policy, ICES' Chief Executive Officer has ultimate accountability for ensuing personal health information is protected and agents comply with ICES' security policies and procedures. The policy identifies the positions at ICES with day-to-day authority to manage the information security and physical security programs, and their associated responsibilities and reporting relationships with ICES' Chief Executive Officer. Other ICES agents who support the security program are also identified in the policy.

The policy designates the Finance, Audit and Risk Committee of ICES' Board of Directors to oversee security at ICES. Designated security agents are required to provide annual updates, through a written report, to this committee. The report is required to contain information about initiatives undertaken by the security program, including training and policy development, as well as security audits and any security breaches investigated, including the results and any recommendations arising from the audits or breach investigations and the implementation status of the recommendations. The method by which the policy must be communicated to agents, and responsibility for communication, are stipulated in the policy.

3. Terms of Reference for Committees with Roles with Respect to the Privacy Program &/or Security Program

APPLICATION		
Not applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Finance, Audit & Risk Committee Terms of Reference	Implemented

DESCRIPTION

ICES' privacy and security programs are overseen by a committee of ICES' Board of Directors. Terms of reference for ICES' Finance, Audit and Risk Committee identify the mandate and responsibility of that committee in respect of ICES' privacy and security programs. They require that:

- The committee be comprised of at least three individuals, all of whom are members of the ICES' Board of Directors;
- The ICES' Board of Directors appoint one of the committee members as chair of the committee; and
- The committee review annual written reports prepared by ICES' Chief Privacy Officer and its Senior Director, Data Platform, as well as reports of any privacy and security audits and breaches and the sufficiency of associated remedial action.

In addition, the terms of reference require that all meetings of the committee be minuted, and once approved by it, circulated to ICES' Board of Directors. The committee is required to convene at least three times each year. No additional reports are required.

4. Corporate Risk Management Framework

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Integrated Risk Management Plan	Implemented
	b. ICES Risk Register	Implemented

DESCRIPTION

ICES has defined a comprehensive and integrated risk management framework to identify, assess, mitigate and monitor risks, including risks that may negatively affect its ability to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

ICES has recently appointed a new Senior Director, Corporate Services, who has operational responsibility for risk management. As part of this, she has been charged with reviewing ICES' existing risk management framework and the roles and responsibilities required to effectively implement risk management in ICES' current structure. In the meantime, risk management activities are carried out through ICES' Executive Committee, which includes the senior director and ICES' Chief Executive Officer and Chief Privacy Officer. These activities must, in turn, be reported by the senior director to the Finance, Audit and Risk Committee of ICES' Board of Directors, which has a duty to review all risks.

Risk management activities of ICES' Executive Committee include:

- Identifying, assessing and ranking risks;
- Determining whether to accept or mitigate risks;
- Devising, approving and overseeing the implementation of risk mitigation plans;
- Ensuring ICES' policies, procedures and practices as a prescribed entity are updated, where required, to take into account identified risks and mitigation activities;
- Documenting all of the above in the corporate risk register; and
- Reviewing, and updating, the risk register 4 times each year.

For clarity, the risks addressed by the Executive Committee include privacy risks.

Existing risk management tools, which are available to assist with this work, include:

- A risk register to document risks, assessments of likelihood and impact, risk rankings and rationale, and mitigation plans, timelines and associated roles and responsibilities;
- A risk register scoring template that defines the process to be followed and criteria that must be considered in ranking risks and assessing their likelihood and potential impact; and
- A framework for risk acceptance and mitigation.

5. Corporate Risk Register

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. ICES Risk Register	Implemented
DESCRIPTION		
ICES has a corporate risk register that identifies risks that may negatively affect ICES' ability to protect the privacy of individuals whose personal health information it collects and to maintain the confidentiality of that information. For each risk identified, the register provides an assessment of the risk, a ranking of the risk, a mitigation strategy to reduce the likelihood of the risk occurring and/or to reduce the impact of the risk if it does occur, the date the mitigation strategy was or is required to be implemented, and the agent responsible for implementation of the mitigation strategy.		

6. Policy & Procedures for Maintaining a Consolidated Log of Recommendations

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Consolidated Log of Recommendations	Implemented
IPC minimum content	Compliant ☒	Partially compliant (*explain*)
DESCRIPTION		
ICES has developed a consolidated log of recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches and complaints, the investigation of security breaches, and recommendations arising from reviews of the Information and Privacy Commissioner of Ontario. The log is jointly maintained by ICES' Senior Director, Data Platform and Chief Privacy Officer. Both members of ICES' Executive Committee, they review and update the log continuously. The log is accessible to all members of the Executive, and reviewed 4 times each year.		

7. Consolidated Log of Recommendations

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a. Consolidated Log of Recommendations	Implemented
DESCRIPTION		

ICES has developed a consolidated log of recommendations. The log captures recommendations arising from privacy impact assessments, privacy audits, security audits, the investigation of privacy breaches and complaints, the investigation of security breaches, and recommendations arising from reviews of the Information and Privacy Commissioner of Ontario. The log identifies the name and file number for each item on the log, the date of the document from which the recommendation arose, the recommendation, the manner for addressing the recommendation, the date on which recommendations were addressed and the responsible agent.

8. Business Continuity & Disaster Recovery Plan

APPLICATION		
Fully applicable ☒	Qualified application (*explain*)	
EXISTENCE & IMPLEMENTATION		
ICES vehicle(s)	**Name**	**Status**
	a.	
Comments	ICES undertakes to develop a full business continuity and disaster recovery plan. Please see below.	

DESCRIPTION

ICES has developed and implemented processes and procedures to protect and ensure the continued availability of its information technology environment as a prescribed entity in the event of short and long-term business interruptions or threats to its operating capabilities, including natural, environmental and technical interruptions and threats.

ICES leadership in this area has changed more than once since our last report to the IPC. ICES undertakes to develop a full business continuity and disaster recovery plan that meets the requirements of this section of the IPC Manual. In the meantime, ICES has put in place the following procedures and processes to protect the security and availability of personal health information in the event of any business interruption or disaster.

All ICES' data holdings are backed up and synchronized to a secure third party facility. The ICES-owned servers, storage and switches hosted there are remotely accessible to, and under the control of, ICES at all times. Data cuts created for specific projects, including research, are held in other systems, which are backed up to tape and stored in a secure zone at ICES' main location in fire-proof safes. Together, these arrangements would allow ICES to recover personal health information and resume operations in the event of a disaster or other business interruption.

C. Privacy, Security & Other Indicators

Part 1 – Privacy Indicators

General Privacy Policies, Procedures & Practices

Privacy Indicator	Assessment
Dates privacy policies and procedures were reviewed since prior IPC review	See Appendix A for details.
Whether amendments were made to existing privacy policies and procedures as a result of the review, and a list and description of each	
Whether new privacy policies and procedures were developed and implemented as a result of the review, and description of each	
Date each amended and newly developed privacy policy and procedure was communicated, and nature of communication	
Whether communication materials available to public and other stakeholders were amended as a result of the review, and description of amendments	

Collection

Privacy Indicator	Assessment
Number of data holdings that contain personal health information	Total data holdings: 71. This number includes data holdings that contain personally identifiable information including but not limited to personal health information.
Number of statements of purpose for data holdings that contain personal health information	Total statements of purpose: 71. This number includes statements of purpose for data holdings that contain personally identifiable information including but not limited to personal health information.
Number and list of statements of purpose reviewed since the last IPC review	Outside the ongoing review that occurs as part of ICES' project approval process and built into the ICES Project PIA Form, no statements of purpose have been reviewed. This will change with the implementation of ICES' recently developed Privacy Audit and Monitoring Policy, under which the accuracy and currency of statements of purpose will be verified through annual audits. To date, a mitigating safeguard has been the requirement that for each project conducted by ICES a project privacy impact assessment must be reviewed and approved by the Privacy Office. The review ensures the uses of the information are consistent with the statements of purpose.
Whether amendments were made to existing statements of purpose as a result of the review, and a list of those statements of purpose with a description of amendments made	Not applicable. As stated above, no statements of purpose have been reviewed.

Use

Privacy Indicator	Assessment
Number of agents granted approval to access and use personal health information for non-research purposes	Total agents granted approval: 110. This includes access and use by ICES Abstractors and ICES Data Covenantors, who are the only agents at ICES authorized to access and use personal health information with direct personal identifiers. Otherwise ICES agents are permitted access to and use of coded information only.

Number of requests received for use of personal health information for research since prior IPC	ICES has no record of requests received for use of personal health information for research.
Number of requests for use of personal health information for research purposes that were granted and that were denied since prior IPC review	ICES has no record of requests granted or declined.

Disclosure

Privacy Indicator	Assessment
Number of requests for disclosure of personal health information for non-research purposes since prior IPC review	Total requests: 2.
Number of requests for disclosure of personal health information for non-research purposes that were granted or denied since prior IPC review	Total requests granted: 2.
Number of requests for disclosure of personal health information for research since prior IPC review	Aside from requests for disclosures of personal health information to other prescribed entities whose mandate includes research, ICES has not received any requests for disclosures of personal health information.
Number of requests for disclosure of personal health information for research that were granted or denied since prior IPC review	Total requests granted or denied: 0.
Number of research agreements executed with researchers to whom personal health information was disclosed since the prior IPC review	Total agreements: 0.
Number of requests for disclosure of de-identified and/or aggregate information for research and other purposes since prior IPC review	Total requests: 23
Number of acknowledgements or agreements executed by persons to whom de-identified and/or aggregate information was disclosed for both research and other purposes since prior IPC review	Total agreements: 14. For clarity, of the 23 requests for disclosure referred to above, 6 await approval and 3 await release of information at this time.

Data Sharing Agreements

Privacy Indicator	Assessment
Number of DSAs executed for collection of personal health information since prior IPC review	Total DSAs: 340. This includes DSAs established for collection of personally identifiable information including but not limited to personal health information. ICES' recently developed Collection of Personally Identifiable Information Procedures, which set out the various steps, requirements and roles and responsibilities for collecting personal health information, are designed to track the execution of data sharing agreements more systematically and effectively. These procedures fall under and support ICES' Collection of Personally Identifiable Information Policy.
Number of DSAs executed for disclosure of personal health information since prior IPC review	Total DSAs: 1. Total DSA amendments: 1.

Agreements with Third Party Service Providers

Privacy Indicator	Assessment
Number of agreements executed with third party service providers with access to personal health information since prior IPC review	Total agreements: 1.

Data Linkage

Privacy Indicator	Assessment
Number and list of data linkages of personal health information approved since prior IPC	Total linkages: 548 See Appendix B for a list and details.

Privacy Impact Assessments

Privacy Indicator	Assessment
Number and a list of PIAs completed	Total number: 22 See Appendix C for a list and details.
Number and a list of PIAs undertaken but not completed	Total number: 8 Proposed completion date: 1. 30 Dec 2014 2. 31 Oct 2014 3. 31 Aug 2014 4. 31 Mar 2014 5. 31 Mar 2014 6. To be determined 7. To be determined 8. To be determined See Appendix C for a list and details.
Number and a list of PIAs not undertaken but for which a PIA will be completed and the proposed date of completion	Total number: 0
Number of determinations made that a PIA is not required, and for each the reason	Total number: 5 See Appendix C for a list and details. Reasons for determinations: PIA #13 – No personal health information was involved PIA #18 – Assessment was conducted as part of a separate but related initiative PIA #26 – No personal health information was involved PIA #28 – A decision was made to not move forward with the proposed introduction of new software PIA #29 – No personal health information was involved
Number of PIAs reviewed	Total number: 0

Privacy Audit Program

Privacy Indicator	Assessment
Dates of audits of agents granted approval to access and use personal health information since prior IPC review and for each audit: • A description of each recommendation; • Date each recommendation was addressed or is proposed to be so; and • Manner each recommendation was, or is proposed to be, addressed	To date, ICES has not had a privacy audit program. As a result, ICES has not conducted an audit since the previous review specifically of agents granted access to and use of PHI. An audit program will commence with the implementation of ICES' recently established Privacy Audit and Monitoring Policy. Under the policy, audits of agent access to and use of personal health information must, and will, be conducted.

Number and list of all other privacy audits since prior IPC review and for each audit: • Description of nature and type of audit; • Completion date; • Description of each recommendation; • Date each recommendation was, or is proposed to be, addressed; • Manner in which each recommendation was, or is proposed to be, addressed	Total privacy audits: 5. 1. Assessing ICES data for sensitive variables 2. Assessing ICES data for free text containing sensitive information 3. Verifying continued need for access to ICES controlled use data 4. Assessing completeness and accuracy of ICES project PIA log 5. Verifying renewal of annual confidentiality agreements See Appendix D for details.

Privacy Breaches

Privacy Indicator	Assessment
Total	1
Date notified	11 February 2012
Extent	Clinical records of 9 physicians
Internal/external	Internal
Nature & extent	Clinical data extracted from physician electronic medical records
CEO notified	11 February 2012
Containment	Database access frozen
Containment date	11 February 2012
Third party notice	17 February 2012 (IPC), 27 February 2012 (clinics)
Investigation start	16 February 2012
Investigation close	14 March 2012
Recommendations	(i) Enhance control at point of collection by changes to plug-in; (ii) Replace individual physician agreements with clinic-wide agreements
Implemented	(i) For next 2012 collection cycle; (ii) 1 March 2012

Privacy Complaints

Privacy Indicator	Assessment
Number of privacy complaints since prior IPC review	ICES has not received any privacy complaints since the last IPC review.
Of the privacy complaints received, the number investigated since prior IPC review and for each the: • Date complaint received; • Nature of complaint; • Date investigation commenced; • Date of letter to individual who complained in relation to the commencement investigation; • Date investigation completed; • Description of each recommendation; • Date each recommendation was, or is proposed to be, addressed; • Manner each recommendation was, or is proposed to be, addressed; and • Date of letter to individual who complained describing nature and findings of investigation and measures taken	ICES has not received any privacy complaints since the last IPC review.
Of the privacy complaints received, the number not	ICES has not received any privacy complaints since the

investigated since prior IPC review and for each the: • Date complaint received; • Nature of complaint; and • Date of letter to individual who complained and description of letter's content	last IPC review.

Part 2 – Security Indicators

General Security Policies, Procedures & Practices

Security Indicator	Assessment
Dates security policies and procedures were reviewed since prior IPC review	See Appendix E for details.
Whether amendments were made to existing security policies and procedures as a result of the review, and a list and description of each	
Whether new security policies and procedures were developed and implemented as a result of the review, and description of each	
Date each amended and newly developed security policy and procedure was communicated, and nature of communication	
Whether communication materials available to public and other stakeholders were amended as a result of the review, and description of amendments	

Physical Security

Security Indicator	Assessment
Dates of audits of agents granted approval to access the premises and locations within them where personal health information is retained since the prior IPC review: • Description of each recommendation; • Date recommendation was, or is proposed to be, addressed; • Manner in which recommendation was, or is proposed to be, addressed	See Appendix F for details.

Security Audit Program

Security Indicator	Assessment
Dates of review of system control and audit logs since prior IPC review and description of findings	No reviews of system and audit logs have been conducted since the last IPC review. Such reviews will soon commence with the implementation of ICES' recently established Security Audit Policy and Security Audit SOP.
Number and list of security audits since prior IPC review and for each: • Description of nature and type of audit; • Date completed; • Description of each recommendation; • Date recommendation was, or is proposed to be, addressed • Manner in which recommendation was, or is expected to be, addressed	See Physical Security indicator above.

Information Security Breaches

Security Indicator	Assessment
Number of notifications of actual or suspected information security breaches since prior IPC review	Total security breaches: 5.
For each actual or suspected information security	

breach: • Date of notification; • Extent of actual or suspected breach; • Nature and extent of personal health information at issue; • Date senior management notified; • Containment measures; • Date(s) containment measures implemented; • Date(s) notification provided health information custodians or others; • Date investigation commenced; • Date investigation completed; • Description of each recommendation; • Date recommendation was, or is proposed to be, addressed; • Manner in which recommendation was, or is proposed to be, addressed	See Appendix G for details.

Part 3 – Human Resources Indicators

Privacy Training & Awareness

Human Resources Indicator	Assessment
Number of agents who have, and who have not, received initial privacy orientation since prior IPC review	Total orientations received: 531 Total orientations not received: 2
Date of commencement of employment, contractual or other relationship for agents yet to receive initial privacy orientation and the scheduled orientation date	No agents have yet to receive initial privacy orientation. The two agents above who failed to attend orientation have left ICES.
Number of agents who have, and who have not, attended ongoing privacy training each year since prior IPC review	To this point, ongoing privacy awareness activities have been carried out and have been tracked. These have included presentations at ICES staff meetings, which all agents are invited and expected to attend. But, because awareness activities have not to date included training per se, this has not taken the form of attendance tracking specifically. This will very shortly change when privacy e-learning is launched. That program, which will be mandatory for all agents and subject to annual renewal, will include tracking to monitor and enforce compliance.
Dates, number and description of privacy communications to agents since prior IPC review	Oct 2012 – ICES staff meeting privacy update May 2013 – ICES staff meeting privacy presentation All agents are invited and expected to attend ICES staff meetings.

Security Training & Awareness

Human Resources Indicator	Assessment
Number of agents who have, and who have not, received initial security orientation since prior IPC review	Total orientations received: 531 Total orientations not received: 2
Date of commencement of employment, contractual or other relationship for agents yet to receive initial security orientation and the scheduled orientation date	No agents have yet to receive initial security orientation. The two agents above who failed to attend orientation have left ICES.
Number of agents who have, and who have not, attended ongoing security training each year since prior IPC review	To this point, ongoing security awareness activities have been carried out. These have included updates at ICES staff meetings, which all agents are invited and expected to attend, and ICES staff newsletters, which are distributed electronically to all agents. But, because these have not to date included training per se, this has not taken the form of attendance tracking specifically. This will change under ICES' recently developed Security Training and Awareness Policy and supporting procedures, under which security training must be completed annually and tracked.
Dates and number of security communications to agents since prior IPC review	Total security communications: 6. Dates: 13 Sep 2013; 9 Sep 2013; 25 Jan 2013; 11 Dec 2012; 8 Nov 2012; 15 Jun 2012; 11 May 2012; 22 Dec 2011 Security communications have taken the form of updates at ICES staff meetings, which all agents are invited and expected to attend, and ICES staff newsletters, which are distributed electronically to all agents.

Confidentiality Agreements

Human Resources Indicator	Assessment
Number of agents who have, and who have not, signed confidentiality agreements each year since prior IPC review	Total agreements signed including initial and annual agreements: 01 Nov 2011 - 31 Mar 2012: 144 01 Apr 2012 - 31 March 2013: 980 01 Apr 2013 - 31 Oct 2013: 390 Total annual agreements not signed (all initial agreements were signed): 01 Nov 2011 - 31 Mar 2012: 0 01 Apr 2012 - 31 Mar 2013: 0 01 Apr 2013 - 31 Oct 2013: 23 ICES' recently developed Privacy Awareness Procedures are designed to track the signing of confidentiality agreements more systematically and effectively.
Date of commencement of employment, contract or other relationship for agents yet to execute confidentiality agreements and date agreement must be executed	Commencement dates of the 23 individuals above who have yet to renew their annual agreement: 18-Jan-2013, 1-Nov-2012, 1-Jul-2012, 1-Oct-2011, 2-Feb-2011, 1-Mar-2010, 1-Mar-2010, 1-Mar-2010, 1-Mar-2010, 1-Dec-2009, 1-Sep-2009, 1-Sep-2009, 1-Jun-2009, 1-Apr-2009, 1-Jan-2009, 1-Aug-2007, 1-Sep-2006, 16-Dec-2004, 15-May-2004, 1-Nov-2003, 1-Aug-1999, 1-Jul-1995, 1-Apr-1993 Annual agreement deadline: 15-Jan-2014

Termination or Cessation

Human Resources Indicator	Assessment
Number of notifications from agents since prior IPC review for termination of their employment, contractual or other relationship	Total notifications: 200. This number does not include all students who departed ICES during the prior IPC review. More accurate tracking of student departures will commence with ICES' planned development of defined off-boarding procedures for this role.

Part 4 – Organizational Indicators

Risk Management

Organizational Indicator	Assessment
Dates corporate risk register was reviewed since prior IPC review	Due to a series of organizational and personnel changes, the corporate risk register was not in use during the review period. It has just been re-instituted, and will be reviewed quarterly effective immediately.
Whether amendments were made to the corporate risk register as a result of the review, and description of each	For the reason noted above, the corporate risk register has not been amended.

Business Continuity & Disaster Recovery

Organizational Indicator	Assessment
Dates business continuity and disaster recovery plan was tested since prior IPC review	Development of a business continuity and disaster recovery plan is currently in progress. As such, the plan has not been tested since the prior IPC review. Projected development and implementation TBD.
Whether amendments were made to business continuity and disaster recovery plan as a result of testing, and description of each	Development of a business continuity and disaster recovery plan is currently in progress. As such, the plan has not been tested since the prior IPC review, nor has it been amended.

D. Sworn Affidavit

SWORN AFFIDAVIT

I, Dr. Michael Schull, President & Chief Executive Officer of the Institute for Clinical Evaluative Sciences (ICES), MAKE OATH AND SAY:

1. ICES has in place policies, procedures and practices to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information.

2. The policies, procedures and practices implemented by ICES comply with the *Personal Health Information Protection Act, 2004* and the regulations thereto, as may be amended from time to time.

3. The policies, procedures and practices implemented by ICES comply with the *Manual for the Review and Approval of Prescribed Persons and Prescribed Entities* that has been published by the Information and Privacy Commissioner of Ontario, as it may be amended from time to time.

4. ICES has submitted a written report to the Information and Privacy Commissioner of Ontario in compliance with the *Manual for the Review and Approval of Prescribed Persons and Entities.*

5. ICES has taken steps that are reasonable in the circumstances to ensure compliance with the policies, procedures and practices implemented and to ensure that the personal health information received is protected against theft, loss and unauthorized use or disclosure and to ensure that records containing personal health information are protected against unauthorized copying, modification or disposal.

SWORN (OR AFFIRMED) BEFORE ME

in the City of Toronto on 24 October 2014.

Michael Schull
President & Chief Executive Officer
ICES

Commissioner for Taking Affidavits

E. Appendices

Appendix A – Privacy Policies & Procedures

Name	Description	Status	Implent-ation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Commun-ication (IC)	IC Date	IC Method	Public Commun-ication (PC)	PC Date	PC Description *As applicable*
Privacy Policy	Governs ICES' collection, use and disclosure of personal health information	New	Jan-14	n/a	June-15	n/a	Required	01/17/14; 04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Required	08/23/13	Refreshed public website privacy page
Privacy Information, Inquiries & Complaints Policy	Governs ICES' handling of inquiries and complaints	Replacement	Jun-14	n/a	June-15	New approach to handling inquiries and complaints defined	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Required	08/23/13	Public website privacy page was refreshed as a result of the policy review but no substantive changes were made
Public website privacy page	Describes the personal health information ICES collects, the purposes of collection and ICES' safeguards	Replacement	Aug-13	n/a	Nov-14	Revised description of the personal health information ICES collects, the purposes of collection and ICES' safeguards	Not required	n/a	n/a	Required	08/23/13	Public website privacy page was refreshed as a result of the website review to include a revised description of the personal health information ICES collects, the purposes of collection and ICES' safeguards
Privacy Inquiries & Complaints Procedures	Sets out the steps for responding to inquiries and complaints	New	Jun-14	n/a	June-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email	Required	08/23/13	Refreshed public website privacy page
Privacy Inquiry & Privacy Complaints Log	Used to track inquiries and complaints	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES Privacy Complaint Form	Used to capture information on complaints	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES Privacy Complaint Report	Used to generate a complaint report	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES Privacy Inquiry Report	Used to generate an inquiry report	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
Privacy Complaint Response 1 A	Template communication letter	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a

Name	Description	Status	Implent-ation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Commun-ication (IC)	IC Date	IC Method	Public Commun-ication (PC)	PC Date	PC Description *As applicable*
Privacy Complaint Response 1 B	Template communication letter	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
Privacy Complaint Response 2	Template communication letter	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
Collection of Personally Identifiable Information Policy	Governs ICES' collection of personal health information	New	Jun-14	n/a	June-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Not required	n/a	n/a
Collection of Personally Identifiable Information Procedures	Sets out the steps for collection of personal health information	New	Jun-14	n/a	June-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Data Sharing Agreement (HIC)	Template data sharing agreement	Replacement	Pre 2011 IPC review	Dec-11; Sep-12; Mar-13; Jun-14; Jul-14	June-15	General revision and re-organization; Data linkage and destruction requirements and methodology revised; Certificate of destruction made mandatory; Method of transfer specified in contract; Schedule revised to enable	DPD only	05/01/13	Training, email	Not required	n/a	n/a

Name	Description	Status	Implent-ation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Commun-ication (IC)	IC Date	IC Method	Public Commun-ication (PC)	PC Date	PC Description *As applicable*
						generation of statements of purpose for new data holdings; Miscellaneous revisions to achieve compliance with IPC Manual						
ICES Data Sharing Agreement (Researcher)	Template data sharing agreement	New	Jul-13	Oct-13; Jul-14	June-15	n/a	DPD only	07/03/13	Training, email	Not required	n/a	n/a
Privacy Impact Assessment Policy	Establishes ICES' requirements for PIAs	Replacement	Jun-14	n/a	Jun-15	Scope enlarged from research projects only to include all change scenarios, previously subject to an internal PIA guideline only. The policy was also refined for compliance with relevant IPC Manual requirements.	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Project PIA Form	Used to assess and document approval of ICES projects	Replacement	Planned	n/a	n/a	This is being substantially revised to guide and document assessment of legal authorities and reinforce scrutiny of data selection for	Required	Planned	n/a	Not required	n/a	n/a

Name	**Description**	**Status**	**Implent-ation Date**	**Last ICES Review**	**Next Planned ICES Review**	**Description of Change(s)**	**Internal Commun-ication (IC)**	**IC Date**	**IC Method**	**Public Commun-ication (PC)**	**PC Date**	**PC Description** *As applicable*
						relevance and scope.						
ICES Project PIA Review Procedure	Sets out the steps for reviewing and approving ICES project PIAs	New	Jun-14	n/a	Jun-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES PIA Form - Data Holding	Used to assess and document approval of new data holdings	New	Nov-13	n/a	Nov-14	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES PIA Form - Service Provider	Used to assess and document approval of new service providers	New	Nov-13	n/a	Nov-14	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES PIA Form - General	Used to assess and document approval of new processes or systems	New	Nov-13	n/a	Nov-14	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES PIA Form - Data Disclosure	Used to assess and document approval of data disclosures	New	Nov-13	n/a	Nov-14	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
Privacy Audit & Monitoring Policy	Governs ICES' approach to audits and monitoring	New	Jun-14	n/a	June-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Not required	n/a	n/a
Privacy Monitoring Log & Report Forms Workbook	Used to conduct privacy reviews and track associated remediation	New	Jun-14	n/a	June-15	n/a	Privacy Office only	04/15/14; 06/11/14	Training, Privacy Office meeting	Not required	na	n/a
Privacy Audit Log & Report Forms Workbook	Used to conduct privacy audits and track associated remediation	New	Jun-14	n/a	Jun-15	n/a	Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
Privacy Incident Management Policy	Governs ICES' management of privacy incidents	Replacement	Jun-14	n/a	June-15	New approach to handling privacy	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting,	Not required	n/a	n/a

Name	**Description**	**Status**	**Implent-ation Date**	**Last ICES Review**	**Next Planned ICES Review**	**Description of Change(s)**	**Internal Commun-ication (IC)**	**IC Date**	**IC Method**	**Public Commun-ication (PC)**	**PC Date**	**PC Description** *As applicable*
	and breaches					incidents and breaches defined			staff email			
Protection of ICES Data Policy	Ensures agents access and use the minimum amount of personal health information in the least identifiable form required for the purpose	New	Aug-14	n/a	Aug-15	n/a	Required	Aug-14; Sep-14	Staff meeting, staff email	Not required	n/a	n/a
Privacy Awareness & Training Policy	Establishes ICES' requirements for privacy awareness and training	Replacement	June-14	n/a	June-15	New framework for privacy awareness defined	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Not required	n/a	n/a
Privacy Awareness & Training Procedures	Sets out the steps for scheduling and delivering privacy training	New	Jun-14	n/a	Jun-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting	Not required	n/a	n/a
Privacy Requirements Table	Defines privacy awareness requirements specific to each role at ICES	New	Jun-14	n/a	Jun-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting	Not required	n/a	n/a
Privacy Awareness Log	Used to log attendance at privacy orientation and signing of confidentiality agreements	Revised	Pre 2011 IPC review	Nov-13	Nov-14	Amended to include additional IPC required logging elements	Required	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
Privacy Awareness Attendance Sheet	Used to record attendance at privacy orientation	New	Apr-14	n/a	Nov-14		Privacy Office only	04/15/14	Training, Privacy Office meeting	Not required	n/a	n/a
ICES Confidentiality Agreement (General)	Template confidentiality agreement for general use	Revised	Pre 2011 IPC review	Nov-13	Nov-14	Refined for greater compliance with the IPC Manual	Required	01/10/13; 04/15/14	Intranet posting, staff meeting	Not required	n/a	n/a

Name	**Description**	**Status**	**Implent-ation Date**	**Last ICES Review**	**Next Planned ICES Review**	**Description of Change(s)**	**Internal Commun-ication (IC)**	**IC Date**	**IC Method**	**Public Commun-ication (PC)**	**PC Date**	**PC Description** *As applicable*
ICES Confidentiality Agreement (Abstractor)	Template confidentiality agreement for ICES abstractors	Revised	Pre 2011 IPC review	Nov-13	Nov-14	Refined for greater compliance with the IPC Manual	Required	01/10/13; 04/15/14	Intranet posting, staff meeting	Not required	n/a	n/a
ICES Confidentiality Agreement (Data Covenantor)	Template confidentiality agreement for ICES data covenantors	Revised	Pre 2011 IPC review	Nov-13	Nov-14	Refined for greater compliance with the IPC Manual	Required	01/10/13; 04/15/14	Intranet posting, staff meeting	Not required	n/a	n/a
ICES Collaborating Researcher NDA	Template NDA for ICES collaborating researchers	Revised	Pre 2011 IPC review	Nov-13	Nov-14	Refined for greater compliance with the IPC Manual	Required	01/10/13; 04/15/14	Intranet posting, staff meeting	Not required	n/a	n/a
ICES NDA	Template NDA for general use	Revised	Pre 2011 IPC review	Nov-13	Nov-14	Refined for greater compliance with the IPC Manual	Required	01/10/13; 04/15/14	Intranet posting, staff meeting	Not required	n/a	n/a
Research Ethics Review Policy	Establishes ICES' requirements for research ethics review	New	Jun-14	n/a	Jun-15	n/a	Required	04/15/14; 06/10/14	Training, staff meeting, Privacy Office meeting, staff email, intranet posting	Not required	n/a	n/a
Protecting Personal Health Information on Mobile Devices	Establishes requirements for safeguarding PHI on mobile devices	Revised	Pre 2011 IPC review	Jun-14	Jun-15	Revised to include: cross-reference to new secure retention policies and procedures; compliance and audit requirements; and responsibility for encryption	Required	30/8/14	Intranet posting	Not required	n/a	n/a
Management of Data Convenantors Procedures	Sets out the steps to be followed when ICES data covenantors	New	Aug-14	n/a	Aug-15	n/a	Required	30/8/14	Intranet posting	Not required	n/a	n/a

Name	Description	Status	Implent-ation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Commun-ication (IC)	IC Date	IC Method	Public Commun-ication (PC)	PC Date	PC Description *As applicable*
	change roles											
Abstractor Onboarding and Offboarding Procedure	Sets out the process for offboarding and onboarding ICES Abstractors	New	Planned	n/a	n/a	n/a	Required	Planned	Intranet posting	Not required	n/a	n/a
Creating Coded Data at ICES Procedure	Sets out the procedure for creating coded data	New	Aug-14	n/a	Aug-15	n/a	Required	30/8/14	Intranet posting	Not required	n/a	n/a
Creating Summary Data Procedure	Sets out the procedure for creating summary data	New	Planned	n/a	n/a	n/a	Required	Planned	n/a	Not required	n/a	n/a
ICES Data Risk Assessment Procedure	Sets out the steps for assessing re-identification risk of data	New	Planned	n/a	n/a	n/a	Required	Planned	n/a	Not required	n/a	n/a
Linking ICES Data Procedure	Sets out the steps for linking data	New	Planned	n/a	n/a	n/a	Required	Planned	n/a	Not required	n/a	n/a
Certificate of Destruction	Template certificate of destruction	New	Aug-14	n/a	n/a	n/a	DQIM only	30/8/14	n/a	Not required	n/a	n/a
Dataset Creation Plan Procedure	Sets out steps to create datasets for analysis	New	Planned	n/a	n/a	n/a	Required	Planned	n/a	Not required	n/a	n/a

30-Sep-14

Appendix B – Approved Data Linkages

#	Project Title	ICES Data
1	The effect of post-discharge outpatient care on unplanned readmissions: The EPOC-readmission study	CIHI-DAD 2003-2009 CIHI-NACRS 2003-2009 OHIP 2003-2009 RPDB
2	The prescribing trends of nurse practitioners and family physicians to children and adolescents with a disability or on social assistance in Ontario:1998-2010	ODB 1998-2010 RPDB IPDB CPDB OHIP 1998-2010
3	Exploring variation in prenatal screening services in Ontario	CIHI-DAD 2007-2010 CIHI-SDS 2007-2010 CIHI-NACRS 2007-2010 OHIP 2007-2010 RPDB IPDB CPDB OMMMS 2007-2010
4	Finasteride and breast cancer in men: Feasibility study	ODB 1991-2009 OCR 1991-2009
5	Estimating the economic impact of adopting best-practice recommendations for post-stroke rehabilitation in Ontario	CIHI-DAD 2008-2011 CIHI-CCRS 2008-2011 CIHI-NRS 2008-2011 ODB 2008-2011 OHIP 2008-2011 RCSN 2004-2011
6	A population-based study of cancer incidence and mortality in patients with solid organ transplant: Specific aim 1	CIHI-DAD 1997-2011 RPDB OCR 1964-2010 CORR 1997-2009
7	Estimating the costs associated with infectious diseases: A pilot study	CIHI-DAD 2002-2010 CIHI-SDS 2002-2010 CIHI-NACRS 2002-2010 CIHI-NRS 2002-2010 ODB 2002-2010 OHIP 2002-2010 HCD 2002-2010 LOC 2002-2010 RPDB
8	Sleep deprived surgeons & adverse patient outcomes following cholecystectomies	CIHI-DAD 2002-2010 CIHI-SDS 2002-2010 OHIP 2002-2010 RPDB IPDB
9	Process and outcomes for people who have left the hospital with bacteremia	CIHI-DAD 2003-2011 CIHI-NACRS 2003-2011 ODB 2003-2011 OHIP 2003-2011 RPDB
10	High cost users of the healthcare system: Preliminary high level analyses for the MOHLTC	CIHI-DAD 2007-2008 ODB 2007-2008 OHIP 2007-2008 RPDB IPDB
11	Oxycodone prescribing patterns	ODB 2006-2011 OHIP 2006-2011 RPDB IPDB

#	Project Title	ICES Data
		OCR 1964-2011
12	Robotic-assisted minimally invasive surgery evaluation	CIHI-DAD 1998- March 31, 2012 CIHI-SDS 1998- March 31, 2012 CIHI-NACRS 2002- March 31, 2012 ODB 2002- March 31, 2012 OHIP 1998- March 31, 2012 HCD 2002-2010 RPDB IPDB OCR 1964-2010 OCR 1964-2010 3 Registries of patients who underwent robotic-assisted minimally invasive surgery 2005-2010 CCO synoptic pathology reporting (prostatectomy data) 2005-2011 ODD
13	Effect of gender on escalation of opioid therapy and opioid related mortality	CIHI-DAD 1992-2011 ODB 1996-2011 OHIP 1992-2011 OMHRS 2005-2011 RPDB IPDB ODD Coroners' Data 1994-2006
14	Angiotensin receptor blockers in patients with type II diabetes: A population based study	CIHI-DAD 1995-2011 ODB 2000-2011 OHIP 1995-2011 RPDB ODD 1991-2011 NACRS 2000-2011 SDS 2003-2011
15	Osteoporotic fracture risk in elderly chronic kidney disease patients	CIHI-DAD 1997-2010 CIHI-SDS 1997-2010 CIHI-NACRS 2001-2010 ODB 2001-2009 OHIP 1997-2010 RPDB ODD Cerner & Gamma Dynacare 1999 & 2002 - 2010
16	Validation and use of evidence-based asthma care performance indicators in Ontario (VALUE-API) part 1: Identifying eligible primary care physicians treating patients with asthma	OHIP 2009-2010 IPDB
17	Safety of IV tPA in ischemic stroke patients with alcohol abuse	CIHI-DAD 2003-2010 RCSN 2003-2010
18	Have urinary retention rates following cataract surgery increase after the discovery of "floppy iris syndrome"? A time series analysis	CIHI-DAD 2001-2010 CIHI-SDS 2001-2010 CIHI-NACRS 2001-2010 ODB 2001-2010 OHIP 2001-2010 RPDB
19	Co-prescribing of aspirin with cholinesterase inhibitors and the increased risk of upper gastrointestinal bleeding	CIHI-DAD 1995-2010 CIHI-SDS 1995-2010 CIHI-NACRS 2002-2010 ODB 1999-2010 OHIP 1995-2010 RPDB

#	Project Title	ICES Data
20	Quality of end of life cancer care in Canada: A comparison between BC, AL, ONT and NS	CIHI-DAD 2003-2008 CIHI-NACRS 2003-2008 OHIP 2003-2008 HCD 2003-2008 RPDB OCR 2003-2008
21	CSQI (Cancer System Quality Index) analyses performed under contract with Cancer Care Ontario 2011/12	CIHI-DAD 2001-2010 CIHI-SDS 2001-2010 CIHI-NACRS 2001-2010 OHIP 2001-2010 HCD 2001-2010 RPDB OCR 2001-2010 OBSP Cytobase
22	Accuracy of Ontario administrative health databases in identifying patients with rheumatoid arthritis	CIHI-DAD 1991-2011 CIHI-SDS 1991-2011 CIHI-NACRS 2000-2011 ODB 1991-2011 OHIP 1991-2011 RPDB IPDB
23	Duration of antibiotic therapy among residents of Ontario long-term care facilities: Impact of prescriber	CIHI-DAD 2003-2010 CIHI-CCRS 2008-2010 ODB 2007-2010 OHIP 2008-2010 RPDB IPDB NACRS 2009 – 2010
24	Ontario Drug Benefit (ODB) formulary expenditures	CIHI-DAD 2006-2011 CIHI-SDS 2006-2011 CIHI-NACRS 2006-2011 ODB 2006-2011 OHIP 2006-2011 RPDB IPDB OCR 2001-2011
25	Childhood-onset systemic lupus erythematosus: Determining long-term outcomes	CIHI-DAD 1991-2010 CIHI-NACRS 2002-2010 OHIP 1991-2010 RPDB IPDB OCR 1985-2010 Vital Statistics 1991-2010 Census Area Profiles 1991, 1996, 2001, 2006
26	The risk of mycobacterial infections associated with tumor necrosis factor inhibitors in Ontario	CIHI-DAD 1991-2010 ODB 1991-2010 OHIP 1991-2010 RPDB IPDB ASTHMA CHF COPD HYPERTENSION ODD

#	Project Title	ICES Data
27	Appropriate dosing of antidepressants in patients with CKD	CIHI-DAD 1997-2010 CIHI-SDS 1997-2010 CIHI-NACRS 1997-2010 ODB 2001-2010 OHIP 1997-2010 RPDB Gamma Dynacare & CERNER 2002-2010
28	Quality of care following psychiatric hospitalization	CIHI-DAD 2008-2010 CIHI-NACRS 2008-2010 ODB 2008-2010 OHIP 2008-2010 OMHRS 2008-2010 RPDB IPDB CPDB
29	Patterns of testosterone prescribing in Ontario	CIHI-DAD 1992-2011 ODB 1996-2011 OMHRS 2005-2011 RPDB IPDB ODD
30	Empirical evaluation of a surgical safety checklist in Ontario hospitals	CIHI-DAD 2006-2011 CIHI-NACRS 2006-2011 OHIP 2006-2011 RPDB IPDB Llist of Ontario hospitals, hospital identifier, and date of introduction of surgical safety checklist
31	Patterns and predictors of health care utilization by adult survivors of childhood cancer: A Pediatric Oncology Group of Ontario and Institute for Clinical Evaluative Sciences population database linkage study	CIHI-NACRS 2001-2011 OHIP 1986 - 2011 RPDB IPDB CPDB Statistics Canada
32	Validation of ICD10 CKD codes	CIHI-DAD 2002-2010 CIHI-SDS 2002-2010 CIHI-NACRS 2002-2010 ODB 2006-2010 OHIP 2002-2010 OHIP 2002-2010 RPDB CERNER & Gamma Dynacare 2006 - 2010
33	Effect of undergraduate education on opioid prescribing	ODB 2000-2011 OHIP 2000-2011 RPDB CAPE IPDB CPDB
34	Repeat fractures in children: A population-based study of the incidence and risk factors associated with repeat fractures in Ontario children	CIHI-NACRS 2002-2011 OHIP 1992-2002 RPDB
35	Health administrative data as biomarkers of exposure to toxic substances	OHIP 1991-2011 RPDB IPDB Landed Immigrant Dataset 1980-2011
36	Profiling community dwelling seniors (66+) in Ontario with coexisting chronic conditions	CIHI-DAD 2002-2008 CIHI-SDS 2002-2008

#	Project Title	ICES Data
		CIHI-NACRS 2002-2008 CIHI-CCRS 2006-2008 CIHI-NRS 2006-2008 ODB 2006-2008 OHIP 2002-2008 HCD 2006-2008 RPDB CPRO RAI-HC (OACCAC) 2006-2008
37	TIA patient discharge from the emergency department	CIHI-DAD 2008-2010 CIHI-NACRS 2008-2010 RPDB RCSN 2008-2010
38	Costing of colorectal cancer care by cancer stage, for use in modelling the cost-effectiveness of colorectal screening in Ontario	CIHI-DAD 1988-2011 CIHI-SDS 1988-2011 CIHI-NACRS 1998-2011 CIHI-CCRS 1998-2011 CIHI-NRS 1988-2011 ODB 1992-2011 OHIP 1992-2011 HCD 1992-2011 RPDB ODD OMID OCR 1964-2010
39	Outcomes of cervix cytology screening, collected and submitted by nurse practitioners in Ontario	CIHI-DAD 1988-2011 CIHI-SDS 1988-2011 CIHI-NACRS 1988-2011 OHIP CAPE IPDB CPDB OCR 1964-2010 Cytobase
40	Statistical methods for cohort and case-based designs	CIHI-DAD 1991-2010 CIHI-SDS 1991-2010 CIHI-NACRS 1991-2010 ODB 1991-2011 OHIP 1991 2011 RPD BIPD BCHF COPD ODD OMID EFFECT 1999-2005
41	Trends in incidence & management of intracerebral hemorrhage in ON from 1990 to 2010	CIHI-DAD 1990-2010 RCSN 2003-2010
42	Peri-operative medicine outcomes research program	CIHI-DAD 2003-2011 CIHI-SDS 2003-2011 ODB 2003 - 2011 OHIP 2003-2011 RPDB COPD Hypertension ODD Cardiac Arrest Database

#	Project Title	ICES Data
43	Suicide-related behaviours in children & youth - time trends in Alberta & Ontario	CIHI-DAD 2002-2010 CIHI-NACRS 2002 - 2010 OMHRS 2005-2010 RPDB
44	Socioeconomic status & the risk of opoid-related mortality	Coroner's data 1992-2006 CIHI-DAD 1988-2011 ODB 1992-2011 RPDB OCR 1964-2006 NACRS 2000 - 2011 OHIP 1991 - 2011
45	Clinical presentation & outcomes of colorectal cancers missed by colonoscopy	CIHI-DAD 2002- 2011 CIHI-SDS 2002-2011 OHIP 2002 - 2011 RPDB OCR 2007 -2009
46	Burden of injury among First Nations communities in Ontario: Updated analysis	CIHI-DAD 2006-2010 CIHI-NACRS 2006-2010 RPDB
47	Tousled-like kinase (TLK) Inhibitors and breast cancer	CIHI-DAD 1992-2010 CIHI-SDS 1992-2010 ODB 1997-2010 OHIP 1992-2010 OMHRS 2005-2010 RPDB OCR 1964-2010
48	NSAIDs and the risk of hyperkalemia in older patients receiving an ACEI or ARB	CIHI-DAD 1992-2011 ODB 1992-2011 OHIP 1992-2011 RPDB ODD
49	Validation of ICD10 rhabdomyolysis codes	CIHI-DAD 1998-2010 CIHI-NACRS 1998-2010 ODB 2002-2010 OHIP 1998-2010 RPDB Cerner Gamma Dynacare 2002-2010
50	Preparing for a safety evaluation of rotavirus vaccine using health services data in Ontario: The development of a diagnostic algorithm for intussusception, an estimation of baseline incidence and an evaluation of methods	CIHI-DAD 1995-2010 CIHI-NACRS 1995-2010 OHIP 1995-2010 RPDB CAPE MOMBaby
51	A new model for general internal medicine teaching units	CIHI-DAD 2001-2011 CIHI-NACRS 2001-2011 OHIP 2001-2011 RPDB CPDB
52	Improving diabetes care for frail older adults with comorbid chronic conditions	CIHI-DAD April 2008- April 2010 CIHI-NACRS April 2008- April 2010 ODB April 2008- April 2010 OHIP April 2008- April 2010 HCD April 2009- April 2010 RPDB COPD ODD

#	Project Title	ICES Data
53	Socioeconomic status, diagnostic delay and outcome in pediatric acute lymphoblastic leukemia	CIHI-DAD 1992-2010 CIHI-NACRS 2000-2010 OHIP 1992-2010 RPDB IPDB OCR 1995-2010 Pediatric Oncology Group of Ontario Networked Information System, Landed Immigrant Data System 1995 to 2010
54	Evaluating the effectiveness of a home-based care program	CIHI-DAD 2006-2013 CIHI-NACRS 2006-2013 RAI-HC 2005-2013 ODB 2006-2013 OHIP 2006-2013 HCD 2006-2013 RPDB
55	Breast cancer and reason for hospital visits	CIHI-DAD 2002-2010 CIHI-SDS 2002-2010 CIHI-NACRS 2006-2010 OHIP 2002-2010 RPDB ODD OCR 1964-2010 CCO stage data 2005-2009
56	Difference in patient characteristics among adult Ontario patients with suspected acute stroke who did and did not receive preliminary neuroimaging	CIHI-DAD 2000-2011 CIHI-NACRS 2000-2011 RPDB RCSN 2002-2011
57	Predictors of readmission following acute stroke	CIHI-DAD 2003-2010 RCSN 1 July 2003 - 31 March 2011
58	Impact of the JUPITER trial on prescribing patterns of statins for primary prevention	CIHI-DAD 1998-2011 CIHI-SDS 1998-2011 ODB 2002-2011 RPDB
59	The ability of routine renal imaging to prevent the morbidity and mortality of urinary stone disease in spinal cord injury patients	CIHI-DAD 1992-2011 CIHI-SDS 1992-2011 CIHI-NACRS 2001-2011 CIHI-NRS 2000-2011 OHIP 1992-2011 RPDB
60	Validation of deceased organ donor codes in Ontario, Canada	CIHI-DAD 1991-2011 CIHI-SDS 1991-2011 OHIP 1991-2011 RPDB Trillium Gift of Life Network (TGLN) 2006-2011
61	SES and utilization of CT scanning in the emergency department	CIHI-NACRS 2009-2011 OHIP 2009-2011 RPDB
62	Access to neonatal follow-up care following the implementation of the Canadian Peadiatric Society's 2007 hyperbilirubinemia guidelines	CIHI-DAD 2003-2010 CIHI-NACRS 2003-2010 OHIP 2003-2010 RPDB IPDB MOMBaby Universal Bilirubin Screening Hospital Survey

#	Project Title	ICES Data
63	Nighttime medical encounters by attending physicians/surgeons and outcomes of procedures performed on the subsequent day	CIHI-DAD 2005-2010 CIHI-SDS 2005-2010 CIHI-NACRS 2005-2010 OHIP 2005-2010 RPDB IPDB
64	Impact of income on mammogram use in women with diabetes	CIHI-DAD 1991-2011 CIHI-SDS 1991-2011 CIHI-NACRS 1991-2011 CIHI-CCRS 1991-2011 CIHI-NRS 1991-2011 OHIP 1991-2011 RPDB CAPE IPDB ODD OCR 1964-2011 OBSP
65	Clinical outcomes study in high risk coronary intervention	CIHI-DAD 2000-2011 OHIP 2000-2011 RPDB UHN PCI Database 2000-2011 UHN CABG Database 2000-2010
66	Clinical outcomes of 1st and 2nd generation drug-eluting stents in patients with chronic kidney disease undergoing percutaneous coronary intervention	CIHI-DAD 2000-2011 OHIP 2000-2011 RPDB UHN PCI Database 2000-2010
67	Immigration to Canada and other industrialized countries and maternal and infant morbidity	CIHI-DAD 1988-2011 OHIP 1991-2011 RPDB MOMBaby LIDS 1985-2010
68	Developmental screening and BMI in children: EMR chart abstraction validation	CIHI-DAD 1988-2013 OHIP 1988-2013 RPDB EMRALD 1990-2013
69	Ministry of Education special education funding model	CIHI-DAD 2006-2011 CIHI-NACRS 2006-2011 OHIP MOMBaby
70	Mental health and addictions in youth: EMR chart abstraction validation	CIHI-DAD 1988-2013 CIHI-SDS 1988-2013 CIHI-NACRS 1988-2013 ODB 1988-2013 OHIP 1991-2013 RPDB EMRALD 1990-2013

#	Project Title	ICES Data
71	Economic evaluation of meningococcal serogroup B childhood vaccination in Ontario (Revised title: Assessing the health and economic burden of meningococcal infection to inform meningococcal serogroup B childhood vaccination in Ontario)	CIHI-DAD 1999-2010 CIHI-SDS 1999-2010 CIHI-NACRS 1999-2010 CIHI-CCRS 1999-2010 CIHI-NRS 1999-2010 ODB 1999-2010 OHIP 1999-2010 HCD 1999-2010 RPDB Public Health Ontario Laboratory (PHOL)/Integrated Public Health Information System (iPHIS) dataset
72	Informational continuity between primary care and specialist mental health: Development of a tool for quality improvement	EMRALD 2010-2010
73	The epidemiology and economics of ankle injuries: Implications for health policy	CIHI-DAD 2003-2011 CIHI-NACRS 2003-2011 OHIP 2003-2011 RPDB ERCLAIM 2003-2011
74	Child and youth concussion and other head injuries in Ontario	CIHI-NACRS 2003-2010 OHIP 2003-2010 RPDB
75	Risk of tendon injury in older individuals receiving fluoroquinolone medications	CIHI-DAD 1998-2011 CIHI-SDS 1998-2011 CIHI-NACRS 2002-2011 ODB 2002-2011 OHIP 1998-2011 RPDB IPDB Asthma COPD ODD OCR 1998-2011 CORR 1998-2010
76	Validating and costing liver metastases and their resection, for economic evaluation of colorectal cancer screening in Ontario	CIHI-DAD 1988-2011 CIHI-SDS 1988-2011 CIHI-NACRS 1988-2011 CIHI-CCRS 1988-2011 CIHI-NRS 1988-2011 OHIP 1992-2011 HCD 1992-2011 OCR 1964 - 2011
77	Antipsychotic agents and risk of hyperglycaemic emergencies	CIHI-DAD 1991-2010 CIHI-SDS 1991-2010 CIHI-NACRS 2002-2010 ODB 1991-2010 OHIP 1991-2010 OMHRS 2005-2010 RPDB ODD

#	Project Title	ICES Data
78	Trimethoprim-sulfamethoxazole induced hypoglycemia in elderly patients	CIHI-DAD 1990-2011 CIHI-NACRS 2000-2011 ODB 1990-2011 OHIP 1991-2011 RPDB ODD
79	Adalat XL and the risk of bowel obstruction	CIHI-NACRS 2000-2011 ODB 1992-2011 OHIP 1992-2011 RPDB OCR 1992 - 2011
80	Improving the quality of colonoscopy: The development and pilot testing of an endoscopist audit and feedback report derived from health administrative data	CIHI-DAD 2010-2011 CIHI-SDS 2010-2011 OHIP 2010-2011 RPDB CAPE IPDB OCR 2010-2011 CIRT
81	Ontario CABG, valve and PCI report cards	CIHI-DAD 2008-2011 CIHI-SDS 2008-2011 CIHI-NACRS 2008-2011 ODB 2008-2011 OHIP 2008-2011 RPDB ODD CCN 2008-2011
82	Examining risk of institutionalization among community based home care clients	CIHI-DAD 2006-2011 CIHI-SDS 2006-2011 CIHI-NACRS 2006-2011 ODB 2006-2011 OHIP 2006-2011 HCD 2006-2011 RPDB CAPE RAI-Home Care 2007-2011
83	Schizophrenia understood in the perinatal period: Psychiatric outcomes and reproductive trajectories (SUPPORT) phase 2	CIHI-DAD 1997-2011 CIHI-SDS 1997-2011 CIHI-NACRS 1997-2011 ODB 1997-2011 OHIP 1997-2011 OMHRS 1997-2011 RPDB MOMbaby
84	Risk of readmission to acute psychiatric units in Ontario: A gender-based analysis	CIHI-DAD 2003-2011 CIHI-SDS 2003-2011 CIHI-NACRS 2003-2011 ODB 2003-2011 OHIP 2003-2011 OMHRS RPDB

#	Project Title	ICES Data
85	Measuring the quality of systemic therapy for early breast cancer using population level quality indicators	CIHI-DAD 2007-2009 CIHI-NACRS 2007-2009 ODB 2007-2009 OHIP 2007-2009 RPDB CAPE IPDB OCR 2007-2009 NDFP 2007-2010 CHCCDB 2007-2010
86	New opioid use and motor vehicle trauma - A cohort study	CIHI-DAD 1999-2011 CIHI-NACRS 2001-2011 ODB 1999-2011 OHIP 1999-2011 RPDB IPDB OCR 1980-2011
87	Appropriate dosing of antivirals in patients with CKD	CIHI-DAD 1997-2010 CIHI-SDS 1997-2010 CIHI-NACRS 1997-2010 ODB 2001-2010 OHIP 1997-2010 RPDB Gamma Dynacare, CERNER 2002-2010
88	Appropriate dosing of gabapentin in patients with CKD	CIHI-DAD 1997-2010 CIHI-SDS 1997-2010 CIHI-NACRS 1997-2010 ODB 2001-2010 OHIP 1997-2010 RPDB Gamma Dynacare, CERNER 2002-2010
89	Arterial dissection and stroke: Treatment and recurrence	CIHI-DAD 2000-2012 CIHI-NACRS 2000-2012 RPDB RCSN 2000 - 2012
90	Transitions across the health care system and risk of rehospitalization in older women and men	CIHI-DAD 2003-2012 CIHI-NACRS 2003-2012 CIHI-CCRS 2007-2012 ODB 2003-2012 OHIP 2003-2012 HCD 2007-2012 RPDB CHF COPD ODD CPRO
91	Association between beta blocker usage and cancer survival in Ontario	CIHI-DAD 1990-2011 CIHI-NACRS 2002-2011 ODB 1992-2011 OHIP 1992-2010 RPDB Hypertension OCR 1992-2011

#	Project Title	ICES Data
92	Peritoneal dialysis catheter placement, use and technique failure in Ontario	CIHI-DAD 1991-2011 CIHI-SDS 1991-2002 CIHI-NACRS 2002-2011 OHIP 1991-2011 RPDB IPDB CHF ODD Canadian Organ Replacement Register 2002-2011
93	Statins and new-onset diabetes in an Ontario population	CIHI-DAD 1996-2011 CIHI-SDS 1996-2011 CIHI-NACRS 2000-2011 ODB 1996-2011 OHIP 1996-2011 RPDB ODD
94	Feasibility of using EMRALD to extract bone mineral density reports, risk factors and medications for osteoporosis	OHIP 1991-2015 EMRALD 1988-2015
95	Living to a hundred: Rethinking our definition of old	CIHI-DAD 1994-2011 CIHI-SDS 1994-2011 CIHI-NACRS 2002-2011 CIHI-CCRS 1994-2011 ODB 1994-2011 OHIP 1994-2011 HCD 2005-2011 RPDB IPDB Asthma CHF COPD ODD OCR 1964-2010 RAI-HC 2008-2011
96	Intensity of end-of-life care in Ontario: Defining changing patterns, risk factors and targets for intervention	CIHI-DAD 2002-2011 CIHI-SDS 2002-2011 CIHI-NACRS 2002-2011 CIHI-CCRS 2002-2011 ODB 2002-2011 OHIP 2002-2011 HCD 2002-2011 LOC 2002-2011 RPDB
97	Population based analysis on the use of ultrasound imaging in the assessment of children with cryptorchidism	CIHI-DAD 2000-2011 CIHI-SDS 2000-2011 CIHI-NACRS 2002-2011 OHIP 2000-2011 RPDB
98	Head trauma injuries related to motor vehicles	CIHI-DAD 2006-2010 CIHI-NACRS 2006-2010 OHIP 2006-2010 RPDB
99	Appropriateness of imaging use in Canada: A systematic review	CIHI-DAD 2002-2010 OHIP 2001-2011 RPDB

#	Project Title	ICES Data
100	Eating disorders: Mortality and morbidity follow-up	CIHI-DAD 1988-2012 CIHI-SDS 1991-2012 CIHI-NACRS 2000-2012 OMHRS 2005-2012 RPDB ORGD 1993 - 2012 OCR 1964-2010 Ontario Population Data 1993-2012 Postal Code Conversion Data 1993-2012
101	Measures of community-hospital transitions for children/youth with mental health problems (AHRQ request, CAMH SISC)	CIHI-DAD 2010-2011 CIHI-NACRS 2010-2011 OHIP 2010-2011 OMHRS 2010-2011
102	A population-based study of adherence to atrial fibrillation therapies	CIHI-DAD 2000-2012 CIHI-NACRS 2000-2012 ODB 2000-2012 OHIP 2000-2012 RPDB ODD
103	A patient centred approach toward wait times in the surgical management of breast cancer in the province of Ontario	CIHI-DAD 2002-2009 CIHI-SDS 2002-2009 CIHI-NACRS 2002-2009 CIHI-CCRS 2002-2009 OHIP 2002-2009 RPDB OCR 2002-2009 Ontario Surgical Wait List Database 2002-2009
104	Understanding diagnostic episodes of care in patients with early versus late cancers	CIHI-DAD 2007-2014 CIHI-SDS 2007-2014 CIHI-NACRS 2007-2014 ODB 2007-2014 OHIP 2007-2014HCD 2007-2014 RPDB CAPE IPDB CPDB OCR 2007-2013 OBSP Citizenship Immigration Canada 2000-2013Census, Acute Hospital Hospital Database, Contact PopSubLHIN PSTLyear
105	Diabetes and cardiovascular events in older myocardial infarction patients prescribed intensive-doses and moderate-dose statins	CIHI-DAD 2004-2010 ODB 2004-2010 RPDB OMID
106	Exploration of the pressure ulcer and related skin problems across the spectrum of healthcare settings in Ontario using administrative data	CIHI-DAD 2006-2012 CIHI-SDS 2006-2012 CIHI-NACRS 2006-2012 CIHI-CCRS 2006-2012 OHIP 2005-2012 HOBIC 2006-2012 RPDB CCRS (WR) CCRS_LTC (WR)

#	Project Title	ICES Data
107	Closing the quality feedback loop: A web-based forum to improve the quality of care and outcomes of the Toronto heart attack collaborative (THAC) regional STEMI	CIHI-DAD 2010-2012 CIHI-SDS 2010-2012 CIHI-NACRS 2010-2012 ODB 2010-2012 OHIP 2010-2012 RPDB
108	Gastric band removals in Ontario	CIHI-DAD 2004-2012 CIHI-SDS 2004-2012 CIHI-NACRS 2004-2012 OHIP 2004-2012 RPDB
109	Nurse staffing to clinical outcomes in acute-care HOBIC settings in Ontario	CIHI-DAD 2008-2011 RPDB MIS 2008-2011 HOBIC 2008-2011
110	Hospital specific death or urgent readmission rates vary extensively based on the methods used to calculate them	CIHI-DAD 2005-2010 CIHI-NACRS 2005-2010 RPDB
111	Rivaroxaban drug utilization in Ontario: 2009 to 2011	CIHI-DAD 2009-2011 ODB 2009-2011 OHIP 2009-2011 RPDB
112	Socioeconomic status, quality of primary care and survival following acute myocardial infarction: A ten-year follow-up of the SESAMI study	CIHI-DAD 1991-2014 CIHI-SDS 1991-2014 CIHI-NACRS 2001-2014 ODB 1999-2014 OHIP 1991-2014 HCD 1999-2014RPDB IPDB CPDB Asthma CHF COPD Hypertension ODD OMID Vital Stats 1999-2014
113	A mixed methods study: Examining the relationship between therapeutic self-care and adverse events for home care clients in Ontario	CIHI-DAD 2010-2011 CIHI-NACRS 2010-2011 RPDB HOBIC RAI-HC 2010-2011
114	Association of domperidone with serious abnormal heart rhythms and sudden cardiac death	CIHI-DAD 1998-2011 CIHI-SDS 1998-2011 CIHI-NACRS 2002-2011 ODB 2002-2011 OHIP 1998-2011 RPDB CHF COPD ODD OCR 1964-2011

#	Project Title	ICES Data
115	Adverse outcomes with macrolide antibiotics in patients o no CYP3A4 interacting medications	CIHI-DAD 1998-2010 CIHI-SDS 1998-2010 CIHI-NACRS 1998-2010 ODB-2002-2010 OHIP-1998-2010 RPDP Gamma-Dynacare, Cerner 2002-2010
116	Trends in human immunodeficiency virus (HIV) prevalence, incidence and mortality in Ontario, Canada, 1996-2009	CIHI-DAD 1992 - 2012 OHIP 1992 - 2012 RPDB CIHI-DAD 1992 - 2012 Canada Census (for SES) to 1991
117	Pregnancy outcomes among women using antipsychotic drugs	CIHI - DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI - NACRS 2002 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 OMHRS 2005 - 2011 RPDB MOMBaby ODD
118	Evaluation of the Centre for Movement Disorders: Does Parkinson's disease multidisciplinary team care improve outcomes?	CIHI-DAD 1988 - 2011 CIHI - NACRS 2000 - 2011 OHIP 1991 - 2011
119	Coroner data update: Opioid-related deaths	RPDB Chart Abstraction
120	Paying for primary care: Relationship between incentives and patient profiles	CIHI-DAD 2000 - 2014 CIHI-SDS 2000 – 2014 CIHI-NACRS 2000 - 2014 CIHI-CCRS 2000 - 2014 CIHI-NRS 2000 - 2014 ODB 2000 - 2014 OHIP 2000 - 2014 HCD 2000 - 2014 LOC 2000 - 2014 OMHRS 2000 - 2014 RPDB CAPE IPDB Asthma CHF CPDB COPD Hypertension ODD OBSP Cytobase
121	Trauma risks after intra-vitreal anti-angiogenic drugs (TRIAD Study)	CIHI - DAD 2001 - 2012 CIHI - SDES 2001 - 2012 CIHI - NACRS 2001 - 2012 ODB 2001 - 2012 OHIP 2001 - 2012
122	Total joint arthroplasty of the hip and knee in rheumatoid arthritis	CIHI - DAD 1991 - 2010 CIHI - NACRS 2002 - 2010 ODB 2001 - 2010 OHIP 1991 - 2010 RPDB

#	Project Title	ICES Data
123	Comparison of urologic related complications between patients treated with surgery or radiation	CIHI-DAD 1990-2009 CIHI-SDS 1990-2009 CIHI NACRS 1990-2009 CIHI-CCRS 1990-2009 CIHI-NRS 1990-2009 OHIP 1990-2009 RPDB OCR 1990 - 2009
124	Identifying barriers to participation to colorectal screening	CIHI-DAD 1992-2011 OHIP 1992-2011 RPDB CAPE IPDB OCR 1964 - 2011
125	The impact of ethnicity on breast cancer and colorectal cancer stage at diagnosis	CIHI-DAD 1999 - 2010 CIHI-SDS 1999 - 2010 CIHI-NACRS 2006-2010 ODB 2004 - OHIP 2002-2010 RPDB IPDB CCO 2005 - 2010 CRC-ICES Stage Data Ethnicity Surname Algorithm Data OCR 1964 - 2010 OBSP
126	Impact of clinical data on profiling hospitals with respect to stroke outcomes: Data from the Ontario Stroke Audit	CIHI-DAD 2010 - 2011 RPDB RCSN 2010 - 2011
127	Evaluation of out-of-country care for eating disorders	CIHI-DAD 1995-2011 CIHI-NACRS 2003-2011 OHIP 1995-2011 OMHRS 2005-2011 RPDB IPDB CPDB
128	The effect of cardiac rehabilitation on health service utilization and the secondary prevention of death and cardiovascular disease	CIHI - DAD 1991 - 2013 CIHI - SDS 1991 - 2013 CIHI - NACRS 1991 - 2013 CIHI - CCRS 1991 - 2013 CIHI - NRS 1991 - 2013 ODB 1991 - 2013 OHIP 1991 - 2013 RPDB IPDB CPDB Asthma CHF COPD Hypertension ODD OMID Vital Stats (when available)

#	Project Title	ICES Data
129	Which patients are child psychiatrists seeing?: Exploring the gap between child psychiatry supply and unmet need	CIHI-DAD 2006 - 2010 CIHI-NACRS 2006 - 2010 OHIP 2006 - 2010 OMHRS 2006 - 2010 IPDB CPDB OPHRDC 2006 - 2010
130	Refining a treatment favorability index using propensity-matched observational data	RPDB RCSN 2003 - 2008
131	Severe hyperglycemia with calcium channel blockers among older Ontario residents: A population-based study	CIHI-DAD 1997 - 2011 CIHI-NACRS 2000 - 2011 ODB 1997 - 2011 OHIP 1997 - 2011 RPDB ODD
132	The short-term impact of switching from OxyContin to OxyNEO	CIHI - DAD 2006 - 2012 ODB 2007 - 2012 OHIP 2006 - 2012 RPDB OCR 1964 - 2012
133	Creating an information system from a primary care electronic medical record administrative data linked database to improve rheumatoid arthritis surveillance and quality of care	CIHI-DAD 1988 - 2015 CIHI-SDS 1991 - 2015 CIHI-NACRS 2003 - 2015 ODB 1990 - 2015 OHIP 1991 - 2015 RPDB IPDB Other: EMRALD 1988 - 2015
134	Relationship between PCI appropriateness and improvements in quality of life	CIHI-DAD 2007-2012 CIHI-SDS 2007 - 2012 CIHI-NACRS 2007 - 2012 ODB 2007 – 2012 OHIP 2007 - 2012 LOC RBDP
135	Contemporary survival rates of patients with metastatic hormone refractory prostate cancer	CIHI-DAD 1995 - 2010 CIHI-SDS 1995 - 2010 CIHI-NACRS 2000 - 2010 CIHI - CCRS 1995 - 2010 CIHI - NRS 1995 - 2010 ODB 1995 - 2010 OHIP 1995 - 2010 RPDB Other - NDFP 1995 - 2010 OCR 1995 - 2010
136	Assessing the effectiveness of trivalent inactivated influenza vaccines in preventing serious influenza outcomes among older adults in Ontario, Canada. Part 2: Using cause-specific mortality data and region-specific analyses	OHIP 1993 - 2009 RPDB Cause Specific mortality data when it becomes available 1993 - 2009

#	Project Title	ICES Data
137	Treatment and outcomes of head & neck cancer with regionalization in Ontario	CIHI-DAD 1992 - 2010 CIHI-SDS 1992 - 2010 CIHI-NACRS 2000 - 2010 OHIP 1992 - 2010 HCD 1992 - 2010 RPDB IPDB SDS 1992 - 2010 OCR 1992 - 2010
138	Site of hospital readmission and mortality	CIHI - DAD 1994 - 2012 ODB 1994 - 2012 OHIP 1994 - 2012 RPDB IPDB
139	Trends and costs of spinal fusion surgery in Ontario	CIHI -DAD 1991 - 2011 CIHI - SDS 1991 - 2011 ODB 1991 - 2011 OHIP 1991 - 2011 RPDB OCCI 2005 - 2011
140	Care pathways of psychiatric patients in provincial correctional centres	CIHI - DAD 2004 - 2010 OHIP 2004 - 2010 OMHRS 2004 - 2010 RPDB IPDB
141	An analysis of the outcomes and implementation of a universal funding program for insulin pumps for youth with type 1 diabetes	CIHI - DAD 2004 - 2012 CIHI - NACRS 2004 - 2012 OHIP 2004 - 2012 RPDB IPDB CPDB ODD Survey Assistive Devices Program 2004 - 2012
142	Acute dialysis following non-urgent surgery after epidural anesthesia or analgesia: Incidence, trends, risk factors, and outcomes	CIHI - DAD 2000 - 2011 ODB 2000 - 2010 OHIP 2000 - 2011 RPDB
143	Adherence to prescription drug recommendations made on a provincial formulary for aliskiren	CIHI - DAD 2005 - 2011 ODB 2007 - 2011 OHIP 2007 - 2011 RPDB IPDB Gamma-Dynacare 2007 - 2011
144	Chronic kidney disease quality of care indicators	CIHI - DAD 1996 - 2011 CIHI - NACRS 1996 - 2011 ODB 2001 - 2011 OHIP 1996 - 2011 RPDB Gamma-Dynacare, Cerner, CORR 2001 - 2011
145	EMR implementation analysis: Family physician billings	OHIP 1994/95 - 2011/12 CAPE IPDB EMRALD 1995 - 2011

#	Project Title	ICES Data
146	A population-based study of HIV-associated maternal and neonatal health using Ontario's administrative databases	CIHI-DAD 1997 - 2012 ODB 1997 - 2012 OHIP 1997 - 2012 RPDB Hypertension MOMBaby ODD Census CIC 1997 - 2012
147	The impact of electroconvulsive therapy on medical morbidity in Ontario	CIHI - DAD 1998 - 2011 CIHI - NACRS 2002 - 2011 ODB 2002 - 2011 OHIP 2002 - 2011 OMHRS 2005 - 2011 RPDB CHF COPD Hypertenstion ODD
148	Acute dialysis following non-urgent surgery: Incidence, trends, risk factors, and outcomes. Pre-operative ACEi/ARB use	CIHI-DAD 1992 - 2011 ODB 1994 - 2010 OHIP 1992 - 2011 RPDB
149	The gender gap in cardiovascular risk in adults with and without diabetes	CIHI-DAD April 1, 1997 - March 31, 2011 OHIP April 1, 1997 - March 21, 2011 RPDB IPDB ODD
150	Evaluation of drugs for rare diseases (Ontario Public Drug Program (OPDP))	CIHI-DAD 2008 - 2011 CIHI-SDS 2008 - 2011 CIHI-NACRS 2008 - 2011 ODB 2009 - 2011 RPDB
151	Infant outcomes in the first year of life associated with maternal H1N1 vaccination	CIHI-DAD 2010 - 2011 CIHI-NACRS 2010 - 2011 OHIP 2010 - 2011 RPDB Better Outcomes and Registry Network (BORN) Ontario birth record 2010 - 2011 MOMBaby
152	Understanding rehabilitation transition patterns for acute stroke patients discharged from the hospital: A discrete choice analysis	CIHI - DAD 2010 - 2011 CIHI - CCRS 2010 - 2011 CIHI - NRS 2010 - 2011 RPDB Survey RCSN 2010 - 2011 OSA 2010 - 2011
153	Statins and herpes zoster reactivation	CIHI - DAD 1992 - 2011 CIHI - NACRS 2000 - 2011 ODB 1996 - 2011 OHIP 1992 - 2011 RPDB ODD CONTACT Database 1992 - 2011

#	Project Title	ICES Data
154	Prevalence and/or incidence of ischemic heart disease, cerebrovascular disease and COPD for Peel Public Health	CIHI-DAD 2002 - 2008 OHIP 2002 - 2008 RPDB
155	Community Health Centre (CHC) data analysis - describing non OHIP residents	CIHI - DAD 2008 - 2010 CIHI - NACRS 2008 - 2010 OHIP 2008 - 2010 OMHRS 2008 - 2010 RPDB CAPE OTHER - CHC
156	Pregnancy and injury from traffic yesterday	CIHI - DAD 1994 - 2012 CIHI - NACRS 1994 - 2012 ODB 1994 - 2012 OHIP 1994 - 2012 RPDB Survey: CCHS
157	Testosterone therapy and cardiovascular events	CIHI - DAD 1992 - 2011 ODB 1996 - 2011 OHIP 1992 - 2011 RPDB Hypertension ODD CONTACT Database 1992 - 2011 HIV Database 1996 - 2011
158	Primary care for chronic kidney disease patients who begin dialysis in hospital	CIHI - DAD 1991 - 2011 CIHI - NACRS 2002 - 2011 OHIP 1991 - 2011 RPDB IPDB
159	Inhaled anticholinergics and risk of urinary tract infection in individuals with chronic obstructive pulmonary disease (COPD)	CIHI - DAD 1991 - 2010 CIHI - SDS 1991 - 2010 CIHI - NACRS 2002 - 2010 ODB OHIP 1991 – 2010 OMHRS 2005 - 2010 RPDB IPDB COPD ODD ORGD 1991 - 2010
160	Secular trends in pregnancy-related acute kidney injury	CIHI-DAD 1991 - 2011 OHIP 1991 - 2011 RPDB MOMBaby ODD

#	Project Title	ICES Data
161	HSPRN multiple chronic disease cohort study	CIHI-DAD 1988 - 2011 CIHI-SDS 1988 - 2011 CIHI - NACRS 2003 - 2011 CIHI - CCRS 2005 - 2011 CIHI-NRS 2005 - 2011 ODB 1988 - 2011 OHIP 1988 - 2011 HCD 2005 - 2011 OMHRS 2006 - 2011 RPDB CAPE Asthma CHF COPD Hypertension ODD OMID RAI-Home Care 2002 - 2011
162	Ethnic disparities in diabetic nephropathy in Ontario	CIHI-DAD 1995 - 2011 OHIP 1995 - 2011 RPDB Validated South Asian Surname List(Shah et al BMC 2010) ODD
163	Cardiotoxicity following adjuvant chemotherapy for breast cancer: A population-based analysis	CIHI-DAD 01-Jan-2007 to 31-Dec-2009 CIHI-NACRS 01-Jan-2007 to 31-Dec-2009 ODB 01-Jan-2007 to 31-Dec-2009 OHIP 01-Jan-2007 to 31-Dec-2009 HCD 01-Jan-2007 to 31-Dec-2009 IPDB CPDB CHF OCR 2007 - 2009
164	The relationship between living alone and quality of care and outcomes following stroke	CIHI-DAD 2003 - 2011 RPDB RCSN 2003 - 2008 Registry
165	Examining the impact of stroke on functional ability taking into account prior functional ability	RCSN 10 to 11 OSA
166	Sex differences in the risk of stroke among the elderly with atrial fibrillation in Ontario - a competing risk analysis	CIHI - DAD 1998 - 2007 ODB 1998 - 2007 RPDB Hypertension ODD
167	Management and outcomes of testicular cancer in routine clinical practice: A population based outcomes study	CIHI-DAD 1994 - 2011 OHIP CIHI-SDS 1992 - 2012 (WR) OCR

#	Project Title	ICES Data
168	Use of antidepressants in older adults with chronic kidney disease (CKD) in Ontario	CIHI - DAD 1 Apr 1998 - 31 Mar 2011 CIHI - SDS 1 Apr 1998 - 31 Mar 2011 CIHI-NACRS 1 Apr 2002 - 31 Mar 2011 CIHI - CCRS 1 Apr 1999 - 31 Mar 2011 ODB 1 Apr 2002 - 31 Mar 2011 OHIP 1 Apr 1998 - 31 Mar 2011 OMHRS 1 Apr 1998 - 31 Mar 2011 RPDB IPDB Cerner Database 2001 - 2010 Gamma-Dynacare 2002 - 2010 ODD
169	UWO & Queen's University evaluation of the Quality Improvement & Innovation Partnership (QIIP) learning collaboratives - Administrative health data component	CIHI - DAD 1 Apr 2006 - 30 Jun 2012 CIHI - NACRS 1 Apr 2006 - 30 Jun 2012 ODB 1 Apr 2006 - 30 Jun 2012 OHIP 1 Apr 2006 - 30 Jun 2012 RPDB CAPE IPDB CPDB ODD CPSO OCR 1964 - 2010 OBSP Cytobase
170	Vericella zoster related conditions, Ontario, 1992 - 2010: Vericella vaccine program impact assessment	CIHI - DAD 1992 - 2010 CIHI - NACRS 2002 - 2010 OHIP 1992 - 2010 RPDB
171	Informing population-based health strategies for the prevention of diabetes using a population risk tool	RPBD ODD Survey: NPHS Survey: CCHS
172	Support for organ and tissue donation amongst new Ontarians: A population-based study	CIHI - DAD 1990 - 2010 OHIP 1990 - 2010 RPDB CIC Organ Donor Registration Status 1995dsa - 2012 MOHLTC DSA
173	Prescribing of OxyNEO and EAP criteria	CIHI - DAD 1998 - 2011 ODB 1998 - 2012 OHIP 1998 - 2012
174	Risk of acute kidney injury associated with use of proton pump inhibitors among elderly patients	CIHI - DAD 1997 – 2012 ODB 1997 - 2012 RPDB Hypertension ODD CONTACT
175	Management and health outcomes in adolescents who develop malignancies	CIHI-DAD 1992 - 2010 CIHI-SDS 1992 - 2010 CIHI-NACRS 1992 - 2010 OHIP 1992 - 2010

#	Project Title	ICES Data
176	Assessing the quality of colonoscopy: Validation of new colonoscopy data elements from the Colonoscopy Interim Tool (CIRT v2)	CIHI-DAD 01-OCT-2009 TO 31-DEC-2011 CIHI-SDS 01-OCT-2009 TO 31-DEC-2011 CIHI-NACRS 01-OCT-2009 TO 31-DEC-2011 OHIP 01-OCT-2009 TO 31-DEC-2011 RPDB IPDB OCR 01-Oct-2009 - 31-Dec-2011 CCO-Colonoscopy Interim Reporting Tool (CIRT) 01-Oct-2009 - 31-Dec-2011
177	Ontario cancer Screening Research Network project # N: A case control study of cervix cancer mortality by age	CIHI - DAD 1988 - 2012 CIHI - SDS 1988 - 2012 CIHI - NACRS 1988 - 2012 CIHI - CCRS 1988 - 2012 OHIP 1992 - 2012 RPDB OCR 1964 - 2010 Cytobase
178	Intentional self-poisoning (ISP): Identifying risk factors for future suicide and repeat attempts to facilitate secondary prevention - A population - based study	CIHI - DAD 1992 - 2012 CIHI - NACRS 2002 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB ORGD 1992-2012
179	Antidepressant use and risk of adverse outcomes in the elderly after a hip fracture	CIHI - DAD 1997 - 2011 CIHI - SDS 1997 - 2011 CIHI - NACRS 2002 - 2011 CIHI- NRS 2002 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 OMHRS 2005 - 2011 RPDB Hypertension ODD
180	The burden of asthma in Ontario residents of South Asian descent	CIHI - DAD 1996 - 2011 CIHI - SDS 1996 - 2011 CIHI-NACRS 2002 - 2011 OHIP 1996 - 2011 RPDB Visible Minorities Database 1996 - 2011 Asthma
181	Risk of pneumonia associated with use of angiotensin converting enzyme (ACE) inhibitors and angiotensin receptor blockers (ARB)	CIHI - DAD 1998 - 2011 CIHI - NACRS 1998 - 2011 ODB 1998 - 2011OHIP 1998 - 2011 RPDB IPDB CERNER, Gamma-Dynacare Lab Data 1999 - 2011
182	Isotretinoin use among Ontario women receiving social assistance	ODB 1997 - 2011 RPDB

#	Project Title	ICES Data
183	Population based associations of chronic lymphoncytic leukemia and the metabolic syndrome	CIHI - DAD 2000 - 2010 CIHI - SDS 2000 - 2010 CIHI - NACRS 2000 - 2010 CIHI - CCRS 2000 - 2010 CIHI - NRS 2000 - 2010 ODB 2000 - 2010 OHIP 2000 - 2010 Hypertension ODD OCR 2000 - 2010
184	Enhanced evaluation and uptake of the fee code for the 18-month enhanced well baby visit	CIHI - DAD 1991 - 2012 OHIP 2008 - 2012 RPDB CAPE IPDB CPDB MOMBaby CIC
185	Lithium and renal disease in older adults - A cross-sectional study	CIHI - DAD 2005 - 2011 CIHI - SDS 2005 - 2011 CIHI - NACRS 2005 - 2011 ODB 2005 - 2011 OHIP 2005 - 2011 OMHRS 2005 - 2011 RPDB IPDB CHF ODD Hypertension
186	Cardiovascular & renal outcomes following partial vs radical nephrectomies	CIHI - DAD 1997 - 2012 CIHI - SDS 1997 - 2012 ODB 1997 - 2012 OHIP 1997 - 2012 RPDB IPDB Cerner, Gamma-Dynacare 2002-2012 ODD London Hospitals Data Abstraction
187	Pre-hospital home care in patients discharged from hospital to long-term care (AHRQ request)	CIHI-DAD 2009 - 2011 CIHI-NACRS 2009 - 2011 ODB 2009 - 2011 OHIP 2009 - 2011 HCD 2009 - 2011 RPDB CPDB CPRO 2009-2011
188	Evidence Development and Standards (EDS), Health Quality Ontario (HQO): Annual health exam tests and procedures	OHIP 2005 - 2012RPDB
189	Glucocoricoid-induced osteoporosis (GIOP)	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 1991 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 RPDB

#	Project Title	ICES Data
190	Does neighbourhood activity friendliness affect the age of asthma development and frequency of asthma exacerbations?	CIHI-DAD 1997/98 - 2010/11 CIHI-NACRS 1997/98 - 2010/11 OHIP 1997/98 - 2010/11 RPDB Activity Friendliness Index ON Marginalization Indices 2001-2006 Asthma
191	Cardiac arrest in ischemic stroke (CAIS study): Predisposing factors, clinical features, and process measures	RPDB RCSN 2003 - 2008
192	Operative and non-operative treatment of clavicle fractures in Ontario: A population based study	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 CIHI-NACRS 2002 - 2012 OHIP 2002 - 2012
193	Long-term survivorship of high tibial osteotomy and distal femoral varus osteotomy to total knee replacement in Ontario, Canada	CIHI-DAD July 1991 - June 2010 CIHI-SDS July 1991 - June 2010 OHIP July 1994 - June 2012
194	The effects of quadrivalent HPV vaccination on adolescent health and health behaviours: The Ontario grade 8 HPV vaccine cohort study	CIHI-DAD 1989 - 2015 CIHI-SDS 1989 - 2015 CIHI-NACRS 2000 - 2015 ODB 1989 - 2015 OHIP 1989 - 2015 RPDB IPDB CPDB IRIS 1989 - 2015 MOMBaby
195	Repeat emergency department visits among long-term care residents in Ontario	CIHI - DAD 1 April 2004 - 31 March 2012 CIHI - SDS 1 April 2004 - 31 March 2012 CIHI - NACRS 1 April 2004 - 31 March 2012 CIHI - CCRS 1 April 2004 - 31 March 2012 ODB 1 April 2008 - 31 March 2012 OHIP 1 April 2004 - 31 March 2012 RPDB Hypertension ODD
196	Health Quality Ontario stroke analysis	CIHI - DAD 2001 - 2011 CIHI - NACRS 2001 - 2011 CIHI - CCRS 2002 - 2011 ODB 2002 - 2011 OHIP 2002 - 2011 HCD 2002 - 2011 RCSN 2002 - 2011

#	Project Title	ICES Data
197	Practice profiles for community health centres and aboriginal health access centres	CIHI - DAD 2007 - 2012 CIHI - NACRS 2007 - 2012 ODB 2007 - 2012 OHIP 2007 - 2012 RPDB CAPE IPDB CPDB Asthma CHF COPD Hypertension ODD OCR 1964 – 2010 OBSP Cytobase
198	The incidence of diabetes among colorectal cancer survivors	CIHI - DAD April 1,1997 - March 31, 2012 CIHI - SDS April 1,1997 - March 31, 2012 CIHI - NACRS April 1, 2000 - March 31, 2012 ODB April 1, 2001 - March 31, 2012 OHIP April 1, 1997 - March 31, 2012 RPDB CAPE IPDB ODD OCR 1964 - 2011 NDFP 2001 - 2012
199	Deriving and validating a method to identify surgical site infections using administrative data	CIHI - DAD 2008 - 2010 CIHI - SDS 2008 - 2010 CIHI - NACRS 2008 - 2010 OHIP 2008 - 2010 RPDB
200	Phase-specific and lifetime medical costs of care for childhood cancer in British Columbia and Ontario	CIHI - DAD Jan 1st 1994 - June 30th 2012 CIHI - SDS Jan 1st 1994 - June 30th 2012 CIHI - NACRS Jan 1st 1994 - June 30th 2012 CIHI - CCRS Jan 1st 1994 - June 30th 2012 ODB Jan 1st 1994 - June 30th 2012 OHIP Jan 1st 1994 - June 30th 2012 HCD Jan 1st 1994 - June 30th 2012 RPDB OCR 1994 - 2012 ALR, NDFP, POGONIS 1994 - 2012
201	Rate of breast cancer screening in Ontario, using mammography, according to country of origin and region	CIHI - DAD 1988 - 2012 OHIP 1991 - 2012 RPDB CAPE IPDB CPDB OCR 1991 - 2012 OBSP
202	Mental health service use patterns for immigrant groups and long term residents in Ontario	CIHI - DAD 1991 - 2011CIHI - NACRS 1991 - 2011OHIP 1991 - 2011OMHRS 1991 - 2011RPDBCAPECIC 1985 - 2009

#	Project Title	ICES Data
203	Trends in anticoagulants use among individuals with deep vein thrombosis	CIHI - DAD 2006 - 2011 CIHI - SDS 2006 - 2011 CIHI - NACRS 2006 - 2011 ODB 2006 - 2012 OHIP 2006 - 2011 RPDB
204	Ontario Asthma Surveillance Information System (OASIS): Health services use after ED discharge, a longitudinal study	CIHI - DAD April 1, 1988 - March 31, 2011 or the most current data available at ICES CIHI - NACRS April 1, 1988 - March 31, 2011 or the most current data available at ICES OHIP April 1, 1988 - March 31, 2011 or the most current data available at ICES RPDB Asthma
205	Ontario Asthma Surveillance Information System (OASIS): COPD risks in the asthma cohort	CIHI - DAD April 1, 1991 to March 31, 2011 or the most current data available at ICES CIHI - NACRS July 1, 2000 to March 31, 2011 or the most current data available at ICES OHIP July 1, 1991 to March 31, 2011 or the most current data available at ICES RPDB Asthma COPD
206	Utilization and costs of domperidone, human growth hormones and LABA	ODB 1990 - 2012 RPDB
207	Evaluating access to appropriate concussion care in Ontario	CIH - DAD 2008 - 2011 CIHI - NACRS 2008 - 2011 OHIP 2008 - 2011 RPDB OTR 2006 - 2011
208	Patterns of emergency department use over time in Ontario	CIHI - NACRS 2002 - 2012 RPDB
209	Short-and long-term health effects of temperature change: A population-based study in Ontario, Canada	CIHI - DAD 2000 - 2012 CIHI - SDS 2000 - 2012 CIHI - NACRS 2000 - 2012 OHIP 2000 - 2012 RPDB Asthma CHF COPD Hypertension ODD OMID Survey: CCHS CIC ORGD 1985 - 2012
210	EDS - HQO: Optimizing chronic disease management (OCDM)	CIHI - DAD 2003 - 2010 CIHI - SDS 2003 - 2010 CIHI - NACRS 2003 – 2010 CIHI - CCRS 2003 - 2010 CIHI - NRS 2003 – 2010 ODB 2003 - 2010 OHIP 2003 – 2010 HCD 2003 - 2010 LOC 2003 – 2010 OMHRS 2003 - 2010

#	Project Title	ICES Data
		RPDB CHF COP DODD
211	Careful review and evaluation of the access to timing and examination of the creation of vascular access (CREATE VA)	CIHI - DAD 1997 - 2011 CIHI - NACRS 2000 - 2011 OHIP 1997 - 2011 RPDB Hypertension ODD CORR 2001 - 2011
212	Integrated client care project - palliative care evaluation	CIHI - DAD 11-12 to 12-13 CIHI - NACRS 11-12 to 12-13 ODB 11-12 to 12-13 OHIP 11-12 to 12-13 HCD 11-12 to 12-13 RPDB InterRAI Database FY11 -12 to 12-13
213	Comparative effectiveness of cardiac drugs post-myocardial infarction	CIHI - DAD 2005 - 2011 CIHI - SDS 2005 - 2011 CIHI - NACRS 2005 - 2011 ODB 2005 - 2011 OHIP 2005 - 2011 RPDB Hypertension ODD
214	Validating self-report of cancer screening in Ontario	CIHI - DAD 1988 - 2007 OHIP 1991 - 2007 RPDB CAPE IPDB CPDB OCR 1991 - 2007 OBSP Cytobase CCHS
215	Examination of prescribing to children and adolescents with disabilities or on social assistance and assessment of adverse outcomes of these prescriptions. A population based study 1998 - 2011	CIHI - DAD 1998 - 2012 CIHI - SDS 1998 - 2012 CIHI - NACRS 1998 - 2012 ODB 1998 - 2012 OHIP 1998 - 2012 RPDB IPDB CPDB

#	Project Title	ICES Data
216	Resource utilization among young and midlife Ontarians following discharge from complex continuing care	CIHI - DAD 2001 – 2011 CIHI - SDS 2001 - 2011 CIHI - NACRS 2001 - 2011 CIHI - CCRS 2001 - 2011CIHI - NRS 2001 - 2011 ODB 2001 - 2011 OHIP 2001 - 2011 HCD 2001 – 2011 OMHRS 2001 - 2011 RPDB ORGD 2001 - 2011
217	Inflammatory bowel disease in immigrants to Canada and their children: Epidemiology and access to specialist care	CIHI - DAD 1991 - 2012 CIHI - SDS 1991 - 2012 CIHI - NACRS 1991 - 2012 CIHI - NRS 1991 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 RPDB IPDB MOMBaby PIBD Custom Clinical Dataset, Adult IBD Cohort to developed in (fall 2012) 1991 - 2012 CIC 1985 - 2012
218	Stroke outcome before and after July: The impact of the academic year-end changeover on stroke	CIHI - DAD 2003 - 2012 CIHI - NACRS 2003 - 2012 RPDB RCSN 2003 - 2008 SPIRIT Acute 2009 - 2012
219	The heart failure care-pathway project	CIHI - DAD 1 April 2004 - 31 March 2012 CIHI - SDS 1 April 2004 - 31 March 2012 OHIP 1 April 2004 - 31 March 2012 RPDB IPDB CPDB CHF EFFECT 2004 - 2005
220	Pilot study of the ability to probabilistically link clinical trial patients to ICES data	CIHI - DAD 1988 - 2012 CIHI - SDS 1991 - 2012 CIHI - NACRS 2003 - 2012 OHIP 1991 - 2012 RPDB NCIC CO - 17 & CO 20 OCR 1964 - 2012 OBSP
221	Effect of high potency statins on the risk of incident diabetes in patients with occlusive vascular disease	CIHI - DAD 1991 - 2011 CIHI - SDS 1991 - 2011 CIHI - NACRS 2002 - 2011 ODB 1991 - 2011 OHIP 1991 - 2011 RPDB

#	Project Title	ICES Data
222	Diabetes and its impact on the use of hormone therapy, chemotherapy, and radiation therapy in breast cancer	CIHI-DAD April , 2001 - March 31, 2011 CIHI-SDS April , 2001 - March 31, 2011 CIHI - NACRS April 1, 2002 - March 31, 2011 ODB April 1, 2005 - March 31, 2011 OHIP April 1, 2001 - March 31, 2011 RPDB CCO Staging data 2007 - 2010 NDFP 2006 – 2011 OCR 1964 -2011 ODD
223	Screening for chronic diseases among immigrants in Ontario: ScreenNet project #15	CIHI - DAD 1988 - 2011 OHIP 1991 - 2011 RPDB CAPE IPDB CPDB Registry ODD OMID OCR 1991 - 2011 OBSP Cytobase
224	Does the breast screening programme have better compliance for screening mammography than periodic mammography outside the programme? Screen Net study #14	CIHI - DAD 1988 - 2010 CIHI - SDS 1988 - 2010 CIHI - NACRS 1988 - 2010 OHIP 1988 - 2010 RPDB OBSP OCR 1964 - 2010
225	Humeral malunion osteotomy after operatively treated pediatric supracondylar fractures: A population based study	CIHI - DAD Jan 2002 - Jan 2010 OHIP Jan 2002 - Jan 2010
226	Survivorship in spinal instrumentation in spina bifida scoliosis: A population based study	CIHI - DAD Nov 2005 - April 2010 OHIP Nov 2005 - April 2010
227	Long acting opioids: Prescription quantities, duration of therapy, and dose distribution	ODB 2008 - 2012 OHIP 2008 - 2012 RPDB
228	The Toronto SPV valve study - A retrospective analysis	RPDB Vital Statistics 1991 - 2012
229	An examination of the quality of care for young adults who experience stroke	CIHI - DAD 2003 - 2012 CIHI - NACRS 2003 - 2012 CIHI - NRS 2003 - 2012. RPDB RCSN 2003 - 2011
230	Risk of kidney stones and gastrointestinal bleeding in living kidney donors	CIHI - DAD 1991 - 2012 CIHI - SDS 1991 - 2012 CIHI - NACRS 1991 - 2012 OHIP 1991 - 2012 RPDB TGLN Hypertension ODD

#	Project Title	ICES Data
231	Small molecular targeted agents and vascular outcomes in patients with advanced solid tumors: A population based study	CIHI - DAD January 1, 2000 - March 31, 2012 CIHI - NACRS January 1, 2000 - March 31, 2012 ODB January 1, 2000 - March 31, 2012 OHIP January 1, 2000 - March 31, 2012 RPDB Registry Stage data from CCO OCR 2000 - 2011 NDFP 2000 - 2012
232	Patient care networks data release	CIHI - DAD 2008 - 2010 CIHI - NACRS 2008 - 2010 OHIP 2008 - 2010 CAPE CPDB PhysNet 2008 - 2010
233	Psychiatric reporting to ease vehicular events near traffic (PREVENT) study	CIHI - DAD 2002 - 2011 CIHI - NACRS 2002 - 2011 OHIP 2002 - 2011 OMHRS 2002 - 2011
234	Validation of a minimum data set-based health related quality of life measure by mapping and regression	CIHI - CCRS 2008 - 2009 RPDB
235	Patient health outcomes and professional practice following the implementation of a colorectal community of practice model	CIHI - DAD 1990 - 2011 CIHI - NACRS 2002 - 2011 ODB 1992 - 2011 OHIP 1992 - 2010 RPDB OCR 1992 - 2011
236	Long-term survivorship of resected tarsal coalition: A population based study in Ontario	CIHI - DAD July 1994 - August 2011 OHIP July 1994 - August 2011
237	Large bowel evaluation in small northern communities	CIHI - DAD 1988 - 2011 CIHI - SDS 1988 - 2011 CIHI - NACRS 1988 - 2011 OHIP 1991 - 2012 RPDB OCR 1964 - 2010 Wawa Family Health Team Colonoscopy 2000 - 2012
238	Validation of an administrative data algorithm to identify traumatic spinal cord injured patients	CIHI - DAD 2002 - 2012 CIHI - NACRS 2002 - 2012 OHIP 2005 - 2012 RPDB Chart Abstraction 2002 - 2012
239	Making difficile more facile in Ontario: finding the active ingredients in successful clostridium difficile prevention efforts	CIHI - DAD 2002 - 2011 CIHI - SDS 2002 - 2011 CIHI - NACRS 2002 - 2011 CIHI - CCRS 2002 - 2011 OHIP 2002 - 2011 HCD 2002 - 2011 RPDB MOHLTC and PHO Survey of Hospital Infection Control Strategies

#	Project Title	ICES Data
240	Acute kidney injury and hyponatremia with phosphate and non-phosphate based bowel preparations	CIHI - DAD 1997 - 2011 CIHI - SDS 1997 - 2011 CIHI - NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB IPBD Gamma-Dynacare; Cerner 2002 - 2011
241	The burden of severe adverse drug reactions: Recurrence, outcomes and healthcare costs associated with drug-induced Stevens-Johnson syndrome and toxic epidermal necrolysis	CIHI - DAD 1997 - 2012 CIHI - SDS 1997 - 2012 CIHI - NACRS 2002 - 2012 ODB 2001 - 2012 OHIP 1997 - 2012 RPDB
242	Peripheral vertigo discharged from the emergency department: Examining outcomes in the province of Ontario	CIHI - DAD 1992 - 2012 CIHI - NACRS 2002 - 2011 ODB 1992 - 2012 OHIP 1992 - 2012 OMHRS 2002 - 2011 RPDB IPBD CHF COPD Hypertension ODD OMID
243	Socioeconomic status and access to stroke unit care in Ontario	CIHI - NACRS 2003 - 2012 RCSN 2003 - 2011
244	The relationship between diabetes mellitus and dementia: A population based study	CIHI - DAD April 1, 1992 - March 31, 2012 CIHI - SDS April 1, 1992 - March 31, 2012 CIHI - NACRS April 1, 1992 - March 31, 2012 ODB April 1, 1992 - March 31, 2012 OHIP April 1, 1992 - March 31, 2012 RPDB Hypertension ODD Census data, Ontario Hypertension Database
245	Impact of a chronic disease self-management program on healthcare utilization in eastern Ontario	CIHI - DAD 2007 - 2012 CIHI - NACRS 2007 - 2012 OHIP 2007 - 2012 RPDB IPDB Wawa Family Health Team Colonoscopy database 2000 - 2012
246	A population - based analysis of the natural history and management of diverticulitis	CIHI - DAD 2002 - 2011 CIHI - NACRS 2002 - 2011 OHIP 2002 - 2011 RPDB IPBD CPDB OPHRDC 2002 - 2011

#	Project Title	ICES Data
247	Risk of non-cardiac surgery and colonoscopy in patients with obstructive sleep apnea; A population based study	CIHI - DAD 1999 – 2010 CIHI - SDS 2003 - 2010 CIHI - NACRS 2003 – 2010 OHIP 1999 – 2010 RPDB IPDB Assistive Devices Program 2004 - 2010 CHF COPD Hypertension ODD OMID
248	Inter-RAI as a predictor of psychiatric hospitalization length of stay	CIHI - DAD April 1, 2009 - March 31, 2012 CIHI - SDS CIHI - NACRS April 1, 2009 - March 31, 2012 OHIP OMHRS RPDB IPDB
249	Colorectal cancer screening in persons with HIV in Ontario	CIHI - DAD 1 April 2002 to 31 March 31 2012 OHIP 1 April 2002 to 31 March 2012 RPBD OCR 1/4/2002 - 31/3/2007
250	Comparison of comorbidity indices for predicting mortality in a population-based cohort of persons with HIV	CIHI - DAD 1 April 2007 - 31 March 2010 ODB 1 April 2009 - 31 March 2010 OHIP 1 April 2007 - 31 March 2010 RPDB
251	Examination of preventative health services for persons with multimorbidity in Ontario: Do geography, primary care models, and complexity matter?	CIHI - DAD 1988 - 2011 ODB 1988 -2011 OHIP 1988 - 2011 RPDB CAPE IPBD CPDB OCR OBSP Cytobase Survey: CCHS
252	Effect of age on TPA door to needle times	Registry RCSN April 1, 2007 - March 31, 2011
253	Mental health service use in the greater Toronto area	CIHI - DAD 2009/10 to 2011/12 CIHI - NACRS 2009/10 to 2011/12 OMHRS RPDB 2009/10 to 2011/12
254	HSPRN multiple chronic disease cohort: Epidemiology sub-project	CIHI - DAD 1988 - 2011 CIHI - SDS 1988 – 2011 CIHI - NACRS 2003 - 2011 CIHI - CCRS 2005 – 2011 CIHI - NRS 2005 - 2011 ODB 1988 - 2011 OHIP 1988 – 2011 HCD 2005 - 2011 OMHRS 2006 - 2011 RPDB CAPE Asthma CHF

#	Project Title	ICES Data
		COPD Hypertension ODD OMID RAI - Home 2002 - 2011
255	The safety of bisphosphonates and "drug holidays"	CIHI-DAD 1988 - 2010 CIHI-SDS 1992 - 2010 CIHI-NACRS 2000 - 2010 ODB 1990 - 2010 OHIP 1993 - 2010 RPDB OCR 1964 - 2010
256	Unemployment and disability in Renfrew County	ODB 2001 - 2011 RPDB
257	Hospital use and health behaviours - the development of a predictive tool to estimate the contribution of smoking, unhealthy alcohol consumption, poor diet, physical inactivity and stress	CIHI - DAD 2000 - 2012 CIHI - SDS 2000 - 2012 CIHI - NACRS 2000 - 2012 RPDB CCHS
258	Prevalence rates and drug utilization patterns for myocardial infarction	CIHI - DAD 2001 - 2012 CIHI - SDS 2001 - 2012 ODB 2001 - 2012 OHIP 2001 - 2012
259	Subproject to TRIM# 2013 0904 305 000: Estimating the risks of adverse drug events using Bayesian evidence synthesis - Second stage	CIHI-DAD 1992 - 2012 CIHI-SDS 1992 - 2012 CIHI-NACRS 2002 - 2012 ODB 1996 - 2012 OHIP 1992 - 2012 RPDB Asthma CHF COPD Hypertension ODD OCR 1964 - 2012
260	Main project: Follow-up care after a visit to the emergency department: Assessing the frequency and timeliness in patients with chronic disease exacerbations	CIHI-DAD 1996 - 2012 CIHI - NACRS 2000 - 2012 ODB 1996 - 2012 OHIP 1996 - 2012 RPDB IPDB CHF COPD Hypertension ODD OMID

#	Project Title	ICES Data
261	What can or should we do about this patient's high blood pressure in the ED? A preventative health opportunity while validating the CIHI-NACRS code	CIHI-DAD 1996 - 2012 CIHI-NACRS 2000 - 2012 ODB 1996 - 2012 OHIP 1996 - 2012 RPDB IPDB CHF COPD Hypertension ODD OMID Chart abstraction (chart abstracted data from two hospitals: Sunnybrook and Markham Stouffville Hospital Apr 1/10 to Mar 31/11)
262	Impact of language on health care utilization, morbidity and mortality among diabetics in Ontario	CIHI-DAD 1999 - 2012 CIHI - SDS 1999 - 2012 CIHI - NACRS 2002 - 2012 OHIP 1992 - 2012 ODB 1999 - 2012 RPDB IPDB ODD up to 2005 LIDS - CIC 1985 - 2005 Hypertension up to 2005 CORR April 1, 2005 - February 29, 2012 TGLN April 1, 2005 - February 29, 2012
263	Continuation of temporary medications intended for acute illness: Enhancing medication safety	CIHI - DAD Apr 1, 1998 - Mar 31, 2012 CIHI - SDS Apr 1, 1998 - Mar 31, 2012 CIHI - NACRS Apr 1, 2002 - Mar 31, 2012 ODB Apr 1, 2002 - Mar 31, 2012 OHIP Apr 1, 1998 - Mar 31, 2012 OMHRS Apr 1, 2005 - Mar 31, 2012 RPDB IPDB Asthma CHF COPD Hypertension ODD OCR 1998 - 2012
264	The natural history of very-early onset inflammatory bowel disease (VEO-IBD): A population-based study	CIHI-DAD 1991 - 2011 CIHI-SDS 1991 - 2011 CIHI-NACRS 1991 - 2011 OHIP 1991 - 2011 RPDB IPDB PIBD
265	The rural/urban divide in inflammatory bowel disease: Assessing incidence, outcomes and access to care in Canada	CIHI-DAD 1991 - 2011 CIHI-NACRS 1991 - 2011 OHIP 1991 - 2011 RPDB IPDB PIBD (Ontario Crohn's and Colitis Cohort (Adult IBD Cohort) April 1, 1991 - March 31, 2011 CENSUS 1991 - 2006

#	Project Title	ICES Data
266	Diabetes in immigrants from South Asia and their children: Pilot data on incidence and prevalence	CIHI - DAD 1991 - 2012 CIHI - SDS 1991 - 2012 CIHI - NACRS 1991 - 2012 CIHI - NRS 1991 - 2012 OHIP 1991 - 2012 RPDB MOMBaby ODD CIC 1985 - 2012
267	Asthma in immigrants from South Asia and their children: Pilot data on incidence and prevalence	OHIP 1991 - 2012 RPDB Asthma MOMBaby CIC 1985 - 2012
268	Long-term care wait list analysis - comprehensive profile of demographics and health care needs of those wait-listed for long-term care	CIHI-DAD 2010 - 2011 CIHI-NACRS 2010 - 2011 CIHI-CCRS 2010 - 2011 HCD 2010 -2011 RPDB
269	MedsCheck and Pharmaceutical Opinion services in Ontario	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 CIHI-NACRS 1991 - 2012 CIHI-CCRS 1991 - 2012 CIHI-NRS 1991 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 HCD 1991 - 2012 LOC 1991 - 2012 RPDB IPDB Asthma CHF COPD Hypertension ODD
270	Osteoporosis drug exposure measurement and clinical impact	CIHI-DAD 1996 - 2012 CIHI-NACRS 1996 - 2012 CIHI-CCRS 1996 - 2012 ODB 1996 - 2012 OHIP 1996 - 2012 RPDB
271	Surgical training, experience and diversification of practice	CIHI - DAD 1988 - 2015 CIHI - SDS 1991 - 2015 CIHI - NACRS 2000 - 2015 ODB 1990 - 2015 OHIP 1991 - 2015 RPDB IPDB

#	Project Title	ICES Data
272	Population-based Incidence and costs of non-melanoma skin cancer using a claims-based algorithm	CIHI - DAD 1 Jan 1992 - 31 Dec 2012 CIHI - SDS 1 Jan 1992 - 31 Dec 2012 CIHI - NACRS 1 Jan 1992 - 31 Dec 2012 OHIP 1 Jan 1992 - 31 Dec 2012 RPDB IPDB ORGD 1 Jan 1992 - 31 Dec 2012 OCR 1 Jan 1992 - 31 Dec 2012
273	Long-term effect of a community cardiovascular health awareness program (C-CHAP): 5-year follow-up of community cluster randomized trial	CIHI - DAD 2005 - 2011 CIHI-NARS 2005 - 2011 ODB 2005 - 2011 OHIP 2005 - 2011 RPDB CAPE IPDB CPDB
274	Antibiotic utilization and adverse outcomes in an open cohort of Ontario long-term care residents	CIHI-DAD 2008 - 2011 CIHI-NACRS 2008 - 2011 CIHI-CCRS 2008 - 2011 CIHI-NRS 2009 - 2011 ODB 2008 - 2011 OHIP 2008 - 2011 OMHRS 2009 - 2011 RPDB IPDB
275	Adherence to prescription drug recommendations made on a provincial formulary for sitagliptin	CIHI-DAD 2005 - 2011 ODB 2007 - 2011 RPDB IPDB
276	Neonatal opioid withdrawal in Ontario	CIHI - DAD 1992 - 2011 CIHI - SDS 2000 - 2011 ODB 1991 - 2012 OHIP 1992 - 2011 RPDB MOMBaby
277	Defining palliative care physicians in administrative data	ODB 1991 - 2012 OHIP 1991 - 2012 RPDB CAPE IPDB CPDB OCR 1991 - 2012
278	Canada prime plus: Establishing a theoretical basis for interventions to change clinical practice	CIHI - DAD 2009 To 2014 CIHI - NACRS 2009 To 2014 OHIP 2009 To 2014 RPDB

#	Project Title	ICES Data
279	Economic evaluation of renal nerve denervation for treatment resistant hypertension in Ontario, Canada	CIHI - DAD 1988 - 2012 CIHI - SDS 1988- 2012 CIHI - NACRS 1988 - 2012 CIHI - CCRS 1988 - 2012 CIHI - NRS 1988 - 2012 ODB 1988 - 2012 OHIP 1988 - 2012 HCD 1988 - 2012 RPDB Hypertension PCCF 1996 - 2009 DALHIN 2009
280	Feasibility of an osteoporosis and fracture validation study using EMRALD	CIHI - DAD 1988 - 2013 CIHI - SDS 1991 - 2013 CIHI - NACRS 2000 - 2013 ODB 1990 - 2013 OHIP 1991 - 2013 IPDB EMRALD 1990 - 2013
281	An analysis of outcomes from increasing diagnostic investigations for ischemic stroke	CIHI - DAD 2003 - 2012 ODB 2003 - 2012 RPDB RCSN 2003 - 2012
282	Acetabular fractures: Post-operative morbidity and mortality & the long-term risk of total hip arthroplasty	CIHI-DAD 1991 - 2011 CIHI-SDS 1991 - 2011 OHIP 1991 - 2011 RPDB IPDB CPDB
283	The epidemiology of simple elbow dislocations in Ontario: Incidence, and short & long - term re-operation morbidity	CPDB OHIP 1991 - Present IPDB
284	Waiting times for cervix and head/neck radiation therapy in Ontario and associated cancer outcomes - An update	CIHI-DAD 1988 - 2013 OHIP 1992 - 2013 RPDB OCR 1964 - 2012
285	Quantifying future risk and burden of type 2 diabetes in Canada: Tools to inform the prevention of obesity and diabetes	CIHI-DAD 2002 - 2011 CIHI-SDS 2002 - 2011 CIHI-NACRS 2002 - 2011 CIHI-CCRS 2002 - 2011 ODB 2002 - 2011 OHIP 2002 - 2011 HCD 2005 - 2011 OMHRS 2005 - 2011 RPDB ODD OMID CCHS
286	Using a primary care electronic medical record administrative data linked database (EMRALD) to validate administrative data algorithms to identify patients with myasthenia gravis	CIHI - DAD 1988 - 2013 CIHI - SDS 1991 - 2013 CIHI - NACRS 2000 - 2013 ODB 1990 - 2013 OHIP 1991 - 2013 IPDB EMRALD 1990 - 2013

#	Project Title	ICES Data
287	Survival and access to liver transplantation for hepatocellular carcinoma in Ontario	Other: Linkage to 100 charts of patients with known HCC at the Ottawa Hospital-ONLY THEIR MRN WILL BE USED TO VALIDATE THE CODE FOR HCC 2008 - 2010 CIHI-DAD 1991 - 2010 CIHI-NACRS 1991 - 2010 OHIP 1991 - 2010 RPDB OCR 1991 2010 CORR 1991 - 2010 LIDS 1991 - 2010
288	Evaluating therapeutic decision-making, outcomes & resource utilization in chronic stable angina: An interprovincial population-based study	CIHI - DAD 2005 - 2013 CIHI - SDS 2005 - 2013 CIHI - NACRS 2005 - 2013 CIHI - CCRS 2005 - 2013 CIHI - NRS 2005 - 2013 ODB 2005 - 2013 OHIP 2005 - 2013 HCD 2005 - 2013 RPDB IPDB CCN 2008 - 2012 PCCF 2009 DALHIN 2009 Registry
289	The Ontario cancer study pilot linkage analysis	CIHI-DAD 1988 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 2003 - 2012 OHIP 1991 - 2012 RPDB OCR 1964 - 2012
290	Outcomes of polycystic kidney disease in reference to the general population	CIHI - DAD 1991 - 2011 CIHI - SDS 1991 - 2011 CIHI - NACRS 2000 - 2011 OHIP 1991 - 2011 RPDB
291	Feasibility of conducting large dialysis facility cluster randomization trials in Ontario	CIHI - DAD 1998 - 2011 CIHI - SDS 1998 - 2011 CIHI - NACRS 1998 - 2011 OHIP 1998 - 2011 RPDB ODD CORR 1993 - 2011
292	Acute kidney injury as a result of co-administration of calcium channel blockers and macrolide antibiotics	CIHI - DAD 1998 - 2011 CIHI - SDS 1998 - 2011 CIHI - NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB Cerner, Gamma-Dynacare 2002 - 2011
293	Risk of arrhythmia and mortality among dialysis patients prescribed quinine	CIHI-DAD 1997 - 2012 CIHI - NACRS 1997 - 2012 ODB 2001 - 2012 OHIP 1997 - 2012 RPDB

#	Project Title	ICES Data
294	Adverse outcomes as a result of co-administration of carbamazepine and macrolide antibiotics	CIHI-DAD 1998 - 2011 CIHI-SDS 1998 - 2011 CIHI-NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB IPDB
295	Event rate feasibility in retrospective cohort for PISCES RCT	CIHI-DAD 1995 - 2011 CIHI-SDS 1995 - 2011 ODB 2000 - 2011 OHIP 1995 - 2011 RPDB
296	Adverse outcomes as a result of co-administration of immunosupressants and macrolide antibiotics	CIHI - DAD 1998 - 2011 CIHI-SDS 1998 - 2011 CIHI-NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB IPDB
297	Bowel pro-kinetic drugs and drug dosing in chronic kidney disease patients	CIHI-DAD 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB
298	Optimizing the allocation of "high-risk" deceased donor kidneys: A Canadian perspective	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 CIHI-NACRS 2002 - 2012 OHIP 2002 - 2012 RPDB Hypertension ODD Trillium Gift of Life Network (TGLN) deceased donor data Canadian Organ Replacement Registry (CORR) database
299	Drug causes of acute interstitial nephritis	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB Cerner, Gamma-Dynacare
300	Nitrofurantoin in chronic kidney disease patients	CIHI-DAD 1998 - 2011 CIHI-SDS 1998 - 2011 CIHI-NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB IPDB Gamma Dynacare 2002 - 2011
301	Dipeptidyl peptidase-4 inhibitors, chronic kidney disease and the risk of pancreatitis	CIHI-DAD 2005 - 2013 CIHI-NACRS 2005 - 2013 ODB 2009 - 2013 OHIP 2005 - 2013 RPDB Gamma Dynacare

#	Project Title	ICES Data
302	Appropriate statin dosing in Asian populations	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB IPDB CIC 2001 - 2011
303	Rates and secular trends of major hemorrhage and stroke in incident chronic dialysis patients	CIHI-DAD Jan 1, 1992 - Dec 31, 2012 ODB Jan 1, 1995 - Dec 31, 2012 OHIP Jan 1, 1992 - Dec 31, 2012 RPDB CHF Hypertension ODD CORR Jan 1, 1996 - Dec 31, 2009
304	Risk of hyperkalemia with use of low molecular weight heparins	CIHI-DAD 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011
305	Risk of arrhythmia and mortality among dialysis patients prescribed macrolide antibiotics	CIHI-DAD 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB
306	Risk of arrhythmia and mortality among dialysis patients prescribed selective serotonin reuptake inhibitors	CIHI-DAD 1988 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1991 - 2011 RPDB Cerner Gamma Dynacare CORR IPDB OMHRS
307	Secular trends in cardiovascular disease among kidney transplant recipients	CIHI-DAD 1991 - 2011 CIHI-SDS 1991 - 2011 CIHI-NACRS 2000 - 2011 OHIP 1991 - 2011 RPDB CORR 1991 - 2011
308	adverse effect of tamsulosin and macrolide co-prescriptions	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB IPDB
309	The presence of chronic kidney disease and the effect on drug adherence	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 2000 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB

#	Project Title	ICES Data
310	Acute kidney injury as a result of co-administration of quetiapine and macrolide antibiotics	CIHI-DAD 1998 - 2011 CIHI-SDS 1998 - 2011 CIHI-NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB IPDB
311	Drug causes of thrombotic microangiopathy	CIHI-DAD 1988 - 2012 ODB 2001 - 2012 OHIP 1991 - 2012 RPDB
312	Impact of collaborative care on the health of people with COPD	CIHI - DAD 1991 - 2012 CIHI - SDS 1991 - 2012 CIHI - NACRS 2002 - 2012 ODB 2002 - 2012 OHIP 1991 - 2012 RPDB IPDB COPD
313	Evaluation of short-term neuropsychiatric and cardiovascular outcomes associated with varenicline	CIHI - DAD 2011 - 2012 CIHI - NACRS 2011 - 2012 ODB 2011 - 2012 OHIP 2011 - 2012 OMHRS 2011 - 2012 RPBD ASTHMA CHF OMID
314	Trends over time and regional variation in the use of laparoscopic hysterectomy for the treatment of endometrial cancer in the province of Ontario	CIHI-DAD January 2000 - March 2011 CIHI-SDS January 2000 - March 2011 OHIP January 2000 - March 2011 RPDB IPDB OCR January 2000 - March 2011
315	Holter monitoring in patients with stroke and TIA	OHIP 2003 - 2011 RCSN 2003 - 2011
316	Monitoring quality of diabetes care: A feasibility study linking office-based EMR with administrative databases	CIHI-DAD 2011 - 2012 CIHI-NACRS 2011 - 2012 OHIP 1991 - 2012 RPDB ODD
317	HIV drug prescribing in Ontario	ODB 2007 - 2012 RPDB Facilitated Access List for HIV Prescribers
318	Second line cholesterol lowering drugs and statin use	CIHI - DAD 1999 - 2012 ODB 1999 - 2012 OHIP 1999 - 2012 RPDB
319	Early evaluation of the new Ontario narcotics monitoring system	Ontario Narcotics Monitoring System Database
320	Potentially Inappropriate dispensing of selected monitored prescriptions in Ontario	ODB 1997 - 2013 RPDB
321	Receipt of pharmacist professional services by ODB beneficiaries	ODB 2011 - 2013 RPDB

#	Project Title	ICES Data
322	Diagnostic assessment units' impact on diagnostic delay in breast cancer: A population-based study in Ontario	OCR (2008 - latest) CCO Stage Capture Project (Jan 1st, 2011 - latest) OBSP database (2009 - 2012) CIHI-DAD 2007 - 2011 CIHI-SDS 2007 - 2011 CIHI - NACRS 2007 - 2011 OHIP 2007 - 2011 RPDB CAPE IPDB
323	Physician follow-up visits and repeat emergency department transfers among long-term care residents NOTE: This project is a sub-project of a larger entitled "Emergency department visits by nursing home residents in Ontario"	CIHI - DAD 2009 - 2010 CIHI - NACRS 2009 - 2010 CIHI - CCRS 2009 - 2010 ODB 2009 - 2010 OHIP 2009 - 2010 RPDB
324	The correlates, health outcomes and costs associated with multiple chronic conditions	CIHI-DAD 1 April 2006 - 31 March 2012 CIHI-NACRS 1 April 2006 - 31 March 2012 CIHI-NACRS 1 April 2006 - 31 March 2012 CIHI-CCRS 1 April 2006 - 31 March 2012 CIHI-NRS 1 April 2006 - 31 March 2012 ODB 1 April 2006 - 31 March 2012 OHIP 1 April 2006 - 31 March 2012 HCD 1 April 2006 - 31 March 2012 RPDB 1 April 2006 - 31 March 2012 CHF COPD Hypertension ODD CCHS
325	Secular trends in laryngeal carcinoma: Incidence, treatment, and survival	CIHI-DAD 1991 - 2010 OHIP 1991 - 2010 RPDB OCR January 1, 1991 - December 31, 2010
326	Impact of delisting Imaging (MRI, CT, X-ray) for uncomplicated low back pain on lumbar spine imaging utilization in Ontario, 2009 - 2012	OHIP 2009 - 2013 RPDB IPDB CPDB
327	Comparative analysis of chronic disease rates in Hiawatha First Nation (AHRQ Request)	CIHI - DAD 2006 - 2011 RPDB Asthma CHF COPD MOMBaby OMID OCR 2006 - 2011
328	Musculoskeletal disease in the Metis Nation of Ontario	CIHI-DAD 2006 - 2012 CIHI-SDS 2006 - 2012 CIHI-NACRS 2006 - 2012 ODB 2006 -2012 OHIP 2006 - 2012 RPDB

#	Project Title	ICES Data
329	Clinical outcomes of treatment by PCI vs CaBG in patients with CKD and multivessel or left main coronary artery disease in the province of Ontario	CIHI - DAD 2008 - 2011 OHIP 2008 - 2011 CCN 2008 - 2011
330	Inpatient rehabilitation following metastatic epidural spinal cord compression: A population-based study	CIHI - DAD 2007 - 2010 CIHI - NACRS 2007 - 2010 CIHI - NRS RPDB
331	Characteristics of persons admitted to inpatient rehabilitation settings: A descriptive study	CIHI - NACRS 2003 - 2013 RPDB DAD 2003-2012 NACRS 2003-2012 OHIP 2003-2012 HCD 2003-2012 CCRS 2003-2012 LOC 2003-2012 IPDB 2003-2012
332	Time is spine: Investigating time to surgery for patients with acute traumatic spinal cord injury in Ontario	CIHI-DAD Jan 2003 - Jan 2013 CIHI-NACRS Jan 2003 - Jan 2013 CIHI - NRS Jan 2003 - Jan 2013 OHIP Jan 2003 - Jan 2013 RPDB
333	Risk of pancreatitis associated with sitagliptin use among elderly patients with diabetes	CIHI - DAD 2003 - 2011 CIHI - NACRS 2003 - 2011 ODB 2006 - 2012 OHIP 2003 - 2012 RPDB
334	Factors associated with opioid-related mortality and hospitalization among patients prescribed methadone for opioid dependence treatment	CIHI - DAD 1992 - 2012 CIHI - NACRS 2002 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB IPDB Coroner's Data 1994 - 2010
335	Risk of statin-mediated myopathy with concomitant use of glyburide: A nested case - control study	CIHI - DAD 1992 - 2012 CIHI - NACRS 2002 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB IPDB
336	The impact of long-acting antipsychotics on psychiatric hospitalizations among individuals with schizophrenia	CIHI-DAD 1992 - 2012 CIHI-NACRS 2002 - 2012 ODB 1992-2012 OHIP 1992 - 2012 OMHRS RPDB
337	Evaluating low rates of oral anticoagulant prescribing for secondary stroke prevention in Ontario	CIHI - DAD July 2003 - 2012 CIHI - NACRS July 2003 - 2012 ODB July 2003 - 2012 RPDB RCSN July 2003 - 2012 Registry
338	Assessment of delays in presentation to stroke prevention clinics after TIA or minor stroke: Identifying opportunities for system change	Registry RCSN 2006 - 2011 Specific requests fo SPIRIT SPC and OSR SPV only 2006 - 2011

#	Project Title	ICES Data
339	Determining treatment effects in observational studies: Evaluating the influence of different analytical methods on estimates of treatment effect	RPDB RCSN 2003 - 2008 ORPD
340	Evaluating low rates of oral anticoagulant prescribing for secondary stroke prevention in Ontario	CIHI - DAD July 2003 - 2012 CIHI - NACRS July 2003 - 2012 ODB July 2003 - 2012 RPDB RCSN July 2003 - 2012 Registry
341	Trends in cerebrovascular events and dementia	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 CIHI-NACRS 2002 - 2012 ODB 2002 - 2012 OHIP 2002 - 2012
342	Optimal TIA management	CIHI - DAD 2008 - 2012 CIHI - NACRS 2008 - 2012 ODB 2008 - 2012 OHIP RPDB RCSN 2008 - 2011 Canada Census 2011
343	Access to and outcomes of kidney transplantation in Ontario: Is there a socioeconomic gradient?	CIHI - DAD 1991 - 2010 OHIP 1991 - 2010 RPDB TGLN CORR ODD
344	Impact of ethnicity on long-term major cardiac events after coronary artery bypass grafting surgery	CIHI-DAD 1990 - 2010 ODB 1990 - 2010 OHIP 1990 - 2010 RPDB CCN 1990 - 2010
345	Assess the treatment patterns and outcomes of hospitalized patients with aortic stenosis	CIHI-DAD 2004 - 2013 CIHI-NACRS 2004 - 2013 ODB 2004 - 2013 OHIP 2004 - 2013 ORGD 2004 - 2013
346	Ontario Stroke Network directed research priority #2 - investigating stroke unit care	CIHI- DAD 2001 - 2011 CIHI - SDS 2001 - 2011 CIHI - NACRS 2001 - 2011 CIHI-CCRS 2001 - 2011 CIHI-NRS 2001 - 2011 ODB 2001 - 2011 OHIP 2001 - 2011 HCD 2001 - 2011 RPDB Survey Registry OSA, OSR 2002 - 2010

#	Project Title	ICES Data
347	Direct cost of chronic ulcers	CIHI-DAD 2002 - 2012 CIHI-SDS 2008 - 2012 CIHI - NACRS 2008 - 2012 CIHI-NRS 2008 - 2012 ODB 2008 - 2012 OHIP 2008 - 2012 HCD 2008 - 2012 RPDB ODD OACCAC HC-RAI 2008 - 2012
348	A population-based study of patients with advanced pancreatic cancer receiving first-line single agent gemcitabine	CIHI-DAD 01-01-1998 to 31-12-2012 CIHI-NACRS 01-01-1998 to 31-12-2012 ODB 01-01-1998 to 31-12-2012 OHIP 01-01-1998 to 31-12-2012 RPDB CAPE IPDB OCR 01-01-1998 to 31-12-2012
349	Health service use and outcomes following the first-episode of psychosis	CIHI - DAD 1994 - 2011 CIHI - NACRS 2000 - 2011 OHIP 1994 - 2011 OHRS 2005 - 2011 RPDB
350	Ethnic disparities in healthcare use for infectious diseases	CIHI-DAD 1993 - 2012 CIHI-SDS 1993 - 2012 CIHI-NACRS 2002 - 2012 OHIP 1995 - 2012 Asthma CHF COPD Hypertension ODD OMID OCR 1993 - 2012 NPHS CCHS CIC 1985 - 2010
351	The influence of socioeconomic status on selection of anticoagulation for atrial fibrillation	CIHI-DAD 1992 - 2011 CIHI-SDS 1992 - 2011 CIHI - NACRS 2000 - 2011 ODB 2009 - 2012 OHIP 1992 - 2011 RPDB IPDB
352	The role of insulin and admission blood glucose in predicting mortality after acute heart failure	CIHI-DAD 2000 - 2012 ODB 2000 - 2012 OHIP 2000 - 2012 RPDB ODD

#	Project Title	ICES Data
353	Myocardial perfusion imaging and cardiovascular outcomes	CIHI - DAD 2000 - 2012 CIHI-SDS 2000 - 2012 CIHI- NACRS 2000 - 2012 OHIP 2000 - 2012 RPDB Nuclear Cardiology Database from R. J. Burns Centre of Excellence in Nuclear Cardiology ORGD 2003 - 2012
354	Heart failure quality improvement	CIHI-DAD 2008 - Present CIHI-NACRS 2008 - Present ODB 2008 - Present OHIP 2008 - present
355	Isotretinoin use amongst women of reproductive age and the risk of pregnancy and adverse pregnancy outcomes	CIHI - DAD 1991 - 2011 CIHI - SDS 1991 - 2011 CIHI - NACRS 2002 - 2011 ODB 1991 - 2011 OHIP 1991 - 2011 RPDB IPDB CPDB
356	The influence of diabetes on cancer screening and prognosis	CIHI - DAD April 1, 1996 to March 31, 2013 CIHI - SDS April 1, 1996 to March 31, 2013 CIHI - NACRS April 1, 2002 to March 31, 2013 ODB April 1, 2000 to March 31, 2013 OHIP April 1, 1996 - March 31, 2013 RPDB CAPE IPDB ODD OCR 1964 - 2012 OBSP Cytobase NDFP 1997 - 2012 CCO Stage Data 2005 - 2012 CIC 1985 - 2012
357	Cholinesterase inhibitors (ChEIs) and gastrointestinal (GI) bleeding in elderly patients with dementia: A population-based study	CIHI - DAD 1999 - 2012 CIHI - SDS 1999 - 2012 ODB 1999 - 2012 OHIP 1999 - 2012 RPDB ODD OCR 1999 - 2012 CONTACT 1999 - 2012
358	Evaluating the effectiveness of a home-based care program	CIHI-DAD 2005 - 2013 CIHI-NACRS 2005 - 2013 ODB 2005 - 2013 OHIP 2005 - 2013 HCD 2005 - 2013 RPDB OACCAC RAI-HC 2005 - 2013 Dataset containing OHIP numbers and enrollment dates of individuals enrolled in the program 2008 - 2013
359	Hospital use and health behaviours - the development of a predictive tool to estimate the contribution of smoking, unhealthy alcohol consumption, poor diet, physical inactivity and stress	CIHI - DAD 2000 - 2012 CIHI - SDS 2000 - 2012 CIHI - NACRS 2000 - 2012 RPDB CCHS

#	Project Title	ICES Data
360	Predicting and meeting the need for long-term care in the population	CIHI-DAD April 1995 - March 2012 CIHI-SDS 1995 - March 2012 CIHI-NACRS 1995 - March 2012 CIHI-CCRS April 1996 - March 2012 CIHI-NRS April 2000 - March 2012 ODB April 1995 - March 2012 OHIP April 1995 - March 2012 HCD April 2005 - March 2012 OMHRS Oct. 2005 - Mar. 2012 RPDB CAPE IPDB Asthma CHF Hypertension ODD OMID Facilities/Institution Databases 1988 - 2013
361	Defining the role of the primary care provider for people living with HIV	CIHI-DAD 1993 - 2012 CIHI-SDS 1993 - 2012 CIHI-NACRS 1993 - 2012 ODB 1993 - 2012 OHIP 1993 - 2012 OMHRS 2006 - 2012 RPDB IPDB CPDB Asthma CHF COPD Hypertension ODD OMID
362	Using linked federal and provincial administrative data to understand health and use of health services of immigrants in Ontario, Canada: Condition-specific data quality reporting	CIHI - DAD Apr 1995 - Mar 2012 CIHI - SDS Apr 1995 - Mar 2012 CIHI - NACRS Apr 1995 - Mar 2012 ODB Apr 1995 - Mar 2012 HCD Apr 2005 - Mar 2012 OHIP Apr 1995 - Mar 2012 OMHRS Oct 2005 - Mar 2012 RPDB Asthma CHF COPD Hypertension MOMBaby ODD OMID
363	A feasibility study examining referral to community-based youth violence interventions for youth injured by violence	CIHI - NACRS 2009 - 2011 OTR 2009 - 2011

#	Project Title	ICES Data
364	Screen Net project 17: Disease outcomes and attributable costs of lung cancer in Ontario	CIHI - DAD 1988 - 2012 CIHI - SDS 1988 - 2012 CIHI - NACRS 1988 - 2012 CIHI - CCRS 1988 - 2012 CIHI - NRS 1988 - 2012 ODB 1988 - 2012 OHIP 1988 - 2012 HCD 1988 - 2012 RPDB OCR 1964 - 2012 MIS 2006 - 2012 ORGD 1990 - 2011
365	Waiting times for breast radiation therapy in Ontario and associated cancer outcomes - An update	CIHI-DAD 1988 - 2013 OHIP 1992 - 2013 RPDB OCR 1964 - 2012 Pathology reports from OCR via CCO data sharing agreement to be obtained Custom Clinical dataset / OCR Pathology 2007 - 2012
366	Risk of subsequent HRHPV related health events in a cohort treated by LEEP excision	CIHI-DAD 1988 - 2012 CIHI-SDS 1988 - 2012 CIHI-NACRS 1988 - 2012 CIHI-CCRS 1988 - 2012 CIHI-NRS 1988 - 2012 OHIP 1992 - 2012 ODD OMID OCR 1964 - 2012
367	Inequalities in the burden of HPV-related diseases in Ontario	CIHI-DAD 1988 - 2012 CIHI-SDS 1988 - 2012 CIHI-NACRS 1988 - 2012 OHIP 1992 - 2012 RPDB OCR 1964 - 2011 Cytobase up to 2012 CIC
368	Effects of expanding nurse practitioner (NP) testing authority: A time-series analysis	OHIP 2004 - 2012 RPDB CPDB
369	Age adjusted diabetes and hypertension prevalence rates in Brampton, Ontario for 2011	RPDB Hypertension ODD
370	Comparative effectiveness research: Biologic therapies in rheumatoid arthritis	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 1991 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 RPDB CAPE IPDB Asthma CHF COPD Hypertension ODD

#	Project Title	ICES Data
371	Descriptive epidemiology and health services impact of inborn errors of metabolism in an Ontario newborn cohort	CIHI - DAD 2006 - 2011 CIHI - NACRS 2006 - 2011 OHIP 2006 - 2011 HCD 2006 - 2011 RPDB IPDB CPDB Newborn Screening Ontario 2006 - 2011
372	Critical adverse events following codeine prescription among various ethnic groups	CIHI - DAD 1992 - 2012 CIHI - NACRS 2002 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB MOMBaby CIC ORDG
373	Gender disparities in perinatal & child health & maternal wellbeing associated with maternal country of birth	CIHI-DAD 1992 - 2011 CIHI-SDS 1992 - 2011 CIHI-NACRS 1992 - 2011 OHIP 1992 - 2011 MOMBaby ORGD/CIC 1985 - 2011
374	Maternal ethnicity and risk of cerebral palsy in her child	CIHI-DAD 2001 - 2012 OHIP 2001 - 2012 MOMBaby CIC Dataset 1986 - 2012
375	Bereavement and organ donation yesterday (BODY)	CIHI - DAD 2001 - 2013 CIHI - NACRS 2001 - 2013 OHIP 2001 - 2013 OMHRS 2001 - 2013 MOMBaby
376	The health care burden associated with measles in Ontario	CIHI - DAD 2005 - 2011 CIHI - SDS 2005 - 2011 CIHI - NACRS 2005 - 2011 OHIP 2005 - 2011 Public Health Ontario Laboratories Measles Test Data
377	High-users of Ontario's health care system: A comprehensive look at the characteristics and upstream determines of high cost users	CIHI - DAD 1995 - 2012 CIHI - SDS 2003 - 2012 CIHI - NACRS 2000 - 2012 CIHI - CCRS 1996 - 2012 CIHI-NRS 2000-2012 ODB 1995 - 2012 OHIP 1995 - 2012 HCD 1995 - 2012 LOC 1997 - 2006 OMHRS 2005 - 2012 RPDB CAPE NPHS CCHS
378	Impact of rotavirus immunization on acute gastroenteritis in Ontario	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 CIHI-NACS 2002 - 2012 OHIP 2002 - 2012

#	Project Title	ICES Data
379	Stroke and congestive heart failure, clinical features, risk factors and outcome	RPDB RCSN 2003 - 2008
380	Diabetic retinopathy in the immigrant population of Ontario	CIHI - DAD 1995 - 2012 CIHI - SDS 1995 - 2012 OHIP 1995 - 2012 RPDB IPDB CIC
381	Validation of an administrative data-derived case definition of gestational diabetes mellitus (GDM)	CIHI - DAD January 1, 2002 - March 31, 2012 OHIP January 1, 2002 - March 31, 2012 RPDB ODD Other: Laboratory Data (Mount Sinai Hospital)
382	Provincially-funded insulin pump therapy and health care utilization in adults with type 1 diabetes in Ontario	CIHI-DAD 2006 - 2012 CIHI-NACRS 2006 - 2012 OHIP 2006 - 2012 RPDB ADP Insulin Pump Data Vital Stats
383	Healthcare system sustainability through longitudinal efficiency: Improved quality and lower costs Subproject: Quality indicators	CIHI-DAD 1993 - 2012 CIHI-SDS 1993 - 2012 CIHI-NACRS 1993 - 2012 CIHI-CCRS 1997 - 2012 ODB 1993 - 2012 OHIP 1993 - 2012 HCD (formerly CCHCD) 1993 - 2012 OMHRS 1993 - 2012 RPDB IPDB CPDB ODD OMID OCR 1993 - 2012 RCSN 2010 - 2011 EFFECT 1993 - 2012 OBSP Cytobase NPHS CCHS PCASMIS 1993 - 2012
384	Endoscopic ultrasound in Ontario: Health care utilization and outcomes from 2003 - 2011	CIHI - DAD 2003 - 2011 CIHI-SDS 2003 - 2011 CIHI-NACRS 2003 - 2011 OHIP 2003 - 2011 RPDB IPDB CPDB OCR 2003 - 2011
385	Malignancy risk in childhood recipients of solid organ transplants	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 OHIP 1991 - 2012 RPDB OCR 01-01-1985 to 01-07-2012 Custom Clinical dataset Paediatric Toronto Transplant Cohort from Hospital for Sick Children 1985 - 2011

#	Project Title	ICES Data
386	Optimizing audit and feedback for primary care - testing scalable approaches to providing feedback reports	EMRALD
387	Utilization of cardiac computed tomography (CT) in Ontario, 2011 and 2012	CIHI - DAD 2006 - 2011 OHIP 2010 - 2012 RPDB IPDB
388	CVCD alliance cohort study	CIHI-DAD 2000 - 2017 CIHI-SDS 2000 - 2017 CIHI-NACRS 2000 - 2017 ODB 2000 - 2017 OHIP 2000 - 2017 RPDB Asthma CHF COPD Hypertension OHS/CV Component Prospective provincial cohorts: Ontario Health Study, BC Generations, Alberta Tomorrow, QC Cartagene, Atlantic Canada's PATH; 2 other cohorts: Prospective Urban Rural Epidemiology (PURE), Montreal Heart Institute Biobank Vital Stats/Ontaio Registrar General Death 2000-2017
389	Optimizing the coordination of care between rheumatologists and primary care physicians for patients with inflammatory arthritis	CIHI-DAD 1998 - 2014 CIHI-SDS 1991 - 2014 CIHI-NACRS 2003 - 2014 ODB 1990 - 2014 OHIP 1991 - 2014 RPDB CAPE IPDB EMRALD 1988 - 2014
390	Do EMRs in primary care improve care? (EPIC) - Resubmitted	CIHI-DAD 1988 - 2013 CIHI-SDS 1991 - 2013 CIHI-NACRS 2000 - 2013 ODB 1990 - 2013 OHIP 1991 RPDB CAPE IPDB
391	Rates and waits for cancer surgery in Canada: A mixed methods assessment	CIHI-DAD fiscal 2002 - fiscal 2010 CIHI-SDS fiscal 2002 - fiscal 2010 CIHI-NACRS fiscal 2002 - fiscal 2010 OHIP fiscal 2002 - fiscal 2010 RPBD OCR December 1, 2001 - December 31, 2010
392	Health services utilization after out-of-country bariatric surgery	CIHI-DAD Fiscal 2005 - Fiscal 2012 CIHI-SDS Fiscal 2005 - Fiscal 2012 CIHI-NACRS Fiscal 2005 - Fiscal 2012 OHIP Fiscal 2005 - Fiscal 2012 HCD Fiscal 2005 - Fiscal 2012 OHIP/MOH OOC Bariatric Database

#	Project Title	ICES Data
393	Impact of teaching on duration of surgery	CIHI-DAD 1997 - 2012 CIHI-SDS 1997 - 2012 OHIP 1997 - 2012 RPDB IPDB
394	Maternal & infant health among refugees in Ontario - A population based perspective	CIHI-DAD 1988 - 2013 OHIP 1988 - 2013 RPDB MOMBaby Citizenship & Immigration Canada Database 1985 - 2010 ORGD 1990 - 2011
395	Using administrative data to measure surgical quality of rectal cancer at the Ottawa Hospital from 1996 - 2010	CIHI-DAD 2002 - 2010 OCR 2002 - 2010
396	Use of the ketogenic as a treatment for children with epilepsy and its impact on health service utilization in Ontario	CIHI-DAD 1991-2010 CIHI-NACRS 2002-2010 OHIP 1991-2010 OMHRS 1991-2010 RPDB
397	Trends in survival after hospitalization in Ontario 1994 - 2009	CIHI - DAD 1994 - 2009 RPDB
398	HSPRN multiple chronic disease cohort: Epidemiology sub-project	CIHI - DAD 1988 - 2011 CIHI - SDS 1988 - 2011 CIHI - NACRS 2003 - 2011 CIHI - CCRS 2005 - 2011 CIHI - NRS 2005 - 2011 ODB 1988 - 2011 OHIP 1988 - 2011 HCD 2005 - 2011 OMHRS 2006 - 2011 RPDB CAPE Asthma CHF COPD Hypertension ODD OMID RAI - Home 2002 - 2011
399	Assessment of health care patterns for elderly lung cancer patients in Ontario	CIHI - DAD 1999 - 2011 CIHI - NACRS 2003 - 2011 CIHI - SDS 1999 - 2011 ODB 1999 - 2011 OHIP 1999 - 2011 OHCAS/HCD 1999 - 2011 OCR 1999 - 2011 NDFP 1999 - 2011
400	A novel high-risk TIA/minor stroke rapid assessment unit to improve quality of care and patient outcomes	Registry CIHI - DAD 2011 - 2012 CIHI - NACRS 2011 - 2012 RPDB RCSN Sept 6, 2011 - Aug 31, 2012
401	Urologic outcomes among spinal cord injured patients in Ontario	CIHI - DAD 2002 - 2012 CIHI-NRS 2002 - 2012 OHIP 2002 - 2012 RPDB

#	Project Title	ICES Data
402	Oral hypoglycemic agents and risk of hospital encounters with hypoglycemia	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB Cerner, Gamma Dynacare 2002 - 2011
403	Factors associated with death or admission to hospital within 7 days of discharge from crowded emergency departments	CIHI-DAD 2007 - 2011 CIHI-NACRS 2007 - 2011 OHIP 2007 - 2011 RPDB ORGD Apr 2007 - Mar 2012
404	AHRQ 2012 - 037: Quality of care indicators for patients with spinal cord injury (SCI)	CIHI-DAD 2006 - 2010 CIHI-SDS 2006 - 2010 CIHI-NACRS 2006 - 2010 CIHI-CCRS CIHI-NRS 2006 - 2010 ODB OHIP 2009 - 2011 HCD 2006 - 2010 OMHRS RPDB CAPE IPDB CPDB OTR 2006 - 2009 HOBIC
405	Serum hemoglobin concentration and serum platelet count as a potential predictors of outcomes after acute stroke	CIHI-DAD 2003 - 2011 RCSN 2005 - 2011
406	Do not resuscitate orders, quality of care, and outcomes in patients hospitalized for heart failure- a secondary analysis of the effect registry	CIHI-DAD 1999 - 2005 CIHI-NACRS 1999 - 2005 EFFECT 1999 - 2001 to 2004 - 2005
407	Cardiac events, stroke recurrence, and the effect of diabetes on subsequent vascular events in South Asian stroke patients	CIHI-DAD 2002 - 2012 CIHI-NACRS 2002 - 2012 ODB 2002 - 2012 OHIP 2002 - 2012 RPDB ODD RCSN 2002 - 2012 RPDB 2002 - 2012
408	Trends in opioid prescribing, deaths, and years of life lost in Ontario	CIHI-DAD 1993 - 2010 CIHI-NACRS 1993 - 2010 ODB 1993 - 2010 OHIP 1993 - 2010 RPDB
409	Population-based sequelae of inappropriately dosing cephalosporin antibiotics in CKD patients	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 2000 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB IPDB

#	Project Title	ICES Data
410	Trends and patterns of care for complex pediatric, adult and older adult populations	CIHI-DAD 2010 - 2012 CIHI-SDS 2010 - 2012 CIHI-NACRS 2010 - 2010 CIHI-CCRS 2010 - 2012 CIHI-NRS 2010 - 2012 ODB 2010 - 2012 OHIP 2010 - 2012 HCD 2010 - 2012 OMHRS 2010 - 2012 RPDB CAPE IPDB Asthma CHF COPD Hypertension ODD OMID RAI-HOME Care 2010 - 2012 CHF
411	The Champlain collaborative	CIHI-DAD April 1 2010 - March 31 2012 CIHI-NACRS April 1 2010 - March 31 2012 OHIP April 1 2010 - March 31 2012 RPDB IPDB CPDB
412	Is there and obesity paradox in outcomes following cardiac surgery in Canada?	CIHI-DAD 1991 - 2013 CIHI-SDS 1991 - 2013 CIHI-NACRS 2000 - 2013 ODB OHIP 1991 - 2013 RPDB CCN 1991 -2011
413	Mental health and addictions scorecard and evaluation framework - children and youth (TRIM: 2012 0900 300 000)	CIHI-DAD 2002 - 2011 CIHI-NACRS 2002 - 2011 ODB 2002 - 2011 OHIP 2002 - 2011 OMHRS 2005 - 2011 RPDB IPDB MOMBaby CCHS CIC 2002 - 2010 ORGD 2002 - 2011
414	A population-based study of cancer incidence and mortality in patients with solid organ transplants: Specific aim 2	CIHI-DAD 1997 - 2013 CIHI-NACRS 1997 - 2013 OHIP 1997 - 2013 RPDB OCR 1997 - 2013
415	The risk of fractures following stroke	CIHI-DAD 2002 - 2012 CIHI-NACRS 2002 - 2012 ODB 2002 - 2012 OHIP 2002 - 2012 RCSN 2002 - 2012
416	Canada crazy for our children and youth mental health	CIHI-DAD 1996 - 2009 CIHI-NACRS 2002 - 2009 OHIP 1996 - 2009 OMHRS 2006 - 2009

#	Project Title	ICES Data
417	Serotonin-norepinephrine reuptake inhibitors and acute kidney injury	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 2002 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 RPDB
418	Bupropion vs. SSRI antidepressants: The risk of seizures	CIHI-DAD 1992 - 2012 CIHI-NACRS 2002 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 OMHRS 2005 - 2012 RPDB IPDB
419	Banting and Best Diabetes Centre (BBDC) population-based diabetes registry project: Feasibility phase - Validation exercise using EMRALD data	CIHI-DAD 1991 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 ODD EMRALD Database
420	Lithium, parkinsonism and the use of dopaminergic drugs in older adults: Another prescribing cascade?	CIHI-DAD 1 April 1997 - 31 March 2012 CIHI-SDS 1 April 1997 - 31 March 2012 CIHI-NACRS 1 April 1997 - 31 March 2012 ODB 1 April 2000 - 31 March 2012 OHIP 1 April 1997 - 31 March 2012 OMHRS 1 April 2005 - 31 March 2011 RPDB IPDB
421	Risk of acute-onset psychosis in patients prescribed psychostimulants for the treatment of attention deficit hyperactivity disorder (ADHD)	CIHI-DAD 1992 - 2012 CIHI-NACRS 1992 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 OMHRS RPDB
422	Neighbourhood food environment in relation to fruit & vegetable intake, body weight and diabetes	OHIP 2000 - 2011 RPDB ODD Dunn & Bradstreet food dataset, January 2008
423	Characteristics and outcomes of the early prescribers of direct renin inhibitors in Ontario	CIHI-DAD 2004 - 2012/2013 CIHI-SDS 2004 - 2012/2013 CIHI-NACRS 2004 - 2012/2013 ODB 2007 - 2012/2013 OHIP 2007-2012/2013 RPDB IPDB Hypertension
424	Average emergency department (ED) wait times for mental health presentations across Ontario and by LHIN of service provider	CIHI-NACRS 2007 - 2009 OHIP 2007 - 2009
425	Validation of ICD 10 hypoglycemia codes	CIHI-DAD 1998 - 2011 CIHI-NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB Cerner, Gamma-Dynacare 2002 - 2011

#	Project Title	ICES Data
426	Standardized mortality ratio for dialysis facilities in Ontario	CIHI-DAD 1991-2012 CIHI-SDS 1991-2012 CIHI-NACRS 2002-2012 OHIP 1991-2012 RPDB IPDB CPDB CHF COPD Hypertension ODD ORRS 2010-2012
427	A virtual ward to reduce readmission after hospital discharge	CIHI-DAD 2008-2012 CIHI-NACRS 2008-2012 CIHI-CCRS 2008-2012 CIHI-NRS 2008-2012 ODB 2008-2012 OHIP 2008-2012 HCD 2008-2012 RPDB IPDB
428	The Ontario Stroke Registry's 2012/13 Ontario stroke audit of acute care facilities (OSA-Acute)	CIHI-DAD 1 April 2012-31 March 2013 CIHI-NACRS 1 April 2012-31 March 2013 RPDB
429	Primary care management of cancer screening in Ontario	CIHI-DAD April 1985-March 2013 OHIP April 2002-March 2013 RPDB CAPE IPDB CPDB OCR 1964-March 2013 OBSP
430	The nature, treatment and outcomes of stroke in chronic dialysis and renal transplant in Ontario	CIHI-DAD 1998 - 2011 CIHI-NACRS 1998 - 2011 ODB 2002 - 2011 OHIP 1998 - 2011 RPDB RCSN 2003 - 2011 CORR & Gamma Dynacare 1998 - 2011
431	Rates and secular trends of major hemorrhage and stroke in incident renal transplant patients	CIHI-DAD Jan 1, 1993 - Dec 31, 2011 ODB Jan 1, 1997 - Dec 31, 2008 OHIP Jan 1, 1993 - Dec 31, 2011 RPDB CORR Jan 1, 1997 - Dec 31, 2008
432	Health care access research in developmental disabilities (H-CARDD) program	Developmental Disabilities Cohort from MCSS CIHI-DAD 2005 - 2012 CIHI-SDS 2005 - 2012 CIHI-NACRS 2005-2012 ODB 2005 - 2012 OHIP 2005 - 2012 OMHRS 2005 - 2012 RPDB MOMBaby OCR 2000 - 2012

#	Project Title	ICES Data
433	Modeling a costing profile for incident emergency department atrial fibrillation	CIHI-DAD 2002 - 2013 CIHI-SDS CIHI-NACRS 2002 - 2013 CIHI-CCRS 2002 - 2013 CIHI-NRS 2002 - 2013 ODB 2002 - 2013 OHIP 2002 - 2013 HCD RPDB Hypertension ODD
434	Prostate cancer diagnosis as a metabolic risk factor for cardiovascular disease	CIHI-DAD April 1, 1991 - March 31, 2013 CIHI-SDS April 1, 1991 - March 31, 2013 CIHI-NACRS July 1, 2000 - March 31, 2013 ODB April 1, 1991 - March 31, 2013 OHIP April 1, 1991 - March 31, 2013 RPDB Hypertension ODD OCR April 1, 1964 - Dec 31, 2012
435	Blood glucose test strips: Utilization and economic implications of restrictions in use in Ontario	ODB 2003 - 2012 ODD
436	Cause of hospitalization of patients following discharge from crowded emergency department	CIHI-DAD 2007 - 2011CIHI-SDS 2007 - 2011OHIP 2007 - 2011RPDB
437	Characterizing polycystic kidney disease using ICES databases	CIHI-DAD 1988 - 2011 CIHI-SDS 1991 - 2011 CIHI-NACRS 2000 - 2011 ODB 1990 - 2011 OHIP 1991 - 2011 RPDB
438	Comparative effectiveness of ACE inhibitors and ARBs in rates of AKI	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 IPDB
439	Secular trends in the management and outcomes of acute kidney injury in Ontario	Cerner & Gamma-Dynacare 2003 - 2012 CIHI-DAD 1991 - 2012 CIHI-NACRS 1991 - 2012 OHIP 1991 - 2012 RPDB

#	Project Title	ICES Data
440	Comparing the risk of hospitalization in incident chronic dialysis patients who receive assisted peritoneal dialysis compared to facility-based hemodialysis	CIHI-DAD 2004 - 2012 CIHI-SDS 2004 - 2012 CIHI-NACRS 2004 - 2012 ODB 2004 - 2012 OHIP 2004 - 2012 HCD 2004 - 2012 RPDB LOC RPDB IPDB CPDB CPDB CHF COPD Hypertension ODD DMAR 2004 - 2013 Canadian Organ Replacement Registry & Ontario Renal Reporting System 2004 - 2012&2013
441	Association between local food environment and incidence of chronic diseases among immigrants to Ontario	CIHI-DAD 1996 - 2011 CIHI-SDS 1996 - 2011 CIHI-NACRS 2002 - 2011 OHIP 1996 - 2011 RPDB CHF Hypertension ODD OMID CIC 1996 - 2006
442	International physicians and access to specialist care	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 – 2012 CIHI-NACRS 2002 - 2012ODB 2002 - 2012 OHIP 2002 - 2012 RPDB CAPE IPDB ODD OMID
443	Assessing the utility of the DOC screen (depression, obstructive sleep apnea and cognitive impairment) to identify patients at high risk of adverse outcomes	CIHI-DAD 1 Apr 2003 - 31 Mar 2011 CIHI-NACRS 1 Apr 2003 - 31 Mar 2011 RPDB RCSN
444	The impact of Southwestern Ontario's community stroke rehabilitation teams: an economic analysis	CIHI-DAD January 2012 - March 2013 CIHI- NACRS January 2012 - March 2013 OHIP January 2012 - March 2013 RCSN January 2012 - March 2013 OSA January 2010 - March 2011
445	OATP1B1 metabolized statins and macrolide interactions	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB IPDB CERNER, GAMMA-DYNACARE 2002 - 2011

#	Project Title	ICES Data
446	Readmission and emergency room visits after hospitalization among dialysis patients	CIHI-DAD 1 April 1997 - 31 March 2012 CIHI-SDS 1997 - 31 March 2012 CIHI-NACRS 1997 - 31 March 2012 CIHI-CCRS 1997 - 31 March 2012 CIHI-NRS 1997 - 31 March 2012 ODB 1997 - 31 March 2012 OHIP 1997 - 31 March 2012 OMHRS 1997 - 31 March 2012 RPDB
447	Identifying physician demographic characteristics associated with screening for immigrants	CIHI-DAD 1988 - 2012 OHIP 1988 - 2012 RPDB CAPE IPDB CPDB OCR 1988 - 2012 OBSP Cytobase
448	Fragility fractures as a result of co-administration of calcium channel blockers and macrolide antibiotics	CIHI-DAD 2003 -2011 CIHI-NACRS 2003 - 2012 ODB 2003 - 2012 OHIP 2003 - 2012 RPDB
449	Physician-patient language concordance and diabetes and coronary artery disease related outcomes	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 CIHI-NACRS 2002 - 2012 ODB 2002 - 2012 OHIP 2002 - 2012 RPDB CAPE IPDB Hypertension ODD OMID CIC 2002 - 2010
450	Opioid agonist treatment (OAT) in rural versus urban settings	CIHI-DAD 1997 - 2012 CIHI-NACRS 2002 - 2012 ODB 2002 - 2013 OHIP 2002 - 2013 RPDB IPDB
451	Advancing comparative effectiveness research: Filling in the gaps for bisphosphonates	CIHI-DAD 1996 - 2012 CIHI-NACRS 1996 - 2012 CIHI-CCRS 1996 - 2012 ODB 1996 - 2012 OHIP 1996 - 2012 RPDB
452	Benefit of colorectal cancer mortality reduction due to screening at the upper age range of current guidelines	CIHI-DAD 1988- 2013 CIHI-SDS 1988 - 2013 CIHI-NACRS 1988 - 2013 CIHI-CCRS 1988 - 2013 CIHI-NRS 1988 - 2013 OHIP 1991 - 2013 RPDB OCR 1964 - 2013

#	Project Title	ICES Data
453	Examining the use and impact of androgen deprivation therapy in men with prostate cancer	CIHI-DAD 01/01/92 - END CIHI-SDS 01/01/92 - END CIHI-NACRS START - END ODB 01/01/92 - END OHIP 01/01/92 - END RPDB ODD OMID OCR 01/01/64 - END
454	Leading from the front: Support for organ and tissue donor registration among physicians	RPDB IPDB
455	Hospitalization outcomes among users of atypical antipsychotics with schizophrenia	CIHI-DAD 2006-2012 CIHI-NACRS 2006 - 2012 ODB 2006 - 2012 OHIP 2006 - 2012 OMHRS 2006 - 2012 RPDB
456	Impact of socioeconomic status on adherence to therapy, INR monitoring, and risk of hemorrhage and acute thromboembolic outcomes among those newly treated with warfarin	CIHI-DAD 1992 - 2012 CIHI-NACRS 1992 – 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB Hypertension ODD OMID
457	Health service use among francophone versus anglophone Ontarians	CIHI-DAD 2009 - 2012 CIHI-SDS 2009 - 2012 CIHI-NACRS 2009 - 2012 RPDB CCHS
458	Mental health care utilization among people who die by suicide: Moving towards a more focused understanding	CIHI-DAD 1997 - 2010 CIHI-NACRS 2002 - 2010 OHIP 1997 - 2010 OMHRS 2005 - 2010 RPDB MOMBaby
459	Variations in ambulatory care and outcomes for rural patients with coronary artery disease	CIHI-DAD April 1, 2008 - December 31, 2013 CIHI-NACRS April 1, 2008 - December 31, 2012 ODB April 1, 2008 - December 31, 2012 OHIP April 1, 2008 - December 31, 2012 RPDB CCN April 1, 2008 - December 31, 2012
460	Trends in anticonvulsant use and dosing during pregnancy	CIHI-DAD 1992 - 2012 CIHI-NACRS 2002 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 OMHRS 2005 - 2012 RPDB IPDB MOMBaby

#	Project Title	ICES Data
461	Effects of rehabilitation on postoperative outcomes of older adults with hip fractures and dementia	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 2002 - 2011 CIHI-CCRS 2002 - 2011 CIHI-NRS 2002 - 2011 ODB 1997 - 2011 OHIP 1997 - 2011 HCD 2002 - 2011 OMHRS RPDB IPDB CHF COPD Hypertension
462	The epidemiology of mechanical ventilation and changes in response to the evolution of clinical knowledge in critically ill patients in Ontario	CIHI-DAD 2000 - 2012CIHI-NACRS 2000 - 2012OHIP 2000 - 2012
463	Evaluation of health care utilization and outcomes for new oral anticoagulant-related hemorrhage in the elderly: A population-based study	CIHI-DAD 2000 - 2015 CIHI-NACRS 2000 - 2015 ODB 2000 - 2015 OHIP 2000 - 2015 RPDB Custom Clinical dataset: NOAC Chart Review Datasets (1, 2, and 3) 2010 - 2015 OCCI 2010 - 2015
464	New cancer drugs in Ontario: Patterns of care, lifetime costs, and incremental cost-effectiveness	CIHI-DAD 1996 - 2004 CIHI-NACRS 1996 - 2004 CIHI-SDS 1996 - 2004 ODB 1996 - 2004 OHIP 1996 - 2004 OHCAS/HCD 1996 - 2004 OCR 1996 - 2004 NDFP 1996 - 2004
465	Low molecular weight heparins and anticoagulants and risk of bleeding outcomes	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB
466	Major hemorrhage risk in chronic kidney disease patients	CIHI-DAD July 1, 1991 - March 31, 2012 ODB October 1, 2001 - March 31, 2009 OHIP July 1, 1991 - March 31, 2012 RPDB Gamma-Dynacare, Cerner & CORR July 1, 1991 - March 31, 2009
467	A laboratory study to clinically validate the relationship between the prespecified DCIS score and the likelihood of local recurrence in patients with ductal carcinoma in situ (DCIS) diagnosed in the Ontario DCIS cohort study	CIHI-DAD 1994 - 2012 CIHI-SDS 1994 - 2012 OHIP 1994 - 2012 RPDB OCR 1964 - 2011
468	Delivery of social assistance cheques and opioid morality	ODB 1997 - 2012 Opioid-Related Death Database 2000 - 2010

#	Project Title	ICES Data
469	AHRQ 2011 - 004: Performance measure for impact of improved service to community - dwelling persons with dementia and their caregivers	CIHI-DAD 2007 - 2011 CIHI-SDS 2007 - 2011 CIHI-NACRS 2007 - 2011 CIHI-CCRS 2007 - 2011 CIHI-NRS 2007 – 2011 ODB 2007 - 2011 OHIP 2007 - 2011 HCD 2007 - 2011 LOC 2007 - 2011 OMHRS 2007 – 2011 RPDB CAPE IPDB Asthma CHF Hypertension COPD ODD OCR RAIHC 2007 - 2011 CPRO
470	Epidemiology of revision anterior cruciate ligament reconstruction in Ontario	CIHI-DAD July 1991 - Sep 2012 CIHI-SDS July 1991 - Sep 2012 CIHI-NACRS 01 April 2002 - Sep 2012 OHIP July 1991 - Sep 2012
471	Consumer access to personal health information for asthma self-management	CIHI-DAD 2011 - 2014 CIHI-NACRS 2011 - 2014 ODB 2011- 2014 OHIP 2011 - 2014 RPDB IPDB Asthma Custom Clinical Dataset (Asthma breathe database 2013 - 2013)
472	Health outcomes, utilization and safety in the elderly with inflammatory bowel disease (HOUSE-IBD) study	CIHI-DAD 1999 - 2012 ODB 1991 - 2012 OHIP 1999 - 2012 HCD 2005 - 2012 RPDB IPDB CHF OCR 1964 - 2012
473	High healthcare user children and youth AHRQ	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 2002 - 2012 CIHI-CCRS 1991 - 2012 ODB 2007 - 2012 OHIP 1991 - 2012 RPDB CAPE Asthma ODD PIBD OCR 1991 - 2011

#	Project Title	ICES Data
474	Primary care reform: Optimizing quality, access, integration and equity in Ontario primary care	CIHI-DAD 2005 - 2013 CIHI-SDS 2005 - 2013 CIHI-NACRS 2005 - 2013 CIHI-CCRS 2005 - 2013 CIHI-NRS 2005 - 2013 ODB 2005 - 2013 OHIP 2005 – 2013 OMHRS 2005 – 2013 RPDB CAPE IPDB CPDB Asthma CHF COPD Hypertension ODD PHYSNET OCR 2005 - 2013 OBSP Cytobase CCHS PCAS
475	Evidence of bupropion misuse by recipients of Ontario drug benefits	CIHI-DAD 1997 - 2012 CIHI-NACRS 1997 - 2012 ODB 1997 - 2012 OHIP 1997 - 2012 OMHRS 1997 - 2012 RPDB IPDB
476	Risk of statin toxicity with the concurrent use of clopidogrel: A propensity-score matched cohort study	CIHI-DAD 1992 - 2012 CIHI-NACRS 1992 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB Hypertension ODD OMID
477	Can carotid plaque assessment predict cardiovascular outcomes?	CIHI-DAD 2008 - 2013 CIHI-NACRS 2008 - 2013 OHIP 2008 - 2013 RPDB Custom Clinical Dataset: Johri KGH Cohort 2011 - 2013

#	Project Title	ICES Data
478	AHRQ - London Health Sciences Centre clinical renewal strategy - part 1	CIHI-DAD 2006 - 2011 CIHI-SDS 2006 - 2011 CIHI-NACRS 2006 - 2011 CIHI-CCRS 2010 - 2011 CIHI-NRS 2010 - 2011 ODB 2006 - 2011 OHIP 2006 - 2011 HCD 2010 – 2011 OMHRS 2006 – 2011 RPDB CAPE IPDB CPDB Asthma COPD Hypertension ODD ADP 2010 - 2011
479	Modeling acute hospital and emergency department utilization in chronic dialysis patients	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 2002 - 2012 OHIP 1991 - 2012 RPDB ORRS 2010 - 2012 CORR 1991 - 2012
480	Patient complexity and use of pharmacy services	CIHI-DAD 2010 - 2012 CIHI-SDS 2010 - 2012 CIHI-NACRS 2010 - 2012 ODB 2010 - 2013 OHIP 2010 - 2012
481	Emergency department utilization by persons with HIV in Ontario	CIHI-DAD 1 April 2005 - 31 March 2010 CIHI-NACRS 1 April 2005 - 31 March 2010 ODB 1 April 2005 - 31 March 2010 OHIP 1 April 2005 - 31 March 2010 RPDB Asthma CHF COPD Hypertension ODD
482	Five views on a journey: Developing a systems model of treatment and care for mental health, substance use and violence problems	CIHI-DAD 2007 - 2012 CIHI-NACRS 2007 - 2012 ODB 2007 - 2012 OHIP 2007 - 2012 OMHRS 2007 - 2012 RPDB IPDB
483	Assessing the health and economic burden of mycobacterial infections using laboratory and health administrative data	CIHI-DAD 1997 - 2012 CIHI-SDS 1997 – 2012 CIHI-NACRS 1997 - 2012 CIHI-CCRS 1997 - 2012 CIHI-NRS 1997 – 2012 ODB 1997 - 2012 OHIP 1997 - 2012HCD 1997 – 2012 RPDB Asthma COPD ODD

#	Project Title	ICES Data
484	Deceased donation in South Asians, Chinese and Europeans	CIHI-DAD 2005 - 2012 OHIP 2005 - 2012 RPDB Trillium Gift of Life Database 2006 - 2012
485	Performance indicators of transplantation	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 OHIP 2002 - 2012 RPDB Trillium Gift of Life Network 2002 - 2012 CORR 2002 - 2012
486	Addressing untreated depression and anxiety in people living with HIV: Evidence to inform health policies and practice: Project 1: Prevalence of depression and anxiety disorders and health outcomes Project 2: Use of mental health care and services and prevalence of untreated depression and anxiety disorders	CIHI-DAD 1 January 1983 - 31 Decemeber 2012 CIHI-NACRS 1 January 1983 - 31 December 2012 ODB 1 January 1983 - 31 December 2012 OHIP 1 January 1983 - 31 December 2012 OMHRS 1 January 1983 - 31 December 2012 RPDB IPDB CPDB OCS Core and extended questionnaires from OCS
487	Systematic observational method for narcolepsy and influenza immunization assessment (SOMNIA)	OHIP 2009 - 2012 RPDB CAPE Chart Abstraction Electronic Health Record
488	AHRQ - Secular trends of long-term ventilation use in Ontario	CIHI-DAD 1996 - 2012 CIHI-SDS 1996 - 2012 CIHI-NACRS 2000 - 2012 CIHI-CCRS 1996 - 2012 CIHI-NRS 2000 - 2012 ODB 1996 - 2012 OHIP 1996 – 2012 HCD 2005 - 2012 OMHRS 1996 – 2012 RPDB IPDB Asthma CHF COPD ODD OMID(Assisted Devices Program) ADP 1996 - 2011
489	Rates and secular trends of ischemic stroke in patients undergoing neck dissection	CIHI-DAD 1992 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB
490	Secular trends in fracture in dialysis patients	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 OHIP 1991 - 2012 RPDB CORR 1991 - 2012

#	Project Title	ICES Data
491	Congestive heart failure indicators for Ontario, 2001 - 2011	CIHI-DAD 2001 - 2013 CIHI-NACRS 2001 - 2013 ODB 2001 - 2013 OHIP 2001 - 2013 HCD 2001 - 2013 LOC 2001 - 2013 RPDB
492	Oxaliplatin and long-term toxicity in older adults with CRC: Population based study	CIHI-DAD 1999 - 2012 CIHI-SDS 1999 - 2012 CIHI-NACRS 2003 - 2012 CIHI-CCRS 2003 - 2012 CIHI-NRS 2005 - 2012 ODB 2003 - 2012 OHIP 1999 - 2012 RPDB CHF COPD ODD NDFP 2005 - 2011 ORGD 2005 - 2012 OCR 1964 - 2011 Stage data as part of the ICES OCR data 2005 - 2011
493	Secular trends in fracture among kidney transplant recipients	CIHI-DAD Jan 1st, 1992 - Dec 31, 2012 CIHI-SDS Jan 1st, 1992 - Dec 31, 2012 ODB Jan 1st, 1992 - Dec 31, 2012 OHIP Jan 1st, 1992 - Dec 31, 2012 RPDB CORR Jan 1st, 1992 - Dec 31, 2012
494	Fracture risk in adult kidney transplant recipients	CIHI-DAD 1991 - 2012 CIHI-SDS 1991 - 2012 CIHI-NACRS 2000 - 2012 ODB 1991 - 2012 OHIP 1991 - 2012 RPDB CORR 1991 - 2012
495	Health Quality Ontario (HQO): Lipids screening and frequency of monitoring	CIHI-DAD 2002 - 2012 CIHI-SDS 2002 - 2012 CIHI-NACRS 2002 - 2012 ODB 2002 - 2012 OHIP 2002 - 2012 RPDB Hypertension ODD CCHS
496	Risk of hospitalization for hypomagnesaemia in patients taking proton pump inhibitors	CIHI-DAD 1992 - 2012 CIHI-NACRS 1992 - 2012 ODB 1992 - 2012 OHIP 1992 - 2012 RPDB Hypertension
497	Impact of the inter-professional spine assessment and education (ISAEC) on imaging and specialist referral for patients with low back pain	OHIP 2009 - 2014 RPDB CPDB CPSO and OHIP billing numbers

#	Project Title	ICES Data
498	Evaluation of percutaneous coronary intervention at new stand-alone centres in Ontario	CIHI-DAD 2011 - 2013 ODB 2011 - 2013 OHIP 2011 - 2013 RPDB CCN 2012 - 2013
499	Validation of OHIP immunization delivery codes using EMR data	OHIP 1991 - 2011 RPDB
500	Validation of hemodialysis vascular access elements in ICES data holdings	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 CIHI-NACRS 1997 - 2011 ODB 2001 - 2011 OHIP 1997 - 2011 RPDB VASPRO, DMAR 2002 - 2011
501	Contemporary management and outcomes of chronic total occlusions (CTO) in stable ischemic heart disease: A population based evaluation	CIHI-DAD 2011 - 2013 CIHI-SDS 2011 - 2013 CIHI-NACRS 2011 - 2013 CIHI-CCRS 2011 - 2013 CIHI-NRS 2011 – 2013 ODB 2011 - 2013 OHIP 2011 - 2013 HCD 2011 - 2013 RPDB IPDB CCN 2011 - 2013 PCCF 2011 - 2013 DALHIN 2011 - 2013
502	CONTRA-AMP study: Incidence, risk factors & outcomes of surgical amputation of a contralateral lower limb -- a population-based study	CIHI-DAD 1992 - 2013 CIHI-NACRS 1992 - 2013 CIHI-NRS 1992 - 2013 ODB 1992 - 2013 OHIP 1992 - 2013 RPDB Hypertension ODD Assisstive Devices Program (ADP) 1992 - 2013 Vital Statistics Death Registry 1992 - 2013
503	Estimating the burden of influenza on healthcare use during the 2012 - 13 influenza season	CIHI-DAD 2002 - 2012 CIHI-NACRS 2002 - 2012 OHIP 2002 - 2012

#	Project Title	ICES Data
504	Cardiac management in patients who are cancer survivors in Ontario	CIHI-DAD April 1988 - March 2012 CIHI-NACRS April 2003 - March 2012 CIHI-SDS April 1991 - March 2012 ODB April 1990 - March 2012 OHIP July 1991 - 3 months ago OHCAS / HCD April 1988 -March 2012 RPDB OCR April 1964 - March 2012 NDFP April 1995 - most recent CHF 1991 - 2010 Hypertension 1988 - 2011 ODD 1991 - 2011 OMID 1992 - 2011
505	Utilization of intravitreal injections in the treatment of AMD in Ontario	ODB 2007 - 2013 OHIP 2007 - 2013 RPDB
506	Risk of non-melanoma skin cancer in immunocompromised patients exposed to voriconazole	CIHI-DAD 1 Jan 2005 - 30 Jun 2012 CIHI-SDS 1 Jan 2005 - 30 Jun 2012 CIHI-NACRS 1 Jan 2005 - 30 Jun 2012 OHIP 1 Jan 1991 - 30 Jun 2012 RPDB OCR 1 Jan 1964 - 30 Jun 2012 Canadian Organ Replacement Register (CORR) 1 Jan 2005 - 31 Dec 2009 Citizenship and Immigration Canada (CIC) 1985 - 2009 ORGD 1 Jan 2005 - 30 Jun 2012 Canadian Cystic Fibrosis Patient Data Registry (CPDR) 1 Jan 1981 - 31 Dec 2008 University Health Network Databases (Organ Transplant Tracking Record, Patient Care Management System, Electronic Patient Records, Lung Transplant Database, Bone Marrow Database) 1 Jan 2000 - 30 Jun 2012 MRN OHIP number
507	Prospective syncope/pre-syncope study	CIHI-DAD Sep 2010 - Aug 2017 CIHI-SDS Sep 2010 - Aug 2017 CIHI-NACRS Sep 2010 - Aug 2017 OHIP Sep 2010 - Aug 2017 RPDB IPDB Prospective Syncope Ontario Database Aug 2010 - Jul 2016
508	Validation of codes for stroke and TIA in CIHI DAD/NACRS compared to the Ontario Stroke Registry	CIHI-DAD 2002 - 2012 CIHI-NACRS 2002 - 2012 OHIP 2002 - 2012 RCSN 2002 - 2012
509	Investigation of notable failed endeavours at reproductive treatment and ischemic long-term events	CIHI-DAD 1993 - 2012 OHIP 1993 - 2012 RPDB
510	Tailoring birth weight and infant growth curves to Canadians of various ethnic backgrounds	CIHI-DAD 2001 - 2012 OHIP 2001 - 2012 MOMBaby CIC 1986 - 2012 EMRALD Surnames database 2001 - 2012

#	Project Title	ICES Data
511	Relationship between iScore, SPAN-100, and PLAN prediction scores and total health care costs among patients with acute ischemic stroke in Ontario	CIHI-DAD CIHI-SDS CIHI-NACRS CIHI-CCRS ODB OHIP RCSN 2003 - 2009
512	The association between radical prostatectomy and inguinal hernia: Is this an example of surveillance bias?	CIHI-DAD 1997 - 2011 CIHI-SDS 1997 - 2011 OHIP 1997 - 2011 RPDB
513	Integration of cancer care in management of complex patients	CIHI-DAD 2008 - 2013 CIHI-SDS 2008 - 2013 CIHI-NACRS 2008 - 2013 CIHI-CCRS 2008 - 2013 CIHI-NRS 2008 - 2013 ODB 2008 - 2013 OHIP 2008 - 2013 HCD 2008 - 2013 OMHRS 2008 - 2013 RPDB IPDB OCR 2008 - 2013
514	Demographic profile of home care clients receiving personal support services	HCD 2012 - 2012 RPDB
515	Determinants of unplanned emergency department utilization among home care clients: Predictors beyond person-level need	CIHI-DAD 1 April 2011 - 31 March 2013 CIHI-NACRS 1 April 2011 - 1 October 2012 CIHI-CCRS 1 April 2010 - 1 October 2012 CIHI-NRS 1 April 2010 - 1 October 2012 OHIP 1 April 2009 - 1 October 2012 HCD 1 April 2011 - 31 March 2012 OMHRS 1 April 2010 - 1 October 2012 RPDB CAPE IPDB
516	Identifying policy interventions to reduce household food insecurity	CIHI-DAD 2000 - 2012 CIHI-SDS CIHI-NACRS ODB OHIP OMHRS RPDB IPDB CCHS
517	The risk of type 2 diabetes, cardiovascular outcomes and mortality in HCV-infected	CIHI-DAD 2000 - 2010 ODB 2000 - 2010 RPDB ODD Ottawa Hospital Viral Hepatitis Database Ottawa Hospital Data Warehouse

#	Project Title	ICES Data
518	KINARK child and family services data project	CIHI-DAD 1 April 2004 - 31 March 2013CIHI-NACRS 1 April 2004 - 31 March 2013OHIP 1 April 2004 - 31 March 2013 RPDB IPDB MOMBaby CIC 1985 – 2012 KINARK
519	Annual incidence of acute myocardial infarction, ischemic stroke, and diabetes in the greater Toronto area	CIHI-DAD 1992 - 2011 OHIP 1992 - 2011 RPDB Census 2002 - 2011
520	Middlesex London Health Unit heat-stress related morbidity	CIHI-DAD 2003 - 2012 CIHI-NACRS 2003 - 2012 RPDB Census PCCF+ ON-Marg 2003 - 2012
521	Sudden cardiac death associated with trimethoprim-sulfamethoxazole while on a renin-angiotensin system inhibitor	CIHI-DAD 1992 - 2013 CIHI-NACRS 1992 - 2013 ODB 1992 - 2013 OHIP 1992 - 2013 RPDB Hypertesnion ORGD 1992 - 2013
522	Follow-up after index colonoscopy in hospital and non-hospital settings	CIHI-DAD 1988 - 2013 CIHI-SDS 1988 - 2013 CIHI-NACRS 1988 - 2013 OHIP 1988 - 2013 RPDB CAPE IPDB CPDB OCR 1964 - 2013
523	Long-term outcomes following critical illness	CIHI-DAD April 1, 2000 - March 31, 2013 CIHI-NACRS 2000 - 2012 CIHI-CCRS 2000 - 2012 CIHI-NRS 2000 - 2012 ODB 2000 - 2012 OHIP 2000 - 2012 HCD 2000 - 2012 RPDB CPDB

#	Project Title	ICES Data
524	ICCP wound care impact assessment	CIHI-DAD 2012 - 2016 CIHI-SDS 2012 - 2014 CIHI-NACRS 2012-2014 ODB 2012 - 2014 OHIP 2012 - 2014 HCD 2012 - 2014 RPDB CHF COPD Hypertension ODD OACCAC Wound Care data
525	Centre-volume and outcomes in critically ill patients with acute kidney injury who receive dialysis	CIHI-DAD 1991 - 2012 CIHI-NACRS 1991 - 2012 OHIP 1991 - 2012 RPDB
526	"INFORM" - Investigating fractures and osteoporosis management	CIHI-DAD 1996 - 2013 CIHI-NACRS 1996 - 2013 CIHI-CCRS 1996-2013 ODB 1996 - 2013 OHIP 1996 - 2013 RPDB IPDB
527	Examining the impact of pharmacy smoking cessation services in Ontario	CIHI-DAD 2006 - 2013 CIHI-SDS 2006 - 2013 CIHI-NACRS 2006 - 2013 CIHI-CCRS 2006 - 2013 CIHI-NRS 2006 - 2013 ODB 2006 - 2013 OHIP 2006 - 2013 HCD 2006 - 2013 LOC 2006 - 2013 RPDB IPDB CPDB
528	Impact of the transition from pediatric to adult medical care on health service utilization in inflammatory bower disease (IBD)	CIHI-DAD 1991 - 2012 CIHI-NACRS 1991 - 2012 OHIP 1991 - 2012 RPDB IPDB PIBD
529	HQO: Effectiveness and cost-effectiveness of prostate specific antigen (PSA) screening in Ontario	CIHI-dad 2002 - 2011 CIHI-SDS 2002 - 2011 ODB 2002 - 2011 OHIP 2002 - 2011 RPDB OCR 2002 - 2011
530	Utilization of inhaled corticosteroid and long-acting beta-2 agonist combination products for the treatment of COPD	CIHI-DAD 2000 – 2012 CIHI-SDS 2000 - 2012 CIHI-NACRS 2000 – 2012 ODB 1999 - 2013 OHIP 2000 - 2013 RPDB Asthma COPD

#	Project Title	ICES Data
531	Cost-effectiveness of combination therapy consisting of either cetuximab or pantiumumab with folfox/folfiri as first-line treatment for kras wild-type metastatic colorectal cancer patients	CIHI-DAD 2006-2010 CIHI-NACRS 2006-2010 CIHI-SDS 2006-2009 ODB 2006-2010 OHIP 2006-2010 OHCAS/HCD 2006-2009 OCR 2006-2009
532	Economic evaluation of tests to reveal the source of cancers of unknown primary	CIHI-DAD 1997-2011 CIHI-NACRS 1997-2011 CIHI-SDS 1997-2011 ODB 1997-2011 OHIP 1997-2011 OHCAS/HCD 1997-2011 OCR 1997-2011
533	Stage IV NSCLC treatment in Ontario: Patterns, outcomes and cost-effectiveness of newer biological and chemotherapeutic agents	CIHI-DAD 2005-2009 CIHI-NACRS 2005-2009 CIHI-SDS 2005-2009 ODB 2005-2009 OHIP 2005-2009 OHCAS/HCD 2005-2009 CCRS 2005-2009 OCR 2005-2009 OBSP Cytobase OCRIS
534	Impact of comorbidity and age on radiotherapy delivery to elderly patients with head and neck cancer	CIHI - DAD 2003 - 2011 CIHI - NACRS 2003 - 2011 CIHI - SDS 2003 - 2011 ODB 2003 - 2011 OHIP 2003 - 2011 OCR 2003 - 2011 NDFP 2003 - 2011
535	Is metformin use associated with higher cause-specific and overall survival rates among diabetic patients with gynecological cancer?	CIHI-DAD 1 Jan 1990 to 31 March 2012 CIHI-NACRS 1 April 2003 to 31 March 2012 CIHI-SDS 1 April 1991 to 31 March 2011 ODB 1 April 1990 to 15 Aug 2012 OHIP 1 July 1991 to 31 July 2012 RPDB OCR 1 Jan 1964 to 31 Dec 2011 CCO Pathology 1 July 1991 to 31 Dec 2010
536	A population-based study on early discontinuation of adjuvant trastuzumab in patients with early breast cancer	CIHI-DAD April 1988 to 2012 CIHI-NACRS April 2003 to 2012 ODB April1990 to 2012 OHIP July 1991 to 2012 RPDB April 1990 to 2012 OCR 2003 to 2012 NDFP 1995 to 2012 CHF 1991 – 2010 Hypertension 1988 to 2011 ODD 1991 to2010 OMID 1992 to 2010

#	Project Title	ICES Data
537	Improving gastric cancer survival: Development and measurement of quality indicators using the RAND/UCLA appropriateness methodology, population-based data analysis for outcomes and economic evaluation of interventions	CIHI-DAD 01/04/2003 to 1/09/2012 CIHI-NACRS 01/04/2003 to 1/09/2012 CIHI-SDS 01/04/2003 to 1/09/2012 ODB 01/04/2003 to 1/09/2012 OHIP 01/04/2003 to 1/09/2012 OHCAS/HCD 01/04/2003 to 1/09/2012 CCRS 01/04/2003 to 1/09/2012 RPDB OCR 01/04/2003 to 1/09/2012
538	Pediatric and adolescent thyroid cancer in Ontario	CIHI-DAD 1988 to 2011 CIHI-NACRS 2003 to 2011 CIHI-SDS 1991 to 2011 ODS 1990 to 2011 OHIP 1991 to 2011 OCR 1991 to 2011
539	defining the alzheimer's population and their use of community care services	CIHI - DAD 2005 - 2011 CIHI - NACRs 2005 - 2011 ODB 2005 - 2011 OHIP 2005 - 2011 OHCAS/HCD 2005 - 2011 CCRS 2005 - 2011 NRS 2005 - 2011
540	A personalized approach to the treatment of malignant melanoma: An economic evaluation of ipilimumab	CIHI-DAD 1991 to 2011 CIHI-NACRS 2003 to 2011 CIHI-SDS 1991 to 2011 ODB 1991 to 2011 OHIP 1991 to 2011 OHCAS/HCD 1991 to 2011 CCRS 1996 to 2011 OCR 01 January 1991 to 31 December 2010 NDFP 1996 to 2011
541	Cost analysis of caring for patients with complex congenital disorders: Effect of ad hoc vs. protocolized approach to long-term care and cancer screening for esophageal atresia/tracheoesophageal fistula (EA/TEF) patients	CIHI-DAD April 1 1997 - March 31 2012 CIHI-NACRS April 1 2003 - March 31 2012 CIHI-SDS April 1 1997 - March 31 2012 ODB April 1 1997 - March 31 2012 OHIP April 1 1997 - March 31 2012 OHCAS/HCD April 1 1997 - March 31 2012 CCRS April 1 1997 - March 31 2012 RPDB OCR April 1 1997 - March 31 2012
542	Pilot project to determine feasibility of developing a minimal data set using cd-link in order to develop indicators for traumatic spinal cord injury.	CIHI-DAD 2001 - 2012CIHI-NACRS 2001 - 2012CIHI-SDS 2001 - 2012OHIP 2001 - 2012OHCAS/HCD 2001 - 2012NRS 2001 - 2012

Appendix C – Privacy Impact Assessments

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
1	Stroke registry migration	11/17/2011	Data holding	PIA required	Closed	1. Amend site DSAs to reflect transfer to ICES 2. Reflect transfer in stakeholder information 3. Inform any involved REBs	Recommendations accepted	#1 and #2 – Information was included in site DSAs #3 – Informed involved REBs	31/12/2011
2	Offender Management System	5/24/2012	Data holding	PIA required	Closed	None	n/a	n/a	n/a
3	External researcher safeguards review (individual)	11/14/2012	Disclosure	PIA required	Closed	1. Make secure storage of back-up drive a recipient contractual obligation	Recommendation accepted	#1 – Addressed in the DRA (Data Release Agreement) in the security section	19/12/2012
4	Backup system RFQ	6/5/2012	Information system	PIA required	Closed	1. Require criminal background checks up-front and annual training on ICES procedures, breach notification	Input accepted	#1 – Addressed in the Request for Quote for the suppliers	5/6/2012
5	Backup migration	7/23/2012	Service provider	PIA required	Closed	1. Perform and document pre-move wipe	Recommendation accepted	#1 – ICES' IT performed a pre-move wipe and documented this	8/31/2012
6	External researcher safeguards review (NSHRU)	8/27/2012	Disclosure	PIA required	Closed	1. Limit disclosure to anonymized data 2. Require use reporting in DSA 3. Address retention in DSA	Recommendation accepted	All recommendations were addressed in the DSA	6/9/2013
7	Introduce inter-HIC disclosures to HOBIC service	7/22/2013	Disclosure	PIA required	Closed	1. Amend site DSAs to grandfather third party credentialing and access management and authorize inter-HIC sharing 2. Address ICES' reliance on third party safeguards, including breach detection and response, through a contract 3. Create filter to identify participating sites, and define processes to maintain accurate and current site classifications 4. Conduct TRA	Recommendations accepted	#1 and #2 – Addressed in the DSA #3 and #4 – Addressed as part of the project implementation	7/23/2013

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
8	New patient demographic module (stroke application)	7/26/2012	Technology	PIA required	Closed	1. Implement role- and location-based access controls 2. Implement logging to enable detection and monitoring of inappropriate user activity 3. Reinforce user understanding by adding log-in reminder and privacy footers (nice-to-have)	Recommendations accepted	#1 and #2 – Addressed as part of project implementation #3 – Not implemented	#1 and #2 - 2/28/2013 #3 – Will not be implemented as application was decommissioned as of 04/11/2014
9	Third party data cleaning module	10/10/2012	Technology	PIA required	Closed	1. Prevent user download and printing 2. Store data on encrypted hard drive 3. Document wipe process 4. Require destruction certificate and sign off	Recommendations accepted	All recommendations were addressed as part of the project implementation	5/10/2012
10	ICES network architecture (initial)	8/16/2012	Information system	PIA required	Closed	None	n/a	n/a	n/a
11	Clean room protocol (Privacy Preserving Protocol)	Proposed date: TBD	Data holding	PIA required	Ongoing	n/a	n/a	n/a	n/a
12	Patient-level feedback (EMRALD - SAFIRE)	7/31/2013	Disclosure	PIA required	Closed	1. Develop formal data upload and transfer process 2. Implement small cell size restriction 3. Define and implement procedures to keep patient-physician associations, and associated access controls 4. Defer launch until all TRA recommendations cleared 5. Implement audit and monitoring	Recommendations accepted	#1 – Addressed through creation of SOP #2 and #3 – Implemented as part of the technology solution #4 – Implemented as part of the technology solution #5 - Implementation planned	#1 - 05/30/2013 #2 and #3 – 07/29/3013 #4 – 8/14/2013 #5 – Proposed date: 03/31/2015
13	Skillsoft e-learning software	10/4/2012	Service provider	Not required Reason: No personal	Closed	n/a	n/a		n/a

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
				health information involved					
14	Web content software	10/17/2012	Information system	PIA required	Closed	1. Develop an Internet Usage Privacy policy to reflect what is being collected from the users and for what purpose and usage. 2. Privacy Office will need to be involved in the design process to understand the solution design and ensure that accurate information is covered under the privacy website statement	Recommendation accepted	#1 – Privacy Office was actively involved in meetings related to web content software #2 – Privacy website statement was posted on the ICES website	02/28/2014
15	UNIX system upgrade	Proposed data: 10/31/2014	Technology	PIA required	Ongoing	1. Maintain configuration documentation related to server hardening and patching 2. Assign responsibility for identification of test data and uses cases 3. Maintain data migration documentation, including validation and sign offs 4. Securely destroy decommissioned servers, and in other cases perform, document and verify secure wipe 5. Configure logging to capture unauthorized attempts and implement regular review 6. Document intrusion detection configurations, including purposes	n/a	n/a	Proposed date: 03/31/2015

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
16	New enterprise printers	12/21/2012	Technology	PIA required	Closed	1. Use automated hard drive wipe functionality and set timeframe 2. Reinforce in SLA no vendor access to print job content, by remote reporting or otherwise 3. Restrict scan-to-email and fax functionality to internal addresses 4. Require service personnel NDA	Recommendations accepted	#1, #2 and #3 – Addressed as part of the technology solution #4 – Address in the vendor contract	3/31/2013
17	Backup system	1/4/2013	Information system	PIA required	Closed	1.Require encryption of data storage disk 2.Require security of transfer and associated logging 3.Verify process for making backed up data/records available	Recommendations accepted	All recommendation addressed in Request for Quote	1/04/2013
18	Enterprise storage area network	n/a	Service provider	Not required Reason: Initiative was covered under UNIX system upgrade (above)	n/a	n/a	n/a	n/a	n/a
19	External researcher environment	7/25/2013	Disclosure	PIA required	Closed	1. Adapt offline researcher user terms to new delivery method 2. Build in mechanism to reinforce appropriate use (e.g. log-in message, online privacy footer/FAQ) 3. Implement intrusion detection and event alerts with supporting response processes 4. Create user agreement and create meaningful mechanisms to reinforce appropriate use	Recommendations accepted	All recommendations to be addressed as part of project implementation	Proposed date: 01/02/2014

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
						(e.g. log-in message, online privacy footer/FAQ)			
20	Enterprise backup system RFP response (Open Storage)	3/11/2013	Technology	PIA required	Closed	1. Encrypt tapes 2. Set retention schedule, and configure to, comply with ICES requirements 3. Incorporate reporting and notifications of backup and restore activities, and create supporting roles and responsibilities and routines for review 4. Address vendor staff confidentiality duties in any SLA	Recommendations accepted	#1, #2 and #3 – Addressed as part of technology solution #4 Addressed in SLA (Service Level Agreement)	03/11/2013
21	Secure file transfer application (Axway)	Proposed completion date- 8/31/2014	Information system	PIA required	Ongoing	n/a	n/a	n/a	n/a
22	Ministry of Education aggregate data	5/13/2013	Data holding	PIA required	Closed	1. Adjust variables list in DSA to prevent re-identification	Recommendation accepted	#1 – Variable list in DSA was adjusted to prevent re-identification	7/10/2013
23	Linkage software testing	6/7/2013	Technology	PIA required	Closed	1. No authority to use selected data	n/a	#1 – Project team created “dummy” data for testing purposes	6/7/2013
24	Encryption software requirements	Proposed completion date- 3/31/2015	Technology	PIA required	Ongoing	n/a	n/a	n/a	n/a
25	Drug & Alcohol Treatment Information System	6/3/2013	Data holding	PIA required	Closed	1. Add contractual support in DSA for s.44 research uses	Accepted	#1 – DSA was revised to include support for s. 44 research uses	6/17/2013
26	Wireless LAN (requirements)	6/7/2013	Technology	Not required Reason: No personal health information was involved	Closed	n/a	n/a	n/a	n/a

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
27	Intrusion Detection & Penetration System	Proposed date: 5/31/2015	Information system	PIA required	Ongoing	Preliminary recommendations: 1. Perform security/functional testing of IDPS rules and configurations 2. Establish and configure rules for collection of IP addresses 3. Use encrypted tunnels or other cryptographic measures to hide and authenticate IDPS communications 4. Encrypt communication between IDPS components (sensors, middle tier, management console) 5. Assign responsibility to monitor software support centre for bugs, errors and deficiencies 6. Include IDPS in the patch schedule and designate for regular patching 7. Set up a process, and roles and responsibilities, for signature updates 8. Secure logs to limit access and prevent modification 9. Define a process for system administrators to address, assess and report suspicious activity 10. Perform DR site testing and maintain supporting documentation 11. Provide for regular backup of the configuration and servers 12. Require NDA for vendor support workers	n/a	n/a	n/a
28	Gephi software	n/a	Technology	Not required	n/a	n/a	n/a		n/a

#	Description of Data Holding, Information System, Technology or Program	PIA Completion Date	PIA Type	Assessment Determination	PIA Status	Recommendation(s)	Recommendation(s) Status	Manner of Implementing Recommendation(s)	Date Recommendation(s) Implemented
				Reason: Software initiative was discontinued					
29	Mobile calculator	7/17/2013	Technology	Not required Reason: No personal health information involved	n/a	n/a	n/a		n/a
30	Ontario Brain Institute pilot project	Proposed date: TBD	Data holding	PIA required	Ongoing	n/a	n/a	n/a	n/a
31	Stand-alone PC exception	4/23/2013	Information system	PIA required	Closed	None	n/a	n/a	n/a
32	Ontario Brain Institute collaboration	Proposed date: TBD	Data holding	PIA required	Ongoing	n/a	n/a	n/a	n/a
33	Iron Mountain (offsite data storage)	Proposed date: 12/30/2014	Information system	PIA required	Ongoing	n/a	n/a		n/a

Appendix D – Privacy Audits

Privacy audit	Description	Date completed	Recommendation(s)	Date recommendation(s) addressed	Action(s) take to address recommendation
Assessing data for sensitive variables	Entire ICES data repository was scanned for presence of sensitive variables and checked against access permitted to each file.	2013-11-15	Tighten access controls to reflect the nature and sensitivity of the information content.	2013-12-01	File access controls were modified, using the computer's operating system.
Assessing data for free text containing sensitive information	Entire data repository was scanned for presence of fields that might be free-text. In particular, a field was flagged if it was >50 characters long, had at least one value >30 characters long; and contained >50 unique values.	2014-07-07	1. One field in one dataset was found to contain sensitive information. That field has been removed from the de-identified data. 2. The steps for processing of incoming data were modified to examine each dataset for the presence of free-text fields.	1. 2014-07-08 2. 2014-07-09	1. The dataset was deleted, and replaced with a dataset with that field removed. 2. A macro to check for free-text fields was developed, and included in the basic processing macro. A procedure to deal with fields containing such sensitive information is under development.
Verifying continued need for access to ICES controlled use data	Agents receive access to datasets based on the projects they are assigned to. Once a year, the analyst leads are requested by e-mail to verify the continued need for access to such data. Their response is recorded; and access which is no longer needed is removed.	2013-05-30	Remove access for agents who no longer need access to a controlled use dataset.	2013-05-30	ICES' Information Technology was notified to remove agents' access.
Assessing completeness and accuracy of ICES project PIA log	The ICES project PIA log, which captures agents granted approval to access and use de-identified information for ICES projects, was reviewed for accuracy and completeness.	2013-01-13	Address incomplete or inaccurate data access and use information.	2013-01-13	ICES project PIA log was updated to include missing or inaccurate data access and use information.
Verifying renewal of annual confidentiality agreements	The privacy awareness log was reviewed to ensure all applicable agents have renewed their annual confidentiality agreements.	2013-10-30	1. Notify each agent whose renewal is pending. 2. Suspend access to ICES systems for any agent who does not renew prior to a specified deadline.	1. 2013-05; 2013-06; 2013-09; 2013-10; 2014-01 2. 2014-02	1. Several notifications were sent via email. 2. ICES Information Technology suspended access to ICES systems for any agent who had failed to review by the deadline.

Appendix E – Security Policies & Procedures

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
Security Audit Policy	Establishes the framework for conducting security audits of ICES networks and information system resources and processes in order to determine areas of vulnerability and initiate appropriate remediation	New	Jul-13	n/a	Jul-14	n/a	Required	07/22/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
Security Audit SOP	Sets out the steps for executing the internal security audit function	New	Jun-14	n/a	Oct-14	n/a	Security staff only	06/23/14	Training Security staff, SharePoint posting	Not required	n/a	n/a
Security Framework & Governance Policy	Establishes the framework for ICES' governance of security programs, polices, procedures and practices necessary for the protection of personal health information	New	Jun-14	n/a	Jun-15	n/a	Required	06/23/14	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Data Management Policy	Governs ICES' management of personal health information and other data throughout the information life cycle	Revised	Pre 2011 IPC review	Nov-13	Nov-14	The policy was derived from "ICES Information Asset Management Program" developed in Sep-10. The content was revised to cover protection of personal health information and other only.	Required	Communic ation of revised version planned	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Data Management	Defines the standards for	Revised	Pre 2011 IPC	Nov-13	Nov-14	The standard was derived from the	Required	Communic ation of	Training, staff meeting, staff	Not required	n/a	n/a

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
Standard	secure retention, destruction and disposal of personal health information and other data		review			"Physical Assets: Classification and Handling Procedures", developed in Sep-10. The content was revised to cover protection of personal health information and other only		revised version planned	email, intranet posting			
Secure Transfer of Personal Health Information	Sets out the steps for inbound and outbound transfers of personal health information and other data	New	Aug-14	n/a	Aug-15	n/a	Required	26/08/14	Intranet posting	Not required	n/a	n/a
Information Media Destruction SOP	Sets out the approved methods and steps for secure destruction of personal health information and other data in electronic or paper format	New	Planned	n/a	n/a	n/a	Required	Planned	n/a	Not required	n/a	n/a
Destruction of ICES Data SOP	Sets of the steps for secure destruction of personal health information in electronic form	New	Aug-14	n/a	Aug-15	n/a	Required	26/08/14	Intranet posting	Not required	n/a	n/a
Security Training Policy	Governs ICES' security training program	New	Oct-13	n/a	Oct-14	n/a	Required	11/01/13	Intranet posting	Not required	n/a	n/a
ICES Security Training - Delivery Method SOP	Sets out the steps for scheduling and delivering security training	New	Jun-14	n/a	Oct-14	n/a	Required	06/23/14	Training, staff meeting	Not required	n/a	n/a

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
ICES Security Training - Content Management SOP	Defines the content of ICES' security training	New	Jun-14	n/a	Oct-14	n/a	Security staff only	06/23/14	Training Security staff, SharePoint posting	Not required	n/a	n/a
Initial Security Orientation Attendance Sheet	Used to record attendance at security orientation	New	Jun-14	n/a	Nov-14	n/a	Security staff only	06/23/14	Training Security staff, SharePoint posting	Not required	n/a	n/a
Security Training & Awareness Log	Used to log completion of security training	New	Jun-14	n/a	Nov-14	n/a	Security staff only	06/23/14	Training Security staff, SharePoint posting	Not required	n/a	n/a
Physical Security Policy	Governs the physical security of ICES facilities	New	May-13	n/a	May-14	n/a	Required	07/22/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
ICES-Central Physical Security SOP	Sets out the configuration and steps for management of physical security systems including electronic access systems, intrusion detection systems and CCTV system	New	Jun-13	Nov-13	Jun-15	n/a	Required	06/01/13; 06/13/14	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
Visitors Policy	Governs the responsibilities of ICES staff who are supervising visitors at ICES	Revised	Jul-13	Nov-13	Jul -14	Updated to include new requirements for granting physical access to visitors	Required	07/22/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Central Visitors SOP – Electronic Access Badge	Sets out the steps for granting physical access to visitors	New	Jun-14	n/a	Jun-15	n/a	Required	06/13/14	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Central Visitors SOP	Sets out the steps for granting	New	Jun-14	n/a	Jun-15	n/a	Required	06/13/14	Training, staff meeting, staff	Not required	n/a	n/a

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
– Non-Electronic Access Badge	physical access to visitors								email, intranet posting			
Acceptable Use Policy	Defines the rights and responsibilities for agents accessing and using ICES computing systems	Revised	Pre 2011 IPC review	Nov-13	Oct-14	The “Appropriate Use of Computer Equipment Policy” was revised and updated to clearly articulate an agent’s responsibilities, with respect to accessing and using ICES computing systems	Required	11/01/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
System Control and Audit Log Policy	Governs the requirements for creating, maintaining and reviewing system control and audit logs	New	Jun-14	n/a	Jun-15	n/a	Required	06/23/14	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
System Control and Audit Log SOP	Sets the steps for configuration, scheduling and review of system controls and audit events	New	Jun-14	n/a	May-15	n/a	Security staff only	06/23/14	Training	Not required	n/a	n/a
System Control and Audit Log Standard	Defines the standard list of system controls and audit events to be monitored and collected into the Security Information and Events Management (SIEM) system	New	Jun-14	n/a	May-15	n/a	Required	06/23/14	Training Security and IT staff, SharePoint posting	Not required	n/a	n/a
Password Policy	Defines ICES’ standards for the creation of strong	New	May-13	Nov-13	May-15	n/a	Required	07/22/13	Training, staff meeting, staff email,	Not required	n/a	n/a

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
	passwords, the protection of the passwords and the frequency of password changes								intranet posting			
Remote Access Policy	Sets out the security principles to protect ICES information and systems when accessed remotely by authorized agents	New	Oct-13	n/a	Oct-14	n/a	Required	11/01/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
Information System Acquisition, Development and Maintenance Policy	Governs the adoption of the "built-in security" principle throughout the entire life-cycle of an information system, from planning, acquisition and/or development, design to operational stage	New	Sep-13	n/a	Sep-14	n/a	Required	09/25/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
Information System Acquisition, Development and Maintenance SOP	Sets out the steps to be followed in the following phases of the life-cycle of an information system: planning phase, RFP/RFQ phase, design phase, deployment phase	New	Jun-13	n/a	Oct-14	n/a	Required	06/01/13; 06/23/14	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
Patch Management	Governs the requirements for	New	Jun-13	n/a	Jun-14	n/a	Required	07/22/13	Training, staff meeting, staff	Not required	n/a	n/a

Name	**Description**	**Status**	**Implem-entation Date**	**Last ICES Review**	**Next Planned ICES Review**	**Description of Change(s)**	**Internal Communication (IC)**	**IC Date**	**IC Method**	**Public Communication (PC)**	**PC Date**	**PC Description** *As applicable*
Policy	ICES' computing systems patching process in order to minimize security vulnerabilities								email, intranet posting			
Security Incident Management Policy	Establishes a standard for managing security incidents	Revised	Pre 2011 IPC review	Nov-13	Sep-14	Reference to all procedural controls were moved into ICES Security Incident Management SOP	Required	09/25/13	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
ICES Security Incident Management SOP	Sets out procedures for notifying, containing, investigating and remediating security incidents and breaches	New	May-13	Nov-13	Nov-14	n/a	Required	06/23/14	Training, staff meeting, staff email, SharePoint posting	Not required	n/a	n/a
ICES Security Incident Report Template	Used to document security incidents and breaches	New	Oct-13	n/a	Oct-14	n/a	Security staff only	31/10/2013	Training	Not required	n/a	n/a
Data Backup Policy	Governs the rules and guidelines for Data Backup in order to prevent the loss of information in the event of accidental deletion or corruption of files, system failure or natural disaster, and to permit timely restoration of information when such events occur	Replace ment	Jun-14	n/a	Jun-15	New policy clarifies frequency of back-ups, availability of backed-up records, engagement of third party service providers, and roles and responsibilities	Required	06/23/14	Training Security and IT staff, SharePoint posting	Not required	n/a	n/a
Information Technology	Defines rules and guidelines for	Replace ment	Jun-14	n/a	Jun-15	New policy clarifies scope of policy,	Required	06/23/14	Training Security and	Not required	n/a	n/a

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
Change Management Policy	controlling and managing changes to ICES' computing systems					requirements for making changes to ICES' information systems and roles and responsibilities			IT staff, SharePoint posting			
Information Technology Change Management SOP	Sets out the steps for requesting, approving, initiating, testing, executing and verifying a change to ICES information systems	Replace ment	Jun-14	n/a	Jun-15	New SOP clarifies the procedures for requesting, approving, initiating, testing, executing and verifying changes to ICES' operational environment	Security staff only	06/23/14	Training Security and IT staff, SharePoint posting	Not required	n/a	n/a
Mobile Devices Policy	Governs the provisioning and use of mobile devices for ICES business purposes	Revised	Pre 2011 IPC review	Nov-13	Nov-14	n/a	Required	10/01/12	Training, staff meeting, staff email, intranet posting	Not required	n/a	n/a
Security Audit Log	Used to log and document security audits	New	Jun-14	n/a	Jun-15	n/a	Security staff only	06/23/14	Training	Not required	n/a	n/a
Security Incident Log	Used to log and document security incidents	New	Jun-14	n/a	Jun-15	n/a	Security staff only	06/23/14	Training Security and IT staff, SharePoint posting	Not required	n/a	n/a
Security Risk Assessment Log	Used to log the risk assessments as defined in Security Audit Policy, and operationalized through Security Audit SOP	New	Jun-14	n/a	Jun-15	n/a	Security staff only	06/23/14	Training Security and IT staff, SharePoint posting	Not required	n/a	n/a
ICES Threat Risk Assessment Log	Used to log the information security threat risk assessments as	New	Jun-14	n/a	Jun-15	n/a	Security staff only	06/23/14	Training Security and IT staff, SharePoint	Not required	n/a	n/a

Name	Description	Status	Implem-entation Date	Last ICES Review	Next Planned ICES Review	Description of Change(s)	Internal Communication (IC)	IC Date	IC Method	Public Communication (PC)	PC Date	PC Description *As applicable*
	defined in Security Audit Policy, and operationalized through Security Audit SOP.								posting			

30-Sep-2014

Appendix F – Physical Security Audits

#	Location Accessed	Type of Audit	Nature of Audit	Date Audit Completed	Recommendation	Manner Recommendation Addressed	Date Recommendation Addressed
1	ICES Central	Physical access audit	Audit of access to ICES premises.	11/7/2011	To review the list of agents with access to premises and any restricted security zones as defined in the old electronic access system and map it to the access groups list from the new electronic access system before transferring the list into the new access system.	The list of users with access to premises and any restricted security zones was generated from the old key system. The list was reviewed by the Functional Managers, as part of the initial setup for the new EAS. The required level of physical access was determined for each agent and the system was configured accordingly.	1/10/2012
2	ICES Central: physical access to the restricted areas (GG48, IT Corridor, Server Rooms)	Physical Access audit	Audit of access to restricted areas audited (Data Center and IT corridor).	06/18/2012	To remove unrequired access into restricted areas.	Functional Managers were asked to review and update the need for access for each of their staff. All unrequired access was removed.	6/30/2012
3	ICES Central: additional restricted area was created (GG53)	Physical access audit	Audit of the Electronic Access System's configuration and access to a new restricted area (anti-passback, schedules, access level categories).	12/6/2014	To define the group of agents that require access to restricted zone, GG53, and program the system accordingly.	Access to GG53 was restricted to the Data Management group. The DQIM Director was asked to define the name of agents with access to this office. The system was programmed accordingly.	12/6/2012
4	ICES Central	Physical access audit	Audit of the list of Sunnybrook Security Services personnel with approved access to ICES premises.	04/23/2013	To review the list of security personnel with access to ICES perimeter and remove any unrequired access.	Sunnybrook Security Services Manager reviewed the need for access for each of its staff, who normally have access to restricted areas at ICES. It was identified that some of the existing staff on the list have new ID badges, some were no longer with Sunnybrook Security Services, and there were new	4/29/2013

						staff who would require access. The updated list was returned to ICES Security Lead. ICES' System Administrator programmed it accordingly (old ID cards were decommissioned, access was removed for all terminated staff, and new staff were granted access).	
5	ICES Central	Physical access audit	Audit the list of Sunnybrook Security Services personnel with access to premises.	11/13/2013	To review the list of security personnel with access to ICES perimeter and remove any unrequired access.	Sunnybrook Security Services Manager reviewed the need for access for each of their staff, who normally have access to restricted areas at ICES. It was identified that some of the existing staff on the list have new ID badges, some were no longer with Sunnybrook Security Services, and there were new staff who would require access. The updated list was returned to ICES Security Lead. ICES' System's Administrator programmed it accordingly (old ID cards were decommissioned, access was removed for all terminated staff, and new staff were granted access).	11/20/2013

Appendix G – Information Security Breaches

#	Category	Notification Date	Extent	PHI Nature & Extent	Management Notice Date	Containment Measures	Containment Date	Third Party Notice Date	Investigation Start Date	Investigation Complete Date	Recommendation(s)	Manner Recommendation(s) Addressed	Date Recommendation(s) Addressed
1	PHI Breach	7/5/12	Patient data information revealed to the project manager - ICES Central	Patient data information accessed by project manager at ICES Central	7/5/12	Incident was contained by shutting down the database to perform a preliminary investigation. This action terminated access to the application to all agents.	7/5/12	n/a	7/5/12	7/6/12	~ Fix to be developed to remediate this issue ~ Fix to be applied in the staging environment ~ Testing of fix to be performed ~ Results to be validated and signed off by Privacy & Security ~ Fix to be promoted in the production environment ~ User access to be enabled to all users/sites	The recommendations were accepted in full and addressed as proposed	7/10/2012
2	Security Incident	11/12/12	IDS alarm notifications - ICES UofT	n/a	n/a	n/a This security incident was related to malfunctions or misconfigurations reported in relation to the physical security systems. There	n/a	n/a	11/12/12	11/19/12	~ Confirm technical issues with Honeywell network in campus were addressed ~ Properly configure one camera with motion activation	The recommendations were accepted in full and addressed as proposed	11/19/2012

#	Category	Notificat-ion Date	Extent	PHI Nature & Extent	Manage-ment Notice Date	Containment Measures	Contain-ment Date	Third Party Notice Date	Investigation Start Date	Investig-ation Complete Date	Recommend-ation(s)	Manner Recommend-ation(s) Addressed	Date Recommend-ation(s) Addressed
						was no possibility for the issue to spread and affect other systems, nor did it present a risk to ICES computing systems, as the physical security network is segregated from the computing network within ICES' environment. For this reason, containment measures were not necessary.							
3	Security Incident	11/21/12	IDS alarm notifications - ICES UofT	n/a	n/a	n/a This security incident was related to malfunctions or misconfigurations reported in relation to the physical security systems. There was no possibility for the issue to spread and affect	n/a	n/a	11/22/12	11/29/12	~ Confirm technical issues with Honeywell network in campus were addressed ~ For one week, to monitor the IDS activity for false alarms and escalate to Honeywell if any technical issues suspected	The recommendations were accepted in full and addressed as proposed	11/29/2012

#	Category	Notification Date	Extent	PHI Nature & Extent	Management Notice Date	Containment Measures	Containment Date	Third Party Notice Date	Investigation Start Date	Investigation Complete Date	Recommendation(s)	Manner Recommendation(s) Addressed	Date Recommendation(s) Addressed
						other systems, nor did it present a risk to ICES computing systems, as the physical security network is segregated from the computing network within ICES' environment. For this reason, containment measures were not necessary.							
4	Security Incident	11/25/12	IDS alarm notifications - ICES UofT	n/a	n/a	n/a This security incident was related to malfunctions or misconfigurations reported in relation to the physical security systems. There was no possibility for the issue to spread and affect other systems, nor did it present a risk to ICES	n/a	n/a	11/26/12	11/25/12	~ Reset IDS system	The recommendations were accepted in full and addressed as proposed	11/25/2012

#	Category	Notificat-ion Date	Extent	PHI Nature & Extent	Manage-ment Notice Date	Containment Measures	Contain-ment Date	Third Party Notice Date	Investigation Start Date	Investig-ation Complete Date	Recommend-ation(s)	Manner Recommend-ation(s) Addressed	Date Recommend-ation(s) Addressed
						computing systems, as the physical security network is segregated from the computing network within ICES' environment. For this reason, containment measures were not necessary.							
5	Security Incident	12/08/12	Campus Police lost the communic ation with the site's IDS - ICES UofT	n/a	n/a	n/a This security incident was related to malfunctions or misconfigurations reported in relation to the physical security systems. There was no possibility for the issue to spread and affect other systems, nor did it present a risk to ICES computing systems, as the physical security	n/a	n/a	12/10/12	12/10/12	~ Confirm technical issues with Honeywell network in campus were addressed	The recommendation s were accepted in full and addressed as proposed	12/10/2012

#	Category	Notificat-ion Date	Extent	PHI Nature & Extent	Manage-ment Notice Date	Containment Measures	Contain-ment Date	Third Party Notice Date	Investigation Start Date	Investig-ation Complete Date	Recommend-ation(s)	Manner Recommend-ation(s) Addressed	Date Recommend-ation(s) Addressed
						network is segregated from the computing network within ICES' environment. For this reason, containment measures were not necessary.							
6	Security Incident	5/16/2013	Historical CCTV recordings lost - ICES Western	n/a	n/a	n/a This security incident was related to malfunctions or misconfigurations reported in relation to the physical security systems. There was no possibility for the issue to spread and affect other systems, nor did it present a risk to ICES computing systems, as the physical security network is segregated from the computing	n/a	n/a	5/16/13	6/7/13	~ Connect new external HDD until root cause is identified and addressed and ensure no further video data are lost ~ Investigate root cause and fix it.	The recommendations were accepted in full and addressed as proposed. It was identified that the issue was caused by a configuration setup which was corrected on the same day as identified.	6/7/13

#	Category	Notificat-ion Date	Extent	PHI Nature & Extent	Manage-ment Notice Date	Containment Measures	Contain-ment Date	Third Party Notice Date	Investigation Start Date	Investig-ation Complete Date	Recommend-ation(s)	Manner Recommend-ation(s) Addressed	Date Recommend-ation(s) Addressed
						network within ICES' environment. For this reason, containment measures were not necessary.							
7	Policy Breach	6/12/13	1 transfer USB key - ICES Central	n/a	6/12/13	Transfer logs were checked to identify the files being transferred by the last agent using the USB Transfer key. The files were checked and it was confirmed that they contained only aggregate data.	6/12/13	n/a	6/12/13	6/13/13	~ Wire back the Transfer USB key ~ Explain to user involved in the incident about security requirements around Transfer DTU activities	The recommendations were accepted in full and addressed as proposed	6/13/2013
8	Policy Breach	7/31/13	PROD data found on DEV and STAGE Saphire environments - ICES Central	n/a (this system does not contain identified information)	7/31/13	Production data was removed from both DEV and STAGE environments	7/31/13		7/31/13	7/31/13	~ Production data to be removed from DEV and STAGE environments ~ DBA, AppDev staff were explained that PROD data cannot be used for QA testing as per ICES policies	The recommendations were accepted in full and addressed as proposed	7/31/2013

#	Category	Notificat-ion Date	Extent	PHI Nature & Extent	Manage-ment Notice Date	Containment Measures	Contain-ment Date	Third Party Notice Date	Investigation Start Date	Investig-ation Complete Date	Recommend-ation(s)	Manner Recommend-ation(s) Addressed	Date Recommend-ation(s) Addressed
9	Policy Breach	8/15/13	Passwords changed for some admin level accounts on network devices - ICES Central	n/a	8/15/13	Passwords changed by all system administrators for all admin level accounts	8/15/13	n/a	8/15/13	8/20/13	~ HR to follow up with the dismissed network admin, to recover all passwords ~ Bring in a consultant ~ Review the configurations on the network devices by comparing with the latest backup available ~ Reset all root-level passwords and undo the unapproved configuration changes made since the latest backup	The recommendations were accepted in full and addressed as proposed	8/20/2013
10	Policy Breach	9/17/13	1 temporary password distributed without proper verification of the user - ICES Queen's	n/a	n/a	n/a The password was distributed over the phone to the correct trusted party, but not in accordance with the standard identification process. No		n/a	9/17/13	9/17/13	~ 1. Review latest updates for Accounts Management Policy with the Helpdesk support staff ~ 2. Document the SOP to ensure compliance with the policy	The recommendations were accepted in full to be addressed as proposed: #1 – implemented #2 - planned	*#1 – 9/17/13* *#2 – 31 Oct 2014 (planned)*

#	Category	Notificat-ion Date	Extent	PHI Nature & Extent	Manage-ment Notice Date	Containment Measures	Contain-ment Date	Third Party Notice Date	Investigation Start Date	Investig-ation Complete Date	Recommend-ation(s)	Manner Recommend-ation(s) Addressed	Date Recommend-ation(s) Addressed
						containment measures were necessary.							
11	Security Incident	10/3/13	1 transfer USB key - ICES Central	n/a	n/a	To wire back the Transfer USB key	10/3/13	n/a	10/3/13	10/4/13	~ Explain to users last using unwired Transfer USB Key to, next time, report it to Helpdesk, to avoid similar future issues	The recommendations were accepted in full and addressed as proposed	10/4/2013

Appendix H – Glossary

A. ICES Data

Data	Description
ADP	Assistive Devices Program
ALR	Activity Level Support
Asthma	Ontario Asthma Database
BORN	Better Outcomes Registry & Network
CAPE	Client Agency Program Enrollment
CCHS	Canadian Community Health Survey
CCN	Cardiac Care Network
CCO	Cancer Care Ontario
Cerner	Cerner lab data
CHCCDB	Central Home Care Client Database
CHF	Ontario Congestive Heart Failure Database
CIC	Citizenship and Immigration Canada
CIHI-CCRS	Canadian Institute for Health Information - Continuing Care Reporting System
CIHI-DAD	Canadian Institute for Health Information - Discharge Abstract Database
CIHI-NACRS	Canadian Institute for Health Information - National Ambulatory Care Reporting System
CIHI-NRS	Canadian Institute for Health Information - National Rehab System
CIHI-SDS	Canadian Institute for Health Information - Same Day Surgery Database
CIRT	Colonoscopy Interim Reporting Tool
Contact	Yearly contact with health services
COPD	Ontario Chronic Obstructive Pulmonary Disease Database
Coroner	Cause of Death from Coroner Investigation
CORR	Canadian Organ Replacement Registry
CPDB	Care Provider Database
CPDR	Canadian Cystic Fibrosis Data Registry
CPRO	Client Profile Database
Cytobase	Cervical Cytology Data
DMAR	Dialysis Measurement Analysis Reporting System
EFFECT	Enhanced Feedback for Effective Cardiac Treatment
EMRALD	Electronic Medical Records Administrative Linked Database
ERCLAIM	OHIP emergency claims created at ICES from OHIP claims
HCD	Home Care Database
HIV	Ontario HIV Database
HOBIC	Health Outcomes for Better Information and Care
Hypertension	Ontario Hypertension Database
IBD	Inflammatory Bowel Disease
IPDB	ICES Physician Database
iPHIS	Integrated Public Health Information System

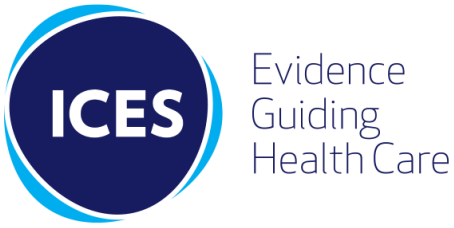
Data	Description
LHIN	Local Health Integration Network
LIDS	Landed Immigrant Data System
LOC	Levels of Care
MIS	Management Information System
MOHLTC	Ministry of Health and Long-Term Care
MomBaby	Mother-baby Linked Database
MRN	Medical Record Number
NCIC	National Cancer Institute of Canada
NDFP	New Drug Funding Program
NOAC	New Oral Anticoagulant
NPHS	National Population Health Survey
OACCAC	Ontario Association of Community Care Access Centres
OBSP	Ontario Breast Screening Program
OCCI	Ontario Case Costing Initiative
OCR	Ontario Cancer Registry Information System
ODB	Ontario Drug Benefit
ODD	Ontario Diabetes Database
OHCAS	Ontario Home Care Administrative System
OHIP	Ontario Health Insurance Plan Claims Database
OHS	Ontario Health Survey
OMHRS	Ontario Mental Health Reporting System
OMID	Ontario Myocardial Infarction Database
OMMMS	Ontario Maternal Multiple Marker Screening
ON-Marg	Ontario Marginalization Index
OPHRDC	Ontario Physician Human Resources Data Centre
ORGD	Ontario Registrar General - Death
ORRS	Ontario Renal Reporting System
OSR	Ontario Stroke Registry
OTR	Ontario Trauma Registry
PCAS	Primary Care Access Survey
PCCF	Postal Code (Macro)
PHO	Public Health Ontario
PHOL	Public Health Ontario Laboratory
Physnet	Ontario Multispecialty Physician Networks
PIBD	Pediatric Inflammatory Bowel Disease Database
POGONIS	Pediatric Oncology Group of Ontario Networked Information System
PSTLyear	Best yearly postal code
RAI-CA	InterRAI Contact Assessment Data
RAI-HC	InterRAI Home Care Data
RCSN	Registry of the Canadian Stroke Network

Data	Description
RPDB	Registered Persons Database
SPIRIT	Stroke Performance Indicators for Reporting, Improvement and Translation
TGLN	Trillium Gift of Life Network
UHN CABG	University Health Network - Coronary Artery Bypass Grafting
UHN PCI	University Health Network - Percutaneous Coronary Intervention

B. Other Terms Used in ICES' Report

Term	Description
CD-Link	Ontario Cancer Data Linkage Project
Coded information	Identifiable information from which direct personal identifiers have been removed or encoded, and which may have an ICES identifier applied using an algorithm that is not known to the user
CEO	Chief Executive Officer
CPO	Chief Privacy Officer
DBA	Database administrator
De-identified information	Information from which any direct personal identifiers have been removed or encoded and other fields have been adjusted so that the data could not, in any reasonably foreseeable circumstance, be used, either alone or in combination with other information, to identify a person
Direct personal identifier	A specific identifier that identifies a person, such as name or personal health number
DP	Data Platform
DPD	Data Partnerships and Development
DQIM	Data Quality and Information Management
DR	Disaster recovery
DSA	Data sharing agreement
EAS	Electronic Article Surveillance
HDD	Hard disk drive
HIC	Health information custodian
ICES	Institute for Clinical Evaluative Sciences
ICES abstractor	A person contracted directly by ICES to abstract information from medical charts or reports
ICES collaborating researcher	A person who is not employed by nor affiliated with ICES but who collaborates on an ICES project
ICES controlled use data	ICES data that is available for ICES projects subject to conditions agreed with the data custodian, typically additional approval or reporting of projects or subject-area restrictions
ICES general use data	ICES data that is available for any ICES project, subject to ICES policies and procedure
ICES data covenantor	A person authorized to access personally identifiable information that contains direct personal identifiers for the purposes of receiving, transferring or destroying data, for the encryption or removal of direct personal identifiers, or for data linkage using direct personal identifiers
ICES data dictionary	The searchable online catalogue of ICES data holdings that describes the attributes and terms and conditions that govern use of ICES data holdings
ICES data holding	An ICES data holding is any ICES general use data or ICES controlled use data
IDPS	Intrusion detection and prevention system
IDS	Intrusion detection system
Identifiable information	Information that identifies a person or for which it is reasonably foreseeable in the circumstances it could be used, either alone or in combination with other information, to identify a person. ICES data that includes direct

Term	Description
	personal identifiers or indirect personal identifiers is identifiable data
Indirect personal identifier	Information that could reasonably be expected to identify an individual through a combination of indirect personal identifiers, such as date of birth or date of admission or service
Individual-level information	Information that relates to a specific individual
IPC	Information and Privacy Commissioner
Knowledge user	A person who can apply the results of an ICES project to make decisions.
LAN	Local area network
NDA	Non-disclosure agreement
PHIPA	Personal Health Information Protection Act
Principal investigator	The individual with principal scientific responsibility for conduct of a project.
PIA	Privacy impact assessment
Privacy impact assessment	A documented assessment designed to identify and manage the elimination or mitigation of privacy risks associated with a process, system or initiative.
PM	Project manager
QA	Quality assurance
Research outputs	Summary information that has been de-identified.
SIEM	System information and event management
Small cell	Summary information, typically in the form of counts, percentages or means, that are based on five or fewer observations
Summary information	Information that has been summarized at a group level, for which, subject to the presence of small cells, the risk of re-identification is very low (e.g., a table of characteristics by age group).
SLA	Service level agreement
SOP	Standard operating procedure


ICES
Evidence
Guiding
Health Care