Exhibit B: PHIPA Review — Privacy, Security, Human Resources and Organizational indicators of the Canadian Institute for Health Information

November 1, 2019 to August 2, 2022

Part 1 — Privacy Indicators

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices	• The dates that the privacy policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC/ON. **Note**: All CIHI privacy documents were reviewed by an external consultant/legal firm to identify any gaps with the stated requirements in the IPC/ON Manual (2021/22). Any gaps identified have been addressed in the relevant privacy documents.	• *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, (*Privacy Policy, 2010*), reviewed October 2020, June 2021, December 2021, and May 2022. • Privacy Policy Procedures reviewed July 2020, October 2020, June 2021, December 2021 and June 2022. • *Privacy and Security Framework, 2010* - reviewed July 2020, September 2020, November 2021 and February 2022. • *Privacy and Security Training Policy* reviewed September 2020 and September 2021. • Procedures related to *Privacy and Security Training Policy* reviewed September 2020, April 2021 and September 2021. • *Privacy Impact Assessment Policy* reviewed January 2020, March 2020 and August 2021, and March 2022 • *Privacy and Security Incident Management Protocol* reviewed December 2019, July 2020, September 2020, October 2021, March 2022 and June 2022.

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		• *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* reviewed June 2020 and August 2021. • *Privacy and Security Risk Management (PSRM) Framework* reviewed January 2020 and April 2021. • *Policy on Privacy and Security Risk Management* reviewed January 2020, and April 2022. • *Privacy and Security Risk Assessment Methodology* reviewed January 2020, August 2021 and January 2022.
	• Whether amendments were made to existing privacy policies and procedures as a result of the review, and if so, a list of the amended privacy policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	• *Privacy Policy, 2010* – **October 2020** - added the mention of list of data holdings of PHI and where to find it, and updated compliance/audit/enforcement section. **June 2021** – s. 34 (Return of Own Data) – Removes "of Health" from the reference to the "Ministry of Health" and adds "or as directed in the data sharing agreement or other legal instrument. **December 2021** - amended compliance/audit/enforcement section. **May 2022** – amended compliance/audit/enforcement section and amended de-identification processes. • ***Privacy Policy Procedures*** **July 2020** – Update s. 10, Replaces Interim Procedures for Access to Sensitive PHI Data Elements. Updates – PHIPA requirements: s. 19.7 (new) – indicates Privacy and Legal Services' (PLS) responsibility for maintenance of a log of approved linkages s. 20.6 (new) – indicates PLS' responsibility for maintenance of a log of approved linkages s. 42.1 – 42.11 (new) – added requirements similar to those for s.41 that indicates the requirement for staff to consult with Privacy and Legal Services (DL-Legal Services) prior to disclosing personal health information and CIHI's responsibilities when processing such disclosures s. 64.1 (revised) – added a reference to the Act and its Regulation.

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		New Requirement - s. 38.10 Indigenous Identifiable data – added requirement for staff to contact the Governance of Indigenous Identifiable Data Committee for disclosures of Indigenous Identifiable data. Updates – Prohibitions on disclosure s. 38.11 (new) – indicates prohibitions on disclosures involving Ontario Insured Persons Registry personal health information to third parties s. 38.12 (new) – indicates prohibitions on disclosures involving Alberta or Saskatchewan Insured Persons Registry personal health information or de-identified data to third parties s. 38.13 (new) – indicates prohibitions on disclosures involving Ontario Patient-Level Physician Billing personal health information to third parties. Removal of Obsolete Forms: Authorization for Release of Own Data Form and Authorization for Release of Third Party Data Form. **October 2020** <u>New – PHIPA requirements:</u> s. 1.7 – indicates PLS maintains log of data protection (sharing) agreements for the collection of personal health information. s. 14.3 – indicates linked records of personal health information must be de-identified or aggregated as soon as practicable s. 38.5 – indicates disclosures of Ontario personal health information or de-identified data must comply with PHIPA and its regulation s. 41.13 – indicates PLS maintains a log of data sharing agreements for disclosure of PHI for non-research purposes. 52.1 and s 56.1- indicates staff must review de-identified and/or aggregate information prior to its disclosure s. 64.1 – 64.7 – indicates the requirements for responding to questions, concerns or complaints, including definitions of “inquiry” and “complaint”. **June 2021** <u>New Procedures:</u> s. 18.2 – indicates staff must contact Quebec CAM for linkages involving Quebec data s. 18.3 – indicates Privacy, Confidentiality and Security (PC&S) Committee approval is not required for linkages *within* sectors, where it involves: o CCRS data and interRAI LTCF data in IRRS o HCRS data and interRAI HC data in IRRS

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		s. 19.1.1 – recognizes the longstanding PC&S Committee approval to link data across the CAD databases (DAD-HMDB and NACRS) for its own purposes, exception where Québec data is involved. s. 19.1.2 – indicates PC&S Committee approval is required for linkages *across* sectors for use by CIHI's for its own purposes, where it involves interRAI HC data and interRAI LTCF data in IRRS, for example. s. 20.1.1 indicates PC&S Committee approval is a requirement to link CAD databases (DAD-HMDB and NACRS) prepared for on or behalf third parties. s. 20.1.2 – adds a new hyperlink to a guidance document for third-party data requests involving the use Québec data in analysis. s. 20.1.3 – indicates PC&S Committee approval is required for linkages *across* sectors performed by CIHI on or on behalf of third parties, where it involves interRAI HC data and interRAI LTCF data in IRRS), for example. s. 34.1 – indicates staff must consult with Legal services in situations of uncertainty <u>Revised Procedures:</u> The following replaces the general de-identification requirements in s. 51.1 and 55.1: s. 51.1 and s. 55.1 – indicates that staff must program area staff must comply with all privacy de-identification requirements, including but not limited to pre-disclosure processing using CIHI-approved software s. 51.2 and s. 55.2 – indicates that If the use of CIHI-approved software for pre-disclosure processing is not possible, then staff must have a pre-disclosure review completed by the Methodology Unit to confirm data is de-identified data. s. 52.1 and s 56.1 - redirects staff to requirements set out in sections 40- 44 with respect to disclosing personal health information. s. 53.2 and 54.2 – adds new hyperlinks to an internal document that consolidates jurisdictional-specific requirements for Data Leaving Canada **December 2021** Gap Analysis: PHIPA Compliance 1.1 *New* – indicates CIHI's commitments around the collection of personal health information

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		1.3 *Amended* – indicates Privacy and Legal Services' role for determining the execution of a Data Sharing Agreement prior to the collection of personal health information 1.3(v) *Amended* - indicates Privacy and Legal Services' responsibility for ensuring the execution of a Data Sharing Agreement prior to the collection of personal health information 1.5(iv) *Amended* – added "collection" 1.6 *Amended* – indicates it is the responsibility of the Director requesting the new collection of data to ensure any conditions or restrictions are satisfied prior to the collection of personal health information 1.8 *Amended* – indicates the Executive Director Chief Privacy Officer & General Counsel it also responsible for maintaining a repository for executed data sharing agreements 3.2 *New* – indicates that CIHI is responsible for personal health information used by employees is in compliance with CIHI's Privacy and Security Framework that is in compliance with legislation, including without limitation PHIPA and its regulation 5.1 *Amended* – added 2 hyperlinks to redirect staff to the appropriate and more detailed requirements associated with use and disclosure of personal health information 7.2 *New* – affirms CIHI permission to use personal health information and de-identified data on a need-to-know basis 10.1 *New* – indicates CIHI's prohibition for staff to access and use personal health information, if other levels of information will serve the identified purpose 10.2 *New* - indicates CIHI's prohibition for staff to access and use more personal health information than is reasonably necessary to meet the identified purpose <u>10.16-10.20.4 (Notification and Termination of Access and Use) – New</u> 10.16 (Off Boarding) 10.17.1 (CIHI Employee Voluntary Departure) 10.17.2 (EPS Contractor/ EPS Vendor Team End of Contract) 10.17.3 (CIHI Employee Involuntary Departure) 10.17.4 (EPS Contractor Early Departure) 10.17.5 (EPS Contractor/ EPS Vendor Team Early Departure)

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		10.18 (Off Boarding - Termination of Access to Systems and Data) 10.19 (Internal Movement – Termination of Access to Systems and Data) 10.20 (Tracking Approved Access and Use of personal health information) 11.1 New – indicates written agreements that CIHI enters into with Third Party Service Providers must contain the relevant language from the Template Agreement for All Third-Party Service Providers 37.1 Amended - redirects staff to requirements set out in sections 40 and 45-47 with respect to disclosing personal health information, and de-identified data, respectively. 41.2 Amended – indicates that for disclosures of personal health information Privacy and Legal Services will review the proposed disclosure to ensure compliance with PHIPA and its regulation. 41.4 Amended – indicates that where personal health information is to be disclosed for purposes other than research (program of work), as described in s. 37(a) and (b), CIHI must enter into a data-sharing agreement 41.9(iv) Amended – indicates that Privacy and Legal Services retains documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research. 41.14 New – indicates that Privacy and Legal Services is responsible for tracking dates/ deadlines to ensure the secure return or destruction of personal health information disclosed under a Research Agreement. 41.15 New – indicates that where the secure return or destruction of personal health information does not occur within the required timeframe, Privacy and Legal Services initiates an escalation process. 42.1 Amended – indicates that prior to disclosing personal health information, staff's consultation with Privacy and Legal Services includes providing the following documentation: • request in writing; • description of the data requested and the intended purpose(s); and • an explanation as to why other information will not serve the identified purpose of the disclosure, and confirmation that no

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		more personal health information is being requested than is reasonably necessary. 42.2 Amended – indicates that Privacy and Legal Services will review the proposed disclosure to ensure there is lawful authority and compliance with PHIPA and its regulation. 42.4 Amended – indicates that where personal health information is to be disclosed for purposes other than research (program of work), as described in s. 37(a) and (b), CIHI must enter into a data-sharing agreement with the third party in accordance with the applicable policies and procedures for the execution of data sharing agreements and the Template Data Sharing Agreement for the Disclosure of Personal Health Information for Non-Research Purposes. 42.5 Amended – indicates that where personal health information is to be disclosed to a third party for research purposes, namely in the circumstances described at s. 37(c) and (d) of this Policy, recipients must enter into a data-sharing agreement in accordance with the Template Data Sharing Agreement. 42.8(iv) Amended – indicates that Privacy and Legal Services retains documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research 42.12 New - indicates that Privacy and Legal Services is responsible for tracking dates/ deadlines to ensure the secure return or destruction of personal health information disclosed under a DSA/ Research Agreement within a reasonable period following the retention period stated in the Agreement or date of termination of the Agreement. 42.13 New – indicates that where the secure return or destruction of personal health information does not occur within the timeframe determined under s.41.14, an escalation process is followed. 48.1 New – indicates that for disclosures of aggregate or de-identified record-level data, staff are to reference, Data Disclosure to Third-Party Data Requestors via CIHI Data Request Program. 48.2 New – indicates that prior to disclosing de-identified data staff must review the information to be disclosed to ensure the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		information could be utilized, either alone or with other information, to identify an individual. 48.3 Amended -indicates that in cases where de-identified data is to be disclosed to a third party for purposes other than research (program of work), CIHI must enter into a data-sharing agreement which prohibits the use of de-identified information, either alone or with other information, to identify an individual. 48.3(iii) Amended – qualifies that disclosures of de-identified data under an agreement are for "[…] purposes other than research […]" 48.6 Amended – indicates where disclosures of de-identified data are for "research" purposes via CIHI's Data Request Program, there is a prohibition for the third party to use of de-identified information, either alone or with other information, to identify an individual—this prohibition is included in CIHI's Third Party Record-Level Data Request Form and Non-Disclosure /Confidentiality Agreement, or another legally binding instrument. 64.8 New – indicates that the results of any investigation of a privacy complaint, including recommendations and the status of the implementation of the recommendations, must be reported to President and CEO. 65.1 New- indicates that on CIHI's website, individuals are advises that they may make a complaint regarding compliance with PHIPA and its regulation to the Information and Privacy Commissioner of Ontario. CIHI provides the mailing address and contact information for the Information and Privacy Commissioner of Ontario. 41.3 Update - Amended – removes New Brunswick Ministry's approval for disclosure of PHI – a new requirement outlined in the DSA. **June 2022 -** 3.1 New, 10.4 New, 10.8 Amended definition of General Use Data files to risk-reduced PHI, 10.9-10 & 10.13 Clarified permission level, 10.14 Added approval by InfoSec, 10.18.1.3 New, 10.18 Updated manager's checklist to offboarding checklist and added CIHI Property definition, 17.1 Amended to indicate Secure Storage and Destruction Standards, 19.1.1 amended to give approval of data linkages for CAD to all departments, 41-43 added titles and amended to comply with IPC/ON requirements, 48.2 amended DE-ID requirements, 48.8-48.9 Amended, 51 added DE-ID committee, 53 Amended to

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		include data request program and removed extended retention, 54 Amended to included data request program, removed internal approval, verification and extended retention sections as it is embedded in CIHInow, removed PLS Destruction Documentation section as it is repetitive, removed Quick Links section. • *Privacy and Security Framework, 2010* – **July 2020** - in section 2a updated contact for SMC, in 2b clarified responsibility for communication of privacy and security policies to staff/public/stakeholders. **September 2020** - in section 2b added contact information for CPO for complaint section, added description of CIHI's status as a prescribed entity, updated section 5 compliance section, and expanded description on openness, transparency and accessibility resulting from IPC/ON review. **November 2021** – updated section 2b to include reference to minimum content in brochures, added mailing address reference, and in section 5 updated compliance section. **February 2022** – updated reporting structure in section 2b, added IPC's role in reviewing/approving polices, in section 4a added communication responsibility for CPO and CISO, in section 5 added notification of breach requirement, and in section 5a elaborated information on the Privacy Audit Program. • *Privacy and Security Training Policy* – **September 2020** - Mandatory privacy and security onboarding training (generic term) replaces CIHI Privacy and Security Core Learning Series; addition of section on privacy and security awareness resulting from IPC/ON review. **September 2021** – In section 4 elaborated on mandatory ongoing training, added section 5 on requirements for annual renewal of CIHI agreement, updated section 15 regarding compliance, audit and enforcement. • Procedures for the *Privacy and Security Training Policy* – **September 2020** - Minor corrections to language and review date aligned to associated policy. **April 2021** – added related policy. **September 2021** – updated wording in section 2,

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		updated section 5 tracking attendance, and CPO is now approval authority for procedures. • *Privacy Impact Assessment Policy* – **January 2020** - Policy updated to include reference to CIHI's Privacy and Security Risk Management Policy; requirement for annual review of PIAs removed and requirements for update of PIAs expanded to include discrepancies between existing PIAs and actual processes or practices. **March 2020** - Policy further revised to identify the Director of the business area as the owner of the PIA. **August 2021** - Changes resulting from IPC/ON review to include new section on Data Management Plan and requirement for an annual review of PIAs by the responsible Directors. **March 2022** – in section 2 updated PHI requirements, in section 7 updated data management plan requirements, and added notification of breach requirement. • *Privacy and Security Incident Management Protocol* – **December 2019** – Chief Information Officer and Vice President, Corporate Services to be notified of any privacy or security breaches; Vice President, Corporate Services to be notified of any incident that may involve a significant business disruption; addition of an appendix on CIHI's breach notification duties. **July 2020** - Protocol amended to refer to both privacy and security breaches. Responsibility for maintaining a log of privacy and security breaches added. **September 2020** - Definition of "incident" expanded to include a suspected privacy or security breach; amended to include reporting of any privacy or security breach to CIHI's Board of Directors. **March 2022** - Updates to meet requirements from IPC/ON: elaborated on containment measures, added manner of notification of privacy or security breach, added the responsibility of the IRT, added responsibility of CEO in the case of PHI from Ontario, added that results of recommendations must be reported to the BoD, added responsibility of addressing the recommendations, elaborated

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		role of CISO/CPO to identify opportunities for training/awareness, updated compliance section. **June 2022 -** Added a bullet in s. 2.2, updated breach definition in s. 3.1, and amended s 6.1.1. • *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* – **June 2020** Added that PHI, Health Workforce Personal Information (HWPI) and De-ID Data shall not be accessed outside of Canada. **August 2021** – updated confidential information definition, removed need for PSRM assessment exception for data to be stored on mobile devices, clarified conditions on retention of PHI on mobile devices, added remote access section, and updated the compliance/audit/enforcement section. • *Privacy and Security Risk Management (PSRM) Framework*- **January 2020** – revised authority from SMC to EC. **April 2021** – no updates. • *Policy on Privacy and Security Risk Management* – **January 2020** - Revised roles and responsibilities: EC responsibility for risk acceptance. **April 2022** – no updates. • Privacy and Security Risk Assessment Methodology – **January 2020** - Risk acceptance authority changed from SMC to EC. **August 2021** – added in section 2.1 that risks identified must be documented following PSRM review. Added section 2.2.4 regarding risk assessment documentation. **January 2022** – Added section 2.5 to include requirements for documentation.

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)	• Whether new privacy policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	• **Privacy Audit Policy** (as per recommendation) The purpose of this policy is to set out the requirements of privacy audits conducted by CIHI. • **Policy for Maintaining and Reviewing a Consolidated Corporate Log of Recommendations and Action Plans** (to meet requirements of Part 4, Section 6 of the Manual). The purpose of this policy is to describe the way CIHI will maintain a consolidated and centralized log of all recommendations and subsequent action plans arising from internal and external audits and reviews (e.g., access management audits, internal audits, privacy impact assessments, privacy audits, security audits, and the investigation of privacy breaches, privacy complaints and security breaches). • **Policy on the Execution of Confidentiality Agreements** (to meet requirements of Part 3, Section 5 of the Manual). The purpose of this Policy is to identify the circumstances requiring CIHI staff to execute a Confidentiality Agreement.

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)	• The date that each amended and newly developed privacy policy and procedure was communicated to agents and, for each amended and newly developed privacy policy and procedure communicated to agents, the nature of the communication.	CIHI communicates material changes to all privacy policies, standards and procedures to those staff that are impacted by the change. Communication mechanisms include CIHI's intranet (CIHIghway), Small Talks, targeted presentations and the like. To date, the following communications have been delivered: • *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*, (*Privacy Policy, 2010*), posted on www.cihi.ca October 2020, June 2021, December 2021 and July 2022. • Privacy Policy and Procedures posted on CIHIghway July 2020, October 2020, June 2021, December 2021 and July 2022. • *Privacy and Security Framework, 2010* – posted on CIHIghway and www.cihi.ca August 2020, October 2020, November 2021 and March 2022. • *Privacy and Security Training Policy* posted on CIHIghway and www.cihi.ca September 2020 and September 2021. • Procedures related to *Privacy and Security Training Policy* posted on CIHIghway September 2020, April 2021 and September 2021. • *Privacy Impact Assessment Policy* posted on CIHIghway and www.cihi.ca January 2020, March 2020 and August 2021, and March 2022. • *Privacy and Security Incident Management Protocol* posted on CIHIghway and www.cihi.ca December 2019, July 2020, September 2020, March 2022 and July 2022. • *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media* posted on CIHIghway and www.cihi.ca June 2020 and August 2021. • *Privacy and Security Risk Management (PSRM) Framework* posted on CIHIghway and www.cihi.ca January 2020

Categories	Privacy Indicators	CIHI Indicators
General Privacy Policies, Procedures and Practices (continued)		• *Policy on Privacy and Security Risk Management* posted on CIHIghway and www.cihi.ca January 2020 and July 2022. • *Privacy and Security Risk Assessment Methodology* posted on CIHIghway January 2020, August 2021 and March 2022. • Privacy Audit Policy posted on CIHIghway and www.cihi.ca January 2022 and November 2022. • Policy for Maintaining and Reviewing a Consolidated Corporate Log of Recommendations and Action Plans posted on CIHIghway August 2021. • Policy on the Execution of Confidentiality Agreements posted on CIHIghway September 2021.
	• Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	• CIHI's *Privacy Policy, 2010* and the *Privacy and Security Framework, 2010* posted on CIHI's external website (www.cihi.ca) • CIHI's Privacy Audit Policy, *Privacy and Security Incident Management Protocol*, *Privacy Impact Assessment Policy*, *Privacy and Security Training Policy*, *Policy on the Security of Confidential Information and Use of Mobile Devices / Removable Media*, *Privacy and Security Risk Management (PSRM) Framework*, and *Policy on Privacy and Security Risk Management* posted on CIHI's external website.

Categories	Privacy Indicators	CIHI Indicators
Collection	• The number of data holdings containing personal health information maintained by the prescribed person or prescribed entity.	• CIHI has 20 data holdings containing personal health information
	• The number of statements of purpose developed for data holdings containing personal health information.	• 2 new statements of purpose were developed during the current reporting period. • A new PIA which will include a statement of purpose for Primary Health Care will be completed in 2022-2023. • Statements of purpose for the remaining 17 data holdings which includes HMHDB are found in the relevant Privacy Impact Assessment
	• The number and a list of the statements of purpose for data holdings containing personal health information that were reviewed since the prior review by the IPC/ON.	• 18 statements of purpose • See Appendix C - Annual Review/5 Year-scheduled Review of PIA and Statement of Purpose where the data holdings whose statements of purpose were reviewed since November 1, 2019
	• Whether amendments were made to existing statements of purpose for data holdings containing personal health information as a result of the review, and if so, a list of the amended statements of purpose and, for each statement of purpose amended, a brief description of the amendments made.	• None
Use	• The number of agents granted approval to access and use personal health information for purposes other than research.	• As of August 2, 2022, 345 agents have approval to access and use personal health information at CIHI.
	• The number of requests received for the use of personal health information for research since the prior review by the Information and Privacy Commissioner of Ontario.	• None. CIHI does not use personal health information for research purposes.
	• The number of requests for the use of personal health information for research purposes that were granted and that were denied since the prior review by the IPC/ON.	• None. CIHI does not use personal health information for research purposes.

Categories	Privacy Indicators	CIHI Indicators
Disclosure	• The number of requests received for the disclosure of personal health information for purposes other than research since the prior review by the IPC/ON.	• None
	• The number of requests for the disclosure of personal health information for purposes other than research that were granted and that were denied since the prior review by the IPC/ON.	• None
	• The number of requests received for the disclosure of personal health information for research purposes since the prior review by the IPC/ON.	• Two • 1 consent (received September 2021) • 1 section 44 (received October 2020)
	• The number of requests for the disclosure of personal health information for research purposes that were granted and that were denied since the prior review by the IPC/ON.	• One granted (section 44) • One currently under review (consent)
	• The number of Research Agreements executed with researchers to whom personal health information was disclosed since the prior review by the IPC/ON.	• Three Research Agreements executed • consent ○ (request received December 2015 during prior reporting period and Research Agreement signed May 2022) ○ (request received August 2019 during prior reporting period and Research Agreement signed May 2022) • 1 section 44 • (request received October 2020 during current reporting period and Research Agreement signed April 2022)
	• The number of requests received for the disclosure of de-identified and/or aggregate information for both research and other purposes since the prior review by the IPC/ON.	• 2019-20: (Q3 – Q4) 178 • 2020-2021: (Q1 – Q4) 365 • 2021-2022: (Q1 – Q4) 313 • 2022-2023: (Q1 – August 2) 87

Categories	Privacy Indicators	CIHI Indicators
Disclosure (continued)	• The 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 the prior review by the IPC/ON.	• 2019-20: (Q3 – Q4) 178 • 2020-2021: (Q1 – Q4) 365 • 2021-2022: (Q1 – Q4) 313 • 2022-2023: (Q1 – August 2) 87
Data Sharing Agreements	• The number of Data Sharing Agreements executed for the collection of personal health information by the prescribed person or prescribed entity since the prior review by the IPC/ON.	• Three
	• The number of Data Sharing Agreements executed for the disclosure of personal health information by the prescribed person or prescribed entity since the prior review by the IPC/ON.	• None
Agreements with Third Party Service Providers	• The number of agreements executed with third party service providers with access to personal health information since the prior review by the IPC/ON.	• 140[i]
Data Linkage	• The number and a list of data linkages approved since the prior review by the IPC/ON.	• 74 linkages of PHI • See Appendix A - Approved Data Linkages

[i] Third-party service providers who need access to CIHI systems and/or data in order to provide the contracted service are required to sign an agreement that is compliant with PHIPA.

Categories	Privacy Indicators	CIHI Indicators
Privacy Impact Assessments	• The number and a list of privacy impact assessments completed since the prior review by the IPC/ON and for each privacy impact assessment: – The data holding, information system, technology or program, – The date of completion of the privacy impact assessment, – A brief description of each recommendation, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	• Since November 1, 2019, 2 **new** Privacy Impact Assessments have been completed: o interRAI Reporting System (IRRS), completed August 2021 o Insured Persons Repository (IPR), completed April 2022 • No recommendations were identified (see Appendix D - CIHI'S Privacy Impact Assessment Program – Summary of Recommendations)
	• The number and a list of privacy impact assessments undertaken but not completed since the prior review by the IPC/ON and the proposed date of completion.	• None
	• The number and a list of privacy impact assessments that were not undertaken but for which privacy impact assessments will be completed and the proposed date of completion.	• 1 – Primary Health Care (scheduled for completion by the end of fiscal 2022/23)
	• The number of determinations made since the prior review by the IPC/ON that a privacy impact assessment is not required and, for each determination, the data holding, information system, technology or program at issue and a brief description of the reasons for the determination.	• A Data Management Plan has been completed for Primary Health Care Data (collection approved May 2020). CIHI is collecting PHC Electronic Medical Record (EMR) data from selected PHC organizations in Ontario, in support of CIHI's mandate, for purposes of evaluating the data. Note: as of July 2022, a decision has been taken to proceed with a PIA.
	• The number and a list of privacy impact assessments reviewed since the prior review by the IPC/ON and a brief description of any amendments made.	• Since November 1, 2019, 15 privacy impact assessments have been reviewed; 2 are currently in progress and 1 to be completed. • See Appendix C-1 - Review of PIAs Since Prior Review by the IPC/ON

Categories	Privacy Indicators	CIHI Indicators
Privacy Audit Program	• The dates of audits of agents granted approval to access and use personal health information since the prior review by the IPC/ON and for each audit conducted: – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	• See Part 2, Security Audit Program – Yearly Internal Access Audit. This is an entry on the "CIHI's Security Audit Program" table found in Appendix G • See Appendix E - CIHI's Privacy Audit Program
	• The number and a list of all other privacy audits completed since the prior review by the IPC/ON and for each audit: – A description of the nature and type of audit conducted, – The date of completion of the audit, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	• Since November 1, 2019, one audit carried out in previous reporting periods was completed (i.e., recommendations addressed). In addition, CIHI has two privacy audits in progress in the current reporting period. • See Appendix E - CIHI's Privacy Audit Program • See Appendix F – IPC's 3-Year Statutory Review

Categories	Privacy Indicators	CIHI Indicators
Privacy Breaches	• The number of notifications of privacy breaches or suspected privacy breaches received by the prescribed person or prescribed entity since the prior review by the IPC/ON.	• Ontario - None • All other jurisdictions – none
	• With respect to each privacy breach or suspected privacy breach: – The date that the notification was received, – The extent of the privacy breach or suspected privacy breach, – Whether it was internal or external, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced, – The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	• N/A

Categories	Privacy Indicators	CIHI Indicators
Privacy Complaints	• The number of privacy complaints received since the prior review by the IPC/ON.	• Ontario – None • All other jurisdictions – None
	• Of the privacy complaints received, the number of privacy complaints investigated since the prior review by the IPC/ON and with respect to each privacy complaint investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, – The date that the investigation was commenced, – The date of the letter to the individual who made the privacy complaint in relation to the commencement of the investigation, – The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, – The manner in which each recommendation was addressed or is proposed to be addressed, and – The date of the letter to the individual who made the privacy complaint describing the nature and findings of the investigation and the measures taken in response to the complaint.	• N/A
	• Of the privacy complaints received, the number of privacy complaints not investigated since the prior review by the IPC/ON and with respect to each privacy complaint not investigated: – The date that the privacy complaint was received, – The nature of the privacy complaint, and – The date of the letter to the individual who made the privacy complaint and a brief description of the content of the letter.	• N/A

Part 2 — Security Indicators

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices	• The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC/ON.	• *Information Security Policy*, reviewed October 2020 and August 2021 • *Acceptable Use of Information Systems Policy*, reviewed December 2020, February, November and December 2021. • *Secure Destruction Policy,* reviewed April 2020 and June 2021. • *Security and Access Policy*, reviewed July 2020, August 2021 and June 2022. • *Security and Access Procedures*, reviewed July 2020 and June 2022 • *Privacy and Security Incident Management Protocol*, see General Privacy Policies, Procedures and Practices above • *Secure Destruction Standard,* reviewed March and December 2020, January and August 2021. • *Third Party Technical Information Disclosure Standard*, reviewed October 2020, March and November 2021. • *COTS Product Technical Requirements Standard,* reviewed July 2022 • *Health Data Collection Standard,* reviewed February 2020, February 2021 and April 2022. • *Secure Information Storage Standard,* reviewed October 2020, September 2021 and February 2022. • *Secure Information Transfer Standard,* reviewed October 2020, August 2021 and February 2022. • *Safe Internet Practices and Email Etiquette Guidelines,* reviewed January and September 2020, February 2021 and May 31, 2022.

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)	• The dates that the security policies and procedures were reviewed by the prescribed person or prescribed entity since the prior review of the IPC/ON. (continued)	• *FAQ – Acceptable Use Policy*, reviewed June 2022 • *Database Access Standard*, reviewed June 2022. • *File Encryption Procedures*, reviewed July 2020, April and October 2021. • *Cloud Service Privacy and Security Assessment Guideline,* reviewed June 2022. • *Policy on the Maintenance of System Control and Audit Logs*, reviewed February 2020, February and August 2021. • *Use of Cloud Services Policy*, reviewed June 2022. • *Respect of Third Party Software Licence Agreements,* reviewed October 2020 and October 2021. • *ISMS Audit Manual,* reviewed April and June 2020, September 2020, July 2021 • *ISMS Risk Management Manual*, reviewed July 2020, March 2021, May 2022 • *ISMS Supplier Management Framework*, reviewed March 2020, July 2020 • *ISMS Infrastructure Security Standard,* reviewed April 2020, April 2021, April 2022 • *ISMS Manual*, reviewed July 2020, July 2021 • Password Management Guidelines, reviewed June and September 2020, July 2021 and May 2022. • *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media, reviewed June 2020 and Aug 2021.*

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)	• Whether amendments were made to existing security policies and procedures as a result of the review and, if so, a list of the amended security policies and procedures and, for each policy and procedure amended, a brief description of the amendments made.	*Information Security Policy* minor revisions and updated compliance section; policy updated to address all requirements of the IPC/ON. *Acceptable Use of Information Systems Policy*, the following terms were added: social media policy link, bullet under general requirements and use of mobile devices and paragraphs on email data breach notification services and printing from home. Updated the ISO footnote and the definition of employees to staff and compliance section. *Secure Destruction Policy*, minor edits and added requirement for electronic secure destruction in the Cloud; updated policy to address all requirements of the IPC/ON. *Security and Access Policy*: July 2020 - added new section for compliance and unreturned security access cards and expanded on the onboarding process; July 2021 - policy updated to address all requirements of the IPC/ON Manual; added a note for all staff and contractors to obey signage in secure spaces as per ISO certification requirement; June 2022 – Updated approval authority to Executive Committee and policy owner to VP/Corporate Services, removed manager responsibilities in section 1.3 and replaced with Corporate Administration department. *Security Access Procedures*: July 2020 - Updates to align with IPC/ON Manual; added section for access to restricted areas; June 2022 - update to Terminated Security Access Cards process; update to Temporary and Contractor cards return process; Added new section on Individuals Attending a CIHI Office. *FAQ Acceptable Use Policy*, no revision history documented since it is a supporting document and not a formal document, last documented review June 2022 *Database Access Standard*, minor revision to update the Compliance section.

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)		*File Encryption Procedures*, Added 7 Zip and WinRar methods of encryption; updated compliance section. *Cloud Service Privacy and Security Assessment Guidelines*, updated to introduce the participation of the CBO (Cloud Business Office) in the process. *Policy on the Maintenance of System Control and Audit Logs*, updated branch name and PHI definition; added more information about retention of audit logs; minor updates and added personal information definition; policy updated to address all requirements of the IPC/ON. *Use of Cloud Services Policy,* revision to update to CIHI's Cloud Computing environment and introduce the role of the Cloud Business Office. *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media,* added PHI, HWPI and De-ID Data shall not be accessed outside of Canada; policy updated to address all requirements of the IPC/ON. *Respect of Third Party Software Licence Agreements,* changed definition of employee; updated compliance section and minor revisions; added language around open source software and compliance with OSS. *Secure Destruction Standard*, added standards for secure destruction in AWS Environments; standard updated to meet the requirements from the IPC/ON. *Third-Party Technical Information Disclosure Standard*, updated compliance section and added information on sharing SAS code.

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)		*Secure Information Transfer Standard*, removed the technical information definition, the cover letter text and double wrapped enveloped; modified the compliance section and updated all the requirements of the IPC/ON. *COTS Product Technical Requirements Standard*, minor editorial changes. *Health Data Collection Standard*, the following terms were updated: branch title, approval authority and Consultation Authorities, the email address in the Standard section and updated the compliance section. Also added Personal Information definition, removed double wrapping envelope and suggested text for using a cover letter under Courier section. *Secure Information Storage Standard*, Updated the compliance section and all requirements of the IPC/ON. *Safe Internet Practices and Email Practices Guideline,* moderate revisions to guidelines while travelling, reviewed and added items 1, 2, 3 to general guidelines, minor edits to wording and updated document links. Password Management Guidelines, added compliance, audit and enforcement section; updated guidelines to address all requirements of the IPC/ON; minor revision to change the document title. *ISMS Audit Manual,* minor clarification and revision, annual review. *ISMS Risk Management Manual,* minor revisions. *ISMS Infrastructure Security Standard,* minor revisions. *ISMS Manual*, no updates noted. *ISMS Supplier Management* Framework, Initial draft, consolidate and include input from PLS, minor revisions from Procurement

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)	• Whether new security policies and procedures were developed and implemented as a result of the review, and if so, a brief description of each of the policies and procedures developed and implemented.	None
	• The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication.	CIHI communicates material changes to all security policies, standards and procedures directly to those staff that are impacted by the change. Communication mechanisms include CIHI's intranet (CIHIghway). To date, the following communications have been delivered: • *Information Security Policy* – Revised Policy posted on CIHIghway October 2020 and August 2021. • *Acceptable Use of Information Systems Policy* – Revised Policy posted on CIHIghway December 2020, February, November and December 2021 • *Database Access Standard* – Revised Standard posted on CIHIghway June 2022. • *File Encryption Procedures* – Revised Procedures posted on CIHIghway July 2020, April and October 2021. • *Cloud Service Privacy and Security Assessment Guideline* – Revised Guideline posted on CIHIghway June 2022. • *Policy on the Maintenance of System Control and Audit Logs* – Revised Policy posted on CIHIghway February 2020, February and August 2021 • *Use of Cloud Services Policy,* Revised Policy posted on CIHIghway June 2022. • *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* – Revised Policy on CIHIghway June 2020 and Aug 2021. • *Respect of Third-Party Software License Agreements,* Revised Policy posted on CIHIghway October 2020 and October 2021.

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)	• The dates that each amended and newly developed security policy and procedure was communicated to agents and, for each amended and newly developed security policy and procedure communicated to agents, the nature of the communication. (continued)	• *COTS Product Technical Requirements Standard* – Revised Standard to be posted on CIHIghway in August 2022 • *Health Data Collection Standard* – Revised Standard posted on CIHIghway February 2020, February 2021 and April 2022. • *Safe Internet Practices and Email Etiquette Guidelines* – Revised Guidelines posted on CIHIghway January and September 2020, February 2021 and May 2022. • *FAQ – Acceptable Use Policy* – Revised supporting document posted on CIHIghway June 2022. • *Secure Destruction Policy* – Revised Policy posted on CIHIghway April 2020 and June 2021. • *Secure Destruction Standard* – Revised Standard posted on CIHIghway March and December 2020, January and August 2021. • *Secure Information Storage Standard* – Revised Standard posted on CIHIghway October 2020, September 2021 and February 2022 • *Secure Information Transfer Standard* – Revised Standard posted on CIHIghway October 2020, August 2021 and February 2022. • *Security and Access Policy* – Revised Policy posted on CIHIghway July 2020, August 2021 and July 2022 • *Security and Access Procedures* – Revised Procedures posted on CIHIghway July 2020 and July 2022 • *Third-Party Technical Information Disclosure Standard* – Revised Standard posted on CIHIghway October 2020, March and November 2021.

Categories	Security Indicators	CIHI Response
General Security Policies, Procedures and Practices (continued)		• Password Management Guidelines posted on CIHIghway June and September 2020, July 2021 and May 2022. • Note: ISMS documents are approved and communicated through the ISMS Steering Committee and the ISMS Working Group
	• Whether communication materials available to the public and other stakeholders were amended as a result of the review, and if so, a brief description of the amendments.	*Information Security Policy*, minor revisions and updated compliance section; updated policy to address all requirements of the IPC/ON *Policy on the Security of Confidential Information and Use of Mobile Devices/Removable Media* added PHI, HWPI and De-ID Data shall not be accessed outside of Canada; policy updated to address all requirements of the IPC/ON; *Health Data Collection Standard* the following terms were updated: branch title, approval authority and Consultation Authorities, the email address in the Standard section and updated the compliance section. Also added Personal Information definition, removed double wrapping envelope and suggested text for using a cover letter under Courier section.
Physical Security	• The dates of audits of agents granted approval to access the premises and locations within the premises where records of personal health information are retained since the prior review by the IPC/ON and for each audit: – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is proposed to be addressed.	• Weekly audit of access cards issued by CIHI Reception • A quarterly audit of cards with access to restricted areas (Finance, HR, IT), confirmed with the respective managers conducted January, April, July and October of each year • Annual physical audit of access cards May 2022 • In lieu of annual physical audit of access cards during office closure caused by the global pandemic (March 2020 - April 2022), all access to the offices was suspended and only given to approved staff. • A list of staff with permanent access during the office closure was held for record. • No recommendations.

Categories	Security Indicators	CIHI Response
Security Audit Program	• The dates of the review of system control and audit logs since the prior review by the IPC/ON and a general description of the findings, if any, arising from the review of system control and audit logs.	• 61155 – IRT investigation held December 2, 2021 • 60167 – IRT investigation held September 29, 2021 • 60129 – IRT investigation held September 28, 2021 • 59601 – IRT investigation held September 7, 2021 • 59526 – IRT investigation held August 13, 2021 • 58552 – IRT investigation held June 2, 2021 • 58050 – IRT investigation held May 7, 2021 **Description of the findings, if any, arising from the review of system control and audit logs**: Log reviews indicated that no unauthorized access to PHI had occurred for any of these incidents.
	• The number and a list of security audits completed since the prior review by the IPC/ON and for each audit: – A description of the nature and type of audit conducted, – The date of completion of the audit, – A brief description of each recommendation made, – The date that each recommendation was addressed or is proposed to be addressed, and – The manner in which each recommendation was addressed or is expected to be addressed.	• See attached Appendix E - CIHI's Privacy Audit Program. • CIHI has completed the following 52 audits: – External Third Party Vulnerability Assessment and Penetration Test (2) – External Third Party Vulnerability Assessment and Penetration Test of 1 Business Application (1) – External Third Party Vulnerability Assessment and Penetration Test of the SAE Environment – Database Security Audit (36) – Yearly Internal Data Access Audit (3) – Local Administrator Audit (4) – ISO/IEC 27001:2013 Surveillance / Re-certification Audit (3) – ISMS Internal Audit (3)

Categories	Security Indicators	CIHI Response
Information Security Breaches	• The number of notifications of information security breaches or suspected information security breaches received by the prescribed person or prescribed entity since the prior review by the IPC/ON.	• Since November 1, 2019, CIHI has logged 1,756 reported privacy and information security incidents, one of which was classified as a security breach. **Notes** (1) Not all incidents necessarily impact data under CIHI's control and may or may not involve Ontario data. (2) Information security incidents include such circumstances as computer viruses, discovered weaknesses in infrastructure, vendor advisories, etc.
	• With respect to each information security breach or suspected information security breach: – The date that the notification was received, – The extent of the information security breach or suspected information security breach, – The nature and extent of personal health information at issue, – The date that senior management was notified, – The containment measures implemented, – The date(s) that the containment measures were implemented, – The date(s) that notification was provided to the health information custodians or any other organizations, – The date that the investigation was commenced, – The date that the investigation was completed, – A brief description of each recommendation made, – The date each recommendation was addressed or is proposed to be addressed, and • The manner in which each recommendation was addressed or is proposed to be addressed.	One security breach – no unauthorized access to personal health information (Report available on request). - The date that the notification was received – December 17, 2021 - The extent of the information security breach or suspected information security breach – There was no CIHI information stolen or disclosed. - The nature and extent of personal health information at issue – N/A - The date that senior management was notified – January 31, 2022 - The containment measures implemented: o the employee was instructed to shut down the computer and stop using it o changed the employee's Office 365 password and removed their computer account from CIHI's Active Directory system o reviewed of Office 365 logs and anti-malware events for both the employee's computer and CIHI user account o employee was instructed to place a note on the laptop warning staff to not turn it on, and to ship it back to CIHI where it will be retained in storage should a forensic investigation be deemed necessary. - The date(s) that the containment measures were implemented – December 17, 2021

Categories	Security Indicators	CIHI Response

Information Security Breaches (continued)		- The date(s) that notification was provided to the health information custodians or any other organizations – N/A
		- The date that the investigation was commenced – December 17, 2021
		- The date that the investigation was completed – December 22, 2021
		- A brief description of each recommendation made:
		  o Create a staff awareness communication to educate staff about this specific method of social engineering and remind them to be diligent against all forms of social engineering
		  o Facilitate a strategic, risk-based analysis and associated recommendations concerning after-hours support for cybersecurity events, including but not limited: to on-call policies, and the use of third-party security monitoring services
		  o Depending on the outcome of Recommendation #2, above, clarify expectations Management and Staff regarding after-hours support for cyber-security events
		- The date each recommendation was addressed or is proposed to be addressed –
		<u>Implementation Timeline:</u>
		- Recommendation #1 – February 2022
		- Recommendation #2 – December 2022
		- Recommendation #3 – December 2022
		
		The manner in which each recommendation was addressed or is proposed to be addressed –
		- Recommendation #1 – Article published on CIHIghway February 7, 2022
		- Recommendation #2 – CIHI will engage 3rd party vendor to use MSSP implementation by Q3 of 2023/24
		- Recommendation #3 - CIHI will engage 3rd party vendor to use MSSP implementation by Q3 of 2023/24

Part 3 — Human Resources Indicators

Categories	Human Resources Indicators	CIHI Response
Privacy and Security Training and Awareness	• The number of agents who have received and who have not received initial privacy orientation since the prior review by the IPC/ON.	• 552 agents (includes third party service providers) have received initial privacy and security orientation training in the review period • 0 agents who began (or re-boarded) an employment, contractual, or other relationship with CIHI between November 1, 2019 – August 2, 2022 but did not receive initial privacy and security orientation on or before August 2, 2022 • Agents returning from an extended leave period of greater than 180 days are required to re-do the privacy orientation training • From November 1, 2019 to August 2, 2022, 59 agents were re-boarded and completed the required mandatory training
	• The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial privacy orientation and the scheduled date of the initial privacy orientation.	• Ongoing process – as per the requirements under CIHI's *Privacy and Security Training Policy*, all new-hires have completed mandatory privacy and security training on their first day of employment or as soon as possible thereafter, but within 15 days of commencement of employment.
	• The number of agents who have attended and who have not attended ongoing privacy training each year since the prior review by IPC/ON.	• 100% completed – mandatory training requirements • January 2020 – 781 agents • January 2021 – 805 agents • January 2022 – 855 agents

Categories	Human Resources Indicators	CIHI Response
Privacy and Security Training and Awareness	• The dates and number of communications to agents by the prescribed person or prescribed entity in relation to privacy since the prior review by the IPC/ON and a brief description of each communication.	• Ongoing Privacy and Security poster campaign “January is Privacy Awareness Month at CIHI” • Ongoing Privacy and Security poster campaign “September is Information Security Awareness Month at CIHI” • On-line mandatory training modules for all new-hires as well as external professional services (EPS) who will have access to CIHI systems and/or data as in order to provide the contracted services. • On-line mandatory training modules for all CIHI agents: 1. January 2020 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents 2. January 2021 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents 3. January 2022 – Privacy Awareness Month Mandatory Training and Confidentiality Agreement Renewal for all agents • January 30, 2020 – Town Hall session regarding Privacy and Security by Design presented to all agents. • March 18, 2020 – email to all agents on Maintaining Privacy and Security While Working from Home • April 8, 2020 – email sent to all agents on important information about privacy and security and the use of personal equipment with CIHI laptops • May 15, 2020 – email to all agents regarding important privacy and security information about MS Teams. • April 12, 2021 – Presentation to ITSPD regarding privacy and security framework. • January 12, 2022 – email to all agents regarding a refresher on working from home.

Categories	Human Resources Indicators	CIHI Response
Privacy and Security Training and Awareness (continued)		• January 17, 2022 – CIHIghway article to all agents on privacy and security requirements when sharing externally with OneDrive. • February 2, 2022 – CIHIghway article to all agents on Homewood Health privacy incident. • March 14, 2022 – email to all agents by the CEO which included an overview on the Privacy Program outlining how excellence in privacy and security is foundational to our culture as a steward of health data. • From April 2021 – June 2022, 31 staff information sessions were delivered on Demonstrable Accountability, focusing on the application of PHIPA to CIH data,
Security Training and Awareness	• The number of agents who have received and who have not received initial security orientation since the prior review by the IPC/ON.	• See Privacy and Security Training and Awareness, above.
	• The date of commencement of the employment, contractual or other relationship for agents that have yet to receive initial security orientation and the scheduled date of the initial security orientation.	• See Privacy and Security Training and Awareness, above.
	• The number of agents who have attended and who have not attended ongoing security training each year since the prior review by the IPC/ON.	• See Privacy and Security Training and Awareness, above.
	• The dates and number of communications to agents by the prescribed person or prescribed entity to agents in relation to information security since the prior review by the IPC/ON.	• Every January and September, CIHI staff receives communication and training as part of Privacy Awareness Month (January) and Information Security Awareness Month (September). • Additionally, regular communication and awareness is offered as required throughout the year. See attached

Categories	Human Resources Indicators	CIHI Response
		InfoSec Staff Awareness, Education and Communication Log found at **Appendix H**.
Confidentiality Agreements	• The number of agents who have executed and who have not executed Confidentiality Agreements each year since the prior review by IPC/ON.	• 552 agents (includes third-party service providers) have executed Confidentiality Agreements in the current reporting period • No agents failed to execute a Confidentiality Agreement in the current reporting period
	• The date of commencement of the employment, contractual or other relationship for agents that have yet to execute the Confidentiality Agreement and the date by which the Confidentiality Agreement must be executed.	• None
Termination or Cessation	• The number of notifications received from agents since the prior review by the IPC/ON related to termination of their employment, contractual or other relationship with the prescribed person or prescribed entity.	• 509 agents (includes third-party service providers)

Part 4 — Organizational Indicators

Categories	Organizational Indicators	CIHI Response

Risk Management	• The dates that the corporate risk register was reviewed by the prescribed person or prescribed entity since the prior review by the IPC/ON.	• The Corporate Risk Register is developed on an annual basis. Action plans for the strategic risks are reviewed and monitored on a quarterly basis.
		• Dates reviewed during the current reporting period are as follows:
		  ○ February 2020
		  ○ February 2021
		  ○ February 2022

	• Whether amendments were made to the corporate risk register as a result of the review, and if so, a brief description of the amendments made.	Privacy and security is a consistent component of the corporate risk register, specifically the susceptibility of a major privacy or security breach. Amendments to the register, if required, are made at the annual review and are based on the environment and emerging issues. Amendments to the register year over year for the reporting period are as follows: **2019-20** • Addressing emerging technology needs • Maintaining focus to achieve the 2016-2021 strategic plan • Developing and maintaining effective stakeholder relationships • Addressing the risk of a major privacy and security breach • Addressing recommendations from the PCHO Review **2020-21** • Addressing current and emerging technology needs • Ensuring CIHI's current and emerging data supply • Ensuring relevancy with stakeholders • Addressing the risk of a major privacy and security breach **2021-22** • Current and emerging technology needs • Current and emerging timely data supply • Demonstrating value to stakeholders

Categories	Organizational Indicators	CIHI Response
Risk Management (continued)		• Susceptibility of a major privacy or security breach • Funding and operational management **2022-23** • Current and emerging technology needs • Current and emerging timely data supply • Demonstrating value to stakeholders • Susceptibility of a major privacy or security breach • Funding and operational management • Workforce uncertainty
Business Continuity and Disaster Recovery	• The dates that the business continuity and disaster recovery plan was tested since the prior review by the IPC/ON. • Whether amendments were made to the business continuity and disaster recovery plan as a result of the testing, and if so, a brief description of the amendments made.	• The BCP was scheduled to be tested in spring 2020, however, due to COVID-19 CIHI took the opportunity to use the global pandemic to "live test" the BCP • Note: Due to COVID-19, the BCP was invoked in March 2020 and successfully supported business functions. • A comprehensive review of the BCP was conducted in the fall of 2021 and VP approved in December 2021. Changes were made to make the plan more actionable during disruptive events. • Changes included adding sections related to the BCM program (DR Framework, BIA results and Crisis Communications Plan (CCP)), review of the BCP plan assumptions, edits to the processes and protocols to reflect recent changes to the ITS Infrastructure services and move to the cloud as well as changes reflecting evolution of how CIHI conducts business – brought on by the pandemic. • The DR Framework, BIA results and Crisis Communications Plan (CCP) were added to the BCP to form a new document called the BCM Program Document.

Categories	Organizational Indicators	CIHI Response
Business Continuity and Disaster Recovery (continued)		• The BCM Program Document was updated in February 2022 to reflect requirements set forth by the IPC/ON • The BCM Program Document is final and was reviewed and approved in July 2022. • Like the BCP, the BCM Program Document will be reviewed on an annual basis • BCM Team wallet cards are reviewed and updated as required • Emergency mass notification system was deemed no longer required as we have sufficient platforms to reach all employees and stakeholders • Annual DR test performed in May 2020, 2021, June 2022 • In 2020, CIHI moved to the Cloud, which has numerous redundancy and resiliency built-in, and meets or exceeds CIHI's DR and availability requirements • The DR Framework was updated in March 2020 to reflect the new cloud-based DR strategy. • DRP updated continuously as changes to technology occur, to ensure that the plan includes most recent procedures. • Disaster recovery external contacts are reviewed and updated yearly as required • All DRP changes are documented in DR Framework in which regular maintenance of the plan as well as participant information is captured throughout the year.

Appendix A — Approved Data Linkages

Linkages for a CIHI Use/Purpose – FY2019/20 (Nov. 1, 2019- March 31, 2020)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
1	2191	Feb 14, 2020	Suitability and utility of the linkage for indication/ confirmation of death and other assessments of data quality	CORR, CCRS, HCRS	Feb. 2023
2	2249	Mar 5, 2020	CJRR annual report	DAD, CJRR, PLPB	March 2023
3	2262	Mar 12, 2020	Drug Use Among Seniors in Canada	NPDUIS, PLPB	March 2023
4	2273	Mar 18, 2020	Choosing Wisely Canada - Knee arthroscopy	DAD, HMDB, NACRS, PLPB	March 2023
5	2314	Mar 24, 2020	Adverse events following the development of COVID-19	DAD, HCRS, CCRS, NACRS	March 2023

Linkages for a CIHI Use/Purpose - FY2020/21 (April 1, 2020- March 31, 2021)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
6	2275	Apr 2, 2020	Shared Health Priorities Caregiver Distress indicator	HCRS, Alberta Client List Assisted Living	April 2023
7	594	Feb. 5, 2021	Unintended Consequences of COVID-19	DAD, HMDB, NACRS, OMHRS	Feb. 2024
8	565	Jan 27, 2021	Data linkage with PLPB and DAD which will be used to support CJRR annual reporting	PLPB, DAD	Jan. 2024
9	547	Jan 26, 2021	Required to test R, Python and SAS Viya capabilities	CAD, OMHRS	Jan. 2024

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
10	424	Dec. 4, 2020	Data linkage to support phase 1 of the Hub Development project with testing the calculation and reporting of the 30-Day Readmissions for Mental Illness indicator	DAD, NACRS, OMHRS	Dec. 2023
11	362	Oct. 15, 2020	Focus on COVID-19 in LTC	DAD, NACRS, CCRS	Oct. 2023
12	200	July 23, 2020	Developing a comparison between estimated full hospital costs and actual full hospital costs by combining the Patient Cost Estimator (PCE) with actual physician costs vs. combining the actual hospital costs with actual physician costs	DAD, CPCD, PLPB	July 2023
13	122	July 7, 2021	Suitability and utility of the linkage for indication/confirmation of death and other assessments of data quality	CORR, IPR	July 2024

Linkages for a CIHI Use/Purpose - FY2021/22 (April 1, 2021- March 31, 2022)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
14	1290	Feb. 17, 2022	One-time linkage of the PLPB repository to NPDUIS, DAD/NACRS to investigate complementary and potentially overlapping data for therapeutic abortions	PLPB, NPDUIS, DAD, NACRS	Feb. 2025
15	1254	March 23, 2022	This new request will link Alliance EMR data to DAD, NACRS, NPDUIS and PLPB on an annual basis, in each of the next 3 years or until the analysis is complete	DAD, NACRS, NPDUIS, PLPB	March 2025
16	1237	Jan. 18, 2022	Data linkage with NPDUIS and CCRS to carry out a methodological investigation to support the planned Drug Use Among Seniors report.	CCRS, NPDUIS	Jan. 2025
17	1051	Oct. 5, 2021	The goal of this product is to present the impact on patient experiences of those who were hospitalized during the COVID-19 pandemic compared with previous years	CPERS, DAD	Oct. 2024
18	983	Aug. 12, 2021	Destination 2021 - enhance the operations and reporting for CIHI's Hip and Knee PROMs and CJRR programs	DAD, HMHDB, NACRS, CPERS, CJRR, PROMs	Aug. 2024

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
19	980	Aug. 13, 2021	Access to palliative care in Canada (2nd Iteration) - IRRS added	DAD, NACRS, CCRS, HCRS, PLPB, NPDUIS, IRRS	Aug. 2024
20	932	July 27, 2021	Choosing Wisely Canada (CWC): "Unnecessary Care in Canada"	DAD, NACRS, PLPB, CCRS, NPDUIS	July 2024
21	905	July 21, 2021	Internal linkage of data sets to support investigative work on constructing an equity stratifier inventory associated with the Insured Persons Repository (IPR)	IPR, CCRS, CJRR, CORR, CPERS, DAD, HMDB, NACR, NPDUIS, NRS, OMHRS, PLPB	July 2024
22	871	June 14, 2021	Advanced Analytics is developing a proof-of-concept multi-state transition model to characterize transition probabilities between acute, post-acute, rehabilitation, mental health, and long-term care settings among home care recipients in Ontario, Canada.	HCRS, DAD, NACRS, CCRS, NRS, OMHRS	June 2024
23	938	Sep. 13, 2021	Ongoing linkage for the Hub system to: calculate mental health and health system indicators; and perform health system performance analysis.	OMHRS, DAD/HMDB, and NACRS	When no longer needed
24	866	June 8, 2021	Determining sufficient levels of de-identification on the linked datasets	CCRS, HCRS, OMHRS, DAD, NACRS, NPDUIS	June 2024
25	851	June 3, 2021	Explore mental health related analyses and the role of virtual care in prescription drug utilization, physician services utilization, and hospital use	PLPB, DAD, HMDB, NACRS, OMHRS, NPDUIS	June 2024
26	701	April 6, 2021	Data linkage to support investigative work on virtual care in Canada.	CORR, DAD, NACRS, NPDUIS, PLPB	April 2024

Linkages for a CIHI Use/Purpose - FY2022/23 (April 1, 2022- August 2, 2022)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
27	1427	May 27, 2022	Linkage of Predictive model repeat hospital mental health	DAD, NACRS, OMHRS, NPDUIS, PLPB, Alliance for Healthier Communities EMR Data	May 2025

Third-Party Requests for Data Linkage - FY2019/20 (Nov. 1, 2019- March 31, 2020)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
28	1992	Nov 6, 2019	Trends and patterns of opioid prescription leading to harms in Canada	DAD, NACRS, NPDUIS	Nov 2022
29	2013	Nov 5, 2019	Comparative Effectiveness and Safety of Biosimilar and Legacy Drugs	NPDUIS, DAD, NACRS	Nov 2022
30	2053	Nov 28, 2019	Health Canada Hip replacement safety study	CJRR, DAD, NACRS	Nov 2022
31	2110	Jan 7, 2020	Update metrics from the 2017 Seniors in Transition report -+ Identifying unique persons entering long-term care	CCRS, DAD, HCRS, OMHRS	Jan 2023
32	2018	Nov 7, 2019	Trends in Hospitalization among People Living with HIV across Canada	DAD, HMDB	Nov 2022
33	2162	Feb 14, 2020	Examining Cardiovascular Care in Canada	DAD, NACRS, NPDUIS	Feb 2023
34	2181	Feb 18, 2020	Drug-initiation-associated hospitalizations for malignant arrhythmias amongst the elderly Canadian population	DAD, NPDUIS	Feb 2023
35	2199	Feb 14, 2020	Severe maternal morbidity and future all-cause hospitalization	DAD	Feb 2023
36	2226	Mar 18, 2020	How Approaches to Care Shape the Pathways of Older Adult Home Care Clients	PLPB, WRHA Clinical Data	Mar 2023

Third-Party Requests for Data Linkage - FY2020/21 (April 1, 2020- March 31, 2021)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
37	643	Feb. 18, 2021	An assessment of COVID-19 transmission mitigation measures implemented to determine the impacted on important hemodialysis-related outcomes in prevalent individuals receiving in-centre hemodialysis (HD) in Canada.	DAD, NACRS, CORR	Feb. 2024
38	532	Feb. 3, 2021	Secular Trends in Hospitalization, Mortality and technique failure in Home versus In-Center Dialysis in Canada	CORR, DAD	Feb. 2024
39	497	Dec. 17, 2020	Assessing Changes in Perinatal Health Associated with the COVID-19 Pandemic Countermeasures	DAD	Dec. 2023
40	363	Oct. 26, 2020	Sequalae of anastomotic leak on oncologic outcomes in colorectal cancer	DAD, NACRS	Oct. 2023
41	276	Sept. 18, 2020	Developing a predictive suicide-attempt risk algorithm for psychiatric inpatients using electronic medical records and machine learning	DAD, NACRS, OMHRS	Sept. 2023
42	251	Sept. 3, 2020	Atrial Fibrillation: National Care Practices and Outcomes	DAD, NACRS	Sept. 2023
43	189	Sept. 23, 2020	Retrospective Database Analysis to Estimate Adherence Rates in PLHIV(Patients living with Human Immunodeficiency Virus) in Canada	NPDUIS	Sept. 2023
44	179	July 16, 2020	Glaucoma and Cataract Study	DAD, NACRS	July 2023
45	112	June 10, 2020	Data linkage to provide Ronald McDonald House Charities (RMHC) with information regarding pediatric inpatient hospitalizations	DAD, NACRS	June 2023
46	111	June 12, 2020	A geospatial evaluation of the incidence and severity of colorectal cancer in Canada	DAD, NACRS	June 2023
47	73	May 25, 2020	Acetaminophen use during Pregnancy	DAD, NPDUIS	May 2023
48	2327	Apr 17, 2020	Hospital Utilization in Patients Before and After Clozapine	DAD, NACRS, NPDUIS	Apr 2023
49	2332	Apr 22, 2020	Cannabis intake and its interaction with marketed health products	DAD, NPDUIS, NACRS	Apr 2023

Third-Party Requests for Data Linkage - FY2021/22 (April 1, 2021- March 31, 2022)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
50	1281	March 7, 2022	A Comprehensive Examination of Cannabis Use in Long-Term Care (Study)	CCRS, NPDUIS	March 2025
51	1276	Feb. 11, 2022	Validating Case Definitions for COVID-19 in Administrative Health Data	DAD, NACRS	Feb. 2025
52	1275	Feb. 3, 2022	The Canadian Alliance for Healthy Heart and Minds Study	DAD, NACRS	Feb. 2025
53	1173	Jan. 24, 2022	Survivorship of Modern Cementless Total Knee Arthroplasty: Analysis from the Canadian Joint Replacement Registry	DAD, NACRS, CJRR	Jan. 2025
54	1172	Jan. 26, 2022	Hip Fracture Outcomes in a Canadian Population	DAD, NACRS, CJRR, PLPB	Jan. 2025
55	1036	Sept. 28, 2021	A study to compare the use of certain medications (Tenecteplase and Alteplase) in treating patients with ischemic stroke	DAD, HMHDB, NACRS	Sept. 2024
56	1033	Oct. 8, 2021	Care of older persons with complex chronic conditions	CCRS, HCRS, OMHRS, DAD, NACRS, NPDUIS, PLPB, IRRS	Oct. 2024
57	985	Aug. 17, 2021	Comparative Effectiveness and Safety of Biosimilar and Legacy Drugs	NPDUIS, DAD, NACRS	Aug. 2024
58	902	June 29, 2021	Treatment of (Overt) Hepatic Encephalopathy (HE) in Cirrhosis	DAD, NACRS, NPDUIS	June 2024
59	855	Aug. 19, 2021	Trajectories of Arthritis Pain in Canadian Home Care Settings: Risk Factors, Serious Adverse Outcomes	DAD, HCRS, CCRS, NACRS, NPDUIS	Aug. 2024
60	834	June 23, 2021	Epidemiology and economic burden of Generalized Pustular Psoriasis (GPP), Palmoplantar Pustolosis (PPP) and Plaque Psoriasis (PP)	DAD, NACRS, NPDUIS	June 2024
61	833	May 18, 2021	Surgery to Improve Upper Limb Function in Cervical-Level Spinal Cord Injury (SCI): the current state in Canada	DAD, NACRS	May 2024
62	832	May 31, 2021	Long term outcomes for critically ill neonates and children in Canada	DAD, HMDB	May 2024

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
63	723	April 26, 2021	Study on children with vaping-related lung injuries and other respiratory ailments	DAD, HMDB	April 2024
64	721	April 14, 2021	Health Disparities in relation to management of Undescended Testis	DAD, NACRS	April 2024
65	842	June 10, 2021	The Vulnerable Newborn Measurement Collaborative Project	DAD	June 2024
66	1132	Dec. 16, 2021	The extent of non-traumatic spinal cord injury/dysfunction in Canada: Part 2	DAD, NRS	Dec. 2024
67	1266	Feb.7, 2022	An analysis of Ontario's bundled care roll-out in total hip and total knee arthroplasty	DAD, NACRS	Feb. 2025

Third-Party Requests for Data Linkage - FY2022/23 (April 1, 2022- August 2, 2022)

No.	DL#	Date Approved	Subject/Project or Study Title	Files Linked	Date of Destruction
68	1414	May 10, 2022	Understanding Changes in Acute Care and Mortality Patterns among Children and Youth with Medical Complexity (CMC) during the COVID-19 pandemic	DAD	May 2025
69	1415	May 12, 2022	The Canadian Partnership Against Cancer is requesting aggregate data to help inform their Board of Directors and Health Canada on progress of the organizational work	DAD, NACRS	May 2025
70	1423	May 19, 2022	National Trauma Outcomes Study	DAD	May 2025
71	1426	May 20, 2022	Population-based study of hypertrophic pyloric stenosis-investigating the season variations and potential environmental contributions in Canada	DAD	May 2025
72	1455	June 1, 2022	Formulary Management in Ulcerative Colitis	DAD, NACRS, NPDUIS	June 2025
73	1503	July 25, 2022	Self-harm hospitalizations in Canada	DAD, NACRS, OMHRS	July 2025
74	1530	July 25, 2022	Opportunistic Salpingectomy in Canada: A detailed population-based retrospective study of uptake, and safety	DAD, NACRS	July 2025

Appendix C — Annual/5 Year-scheduled Review of PIA and Statement of Purpose[ii]

Data Holding / Information System / Technology / Program	PIA / Statement of Purpose Review
Hospital Mental Health Database	Annual Review - Under review on the basis that we may be decommissioning the database 5-Year Scheduled Review – N/A Statement of Purpose – N/A
Home Care Reporting System	Annual Review – N/A 5-Year Scheduled Review - completed June 2022 Statement of Purpose - completed June 2022
Continuing Care Reporting System	Annual Review – N/A 5-Year Scheduled Review - completed June 2022 Statement of Purpose - completed June 2022
Ontario Mental Health Reporting System	Annual Review – N/A 5-Year Scheduled Review - completed July 2022 Statement of Purpose - completed July 2022
National Rehabilitation Reporting System	Annual Review – N/A 5-Year Scheduled Review - completed March 2022 Statement of Purpose - completed March 2022
interRAI Reporting System (IRRS)	**NEW** PIA, signed August 2021 Annual Review – completed February 2022 5-Year Scheduled Review – N/A Statement of Purpose - completed February 2022

[ii] The statement of purpose is set out in the PIA under Principle 2: Identifying purposes for personal health information

Data Holding / Information System / Technology / Program	PIA / Statement of Purpose Review
Population Grouping Methodology (POP Grouper) - formerly PRAG Project	Annual Review – N/A 5-Year Scheduled Review - completed February 2022 Statement of Purpose - completed February 2022
National Prescription Drug Utilization Information System	Annual Review – completed February 2022 5-Year Scheduled Review - renewal in progress FY 2022-23 Statement of Purpose - completed February 2022
Patient-Level Physician Billing Repository	Annual Review – N/A 5-Year Scheduled Review - completed April 2022 Statement of Purpose - completed April 2022
Canadian Patient Cost Database	Annual Review – completed February 2022 5-Year Scheduled Review – N/A Statement of Purpose - completed February 2022
Reabstraction Studies	Annual review - completed February 2022 5-Year Scheduled Review – N/A Statement of Purpose - completed February 2022
Your Health System: Insight	Annual review – completed February 2022 5-Year Scheduled Review – completed December 2021 Statement of Purpose - completed February 2022
Canadian Joint Replacement Registry (CJRR)	Annual review – completed February 2022 5-Year Scheduled Review – completed February 2021 Statement of Purpose - completed February 2022
Canadian Organ Replacement Register (CORR)	Annual review – completed February 2022 5-Year Scheduled Review – to be renewed in FY 2022/23 Statement of Purpose - completed February 2022
Clinical Administrative Database (DAD, HMDB, NACRS)	Annual review – completed February 2022 5-Year Scheduled Review – N/A Statement of Purpose - completed February 2022

Data Holding / Information System / Technology / Program	PIA / Statement of Purpose Review
Trauma Registries	Annual review – completed February 2022 5-Year Scheduled Review – N/A Statement of Purpose - completed February 2022
Canadian Patient Experiences Data Collection and Reporting System	Annual review – completed February 2022 5-Year Scheduled Review – completed October 2020 Statement of Purpose - completed February 2022
Patient Reported Outcome Measures (PROMs)	Annual review – completed February 2022 5-Year Scheduled Review – completed November 2019 Statement of Purpose - completed February 2022
Insured Persons Repository	**NEW** PIA, signed April 2022 Annual review – N/A 5-Year Scheduled Review – N/A Statement of Purpose - completed April 2022
Primary Health Care	**NEW** PIA, to be completed in FY 2022-2023 Annual review – N/A 5-Year Scheduled Review – N/A Statement of Purpose - NEW PIA, to be completed in FY 2022-2023

Appendix C-1 —Review of PIAs Since Prior Review by the IPC/ON

Data Holding / Information System / Technology / Program	Description of Amendments
Hospital Mental Health Database	Under review on the basis that we may be decommissioning the database
Home Care Reporting System	5-Year Scheduled Review - completed June 2022 **Amendments**: The major updates to the document are applying current PIA boilerplate text (e.g. adding content to the "Third-party data requests" section to address the secure access environment (SAE) – and also addressing free-text fields.
Continuing Care Reporting System	5-Year Scheduled Review - completed June 2022 **Amendments**: The major updates to the document are applying current PIA boilerplate text (e.g. adding content to the "Third-party data requests" section to address the secure access environment (SAE) – and also addressing free-text fields.
Ontario Mental Health Reporting System	5-Year Scheduled Review - completed July 2022 **Amendments**: The major updates to the document are applying current PIA boilerplate text (e.g. adding content to the "Third-party data requests" section to address the secure access environment (SAE) – and also addressing free-text fields.
National Rehabilitation Reporting System	5-Year Scheduled Review - completed March 2022 **Amendments**: The major change to this privacy impact assessment (PIA) has been applying the current PIA boilerplate text.
Population Grouping Methodology (POP Grouper) - formerly PRAG Project	5-Year Scheduled Review - completed February 2022 **Amendments**: • The program name has changed from Population Risk Adjustment Grouping (PRAG) to population grouping methodology (POP Grouper) • There are no significant changes to the template text to note. However, please note the following:

Data Holding / Information System / Technology / Program	Description of Amendments
	○ Text has been modified in various sections to reflect the fact the POP Grouper does not collect data, instead utilizing existing internal CIHI sources. ○ Where applicable section 3.7 now references general use data files (i.e., if General Use Data files created and in-use). As POP grouper data is PHI and does not have a General Use Data file, the text in this section has been modified to reflect this reality. • There are no substantive changes to the POP Grouper activities or technology since the original PIA in 2015, from a privacy/security perspective— the POP Grouper uses CIHI data, including personal health information, only for internal CIHI purposes, specifically maintenance and enhancement of the POP Grouper. • In the original 2015 PIA there were no privacy/security risks flagged; the 2021 renewal PIA has not identified any new privacy/security risks.
National Prescription Drug Utilization Information System	5-Year Scheduled Review – in process
Patient-Level Physician Billing Repository	5-Year Scheduled Review - completed April 2022 **Amendments**: The data management approach for PLPB, is the basis for the management of the Insured Persons Repository (IPR), with both holdings under the responsibility of the Physician Team. Not surprisingly, the PIAs for both IPR and PLPB are very similar. • There are no significant changes to the template text to note However, where applicable section 3.7 now references general use data files (i.e., if General Use Data files created and in-use). • In summary: • There are no significant changes to the PLPB Repository activities or technology since the original PIA in 2015, other than the following: ○ Since the 2015 PIA, PLPB collection has expanded to include additional provinces (BC, MB and NS)

Data Holding / Information System / Technology / Program	Description of Amendments
	○ Data holding operations have matured, such that PLPB data are now accessible via CIHI's third-party data request program, in accordance with CIHI's Privacy Policy, 2010 (subject to one DSA-related restriction i.e., CIHI must not disclose Ontario PLPB PHI to third parties). Template text addressing this change appears in section 3.7. • In the original 2015 PIA there were no privacy/security risks flagged; This renewal PIA has not identified any new privacy/security risks.
Canadian Patient Cost Database	Annual Review – completed February 2022 **Amendments**: none
Reabstraction Studies	Annual review - completed February 2022 **Amendments**: none
Your Health System: Insight	5-Year Scheduled Review – completed December 2021 **Amendments**: The major changes to the PIA include: distinguishing between data providers and non-data providers; the inclusion of MAID and ToP data and the safeguards implemented to protect them; more clearly describing YHS: Insight data, and data linkage; the general access role that excludes access to Quebec data; updated figures in tables; and current PIA boilerplate text, as of August 16, 2021.
Canadian Joint Replacement Registry (CJRR)	5-Year Scheduled Review – completed February 2021 **Amendments**: The major changes to the privacy impact assessment (PIA) include: • CJRR web-based tool was decommissioned as of April 2018 • CJRR data submissions now accepted through DAD core abstract as of April 2018 Updated data submission flow as a result of changes noted above; and current PIA boilerplate text, as of December 2019. Annual review - completed February 2022 **Amendments**: none

Data Holding / Information System / Technology / Program	Description of Amendments
Canadian Organ Replacement Register (CORR)	Annual review – completed February 2022 **Amendments**: none
Clinical Administrative Database (DAD, HMDB, NACRS)	Annual review – completed February 2022 **Amendments**: none
Trauma Registries	Annual review – completed February 2022 **Amendments**: none
Canadian Patient Experiences Data Collection and Reporting System	Annual review – completed February 2022 **Amendments:** none 5-Year Scheduled Review – completed October 2020 **Amendments**: • Updated to reflect the Canadian Patient Experiences Reporting System (CPERS) has been open for data collection as of April 2015; • Updated to include the CPES: Comparative Results Tool, which was launched in August 2017 and available for participating jurisdictions; • Added Special Projects fields to Quick Facts (i.e. to align with the Clinical Administrative Databases PIA) • Updated figures that clearly describe current data flow and reporting across jurisdictions and current PIA boilerplate text, version 30, dated July 9, 2020.
Patient Reported Outcome Measures (PROMs)	Annual review – completed February 2022 **Amendments:** none 5-Year Scheduled Review – completed November 2019 **Amendments**: includes current PIA boilerplate text, as of March 7, 2019.

Appendix D — CIHI'S Privacy Impact Assessment Program – Summary of Recommendations

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
Population Grouping Methodology (POP Grouper) A renewal of the privacy impact assessment of the privacy and security risks associated with the Population Risk Adjustment Grouping Project which was established to develop a methodology and grouping software for population grouping using CIHI data and expertise.	No recommendations	—	—
Patient Level Physician Billing Data Repository A renewal of the privacy impact assessment of the privacy and security risks associated with the Patient-Level Physician Billing (PLPB) Repository. The PLPB Repository was established to support patient-focused analysis, to support CIHI's development of more comprehensive inpatient cost estimates and to enhance the quality of historical National Physician Database data and indicators.	No recommendations	—	—
National Rehabilitation Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the National Rehabilitation Reporting System which supports the planning and management of publicly funded inpatient rehabilitation services in Canada.	No recommendations	---	---
Insured Persons Repository The Insured Persons Repository was established to support the development and evolution of population grouping methodology (POP Grouper) by CIHI. It supports patient-focused analysis—age–sex- and morbidity-adjusted health care use by different populations—that currently cannot be conducted easily through other data sources.	No recommendations	---	---
Reabstraction Studies A renewal of the privacy impact assessment of the privacy and security risks associated with the reabstraction studies which are intended to enhance and support the existing routine data quality activities that CIHI has implemented to prevent, detect, monitor and resolve data issues.	No recommendations	---	---

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
Canadian Patient Experiences Data Collection and Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Canadian Patient Experiences Data Collection and Reporting System (CPERS). CPERS collects and reports on patient experiences within the health care system in Canada, beginning with inpatient acute care hospitals. The purpose of the CPERS is to provide standardized patient experience information from across Canada.	No recommendations	—	—
interRAI Reporting System (IRRS) A privacy impact assessment of the privacy and security risks associated with IRRS, which is a new data collection method (near real-time message based) and new validation process using a cloud-based application.	No recommendations	—	—
Your Health System: Insight A renewal of the privacy impact assessment of the privacy and security risks associated with Your Health System: Insight which builds on CIHI's years of experience in reporting indicators and measures that support Canada's health systems in monitoring performance and management.	No recommendations	—	—
Patient Reported Outcome Measures (PROMs) A renewal of the privacy impact assessment of the privacy and security risks associated with Patient-Reported Outcome Measures Program for Hip and Knee Arthroplasty. As part of the Ontario pilot, PROMs data is captured on hip and knee arthroplasty patients in participating acute care facilities and provided on a regular basis in electronic format to CIHI via Cancer Care Ontario and other authorized submitters. PROMs are essential to a patient-centred approach to health care, as they provide the patient's perspective on aspects of their health status that are relevant to their quality of life, including symptoms, function, pain and physical health.	No recommendations	—	—
Canadian Joint Replacement Registry A renewal of the privacy impact assessment of the privacy and security risks associated with the Canadian Joint Replacement Registry, a national registry that collects patient-specific information (clinical, surgical and prosthesis) on hip and knee replacement surgeries performed in Canada. It is a longitudinal database that allows for joint replacement patients to be followed over time to monitor their revision rates and outcomes.	No recommendations	—	—

Description of Privacy Impact Assessment	Recommendations	Manner Addressed	Date Recommendation Completed
Home Care Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Home Care Reporting System which is a pan-Canadian database that captures standardized information on publicly funded home care services. HCRS captures information about home care services provided by public agencies, and private agencies which the government hires to provide care to the public.	No recommendations	—	—
Continuing Care Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Continuing Care Reporting System. CCRS is a pan-Canadian database that captures standardized information on continuing care services provided by public facilities, and private facilities which the government hires to provide care to the public. It was developed to fulfill an identified need for consistent, comparable data about continuing care services in Canada.	No recommendations	—	—
Ontario Mental Health Reporting System A renewal of the privacy impact assessment of the privacy and security risks associated with the Ontario Mental Health Reporting System. OMHRS is a CIHI database which contains data about hospital inpatient mental health care. It is used to produce accurate, timely, and comparable statistical information on hospital inpatient mental health care including access to care, quality of care, and the resources consumed in providing that care.	No recommendations	—	—

Appendix E — CIHI'S Privacy Audit Program

Fiscal Year: 2018-19

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audits Completed
A compliance audit of an external third party that received data from CIHI to ensure the third-party is meeting or has met its contractual obligations, as set out in CIHI's confidentiality agreement.	5 non-conformities resulted in 1 opportunity for improvement and 8 recommendations: 1. Establish or amend existing policies for contract execution and management, including termination and closeout to ensure all objectives and requirements related to data acquisition and disposal are met. 2. Establish a person or body with responsibility for overseeing recipients of data from external third parties to ensure they comply with obligations that may be set out in a legal instrument. 3. Implement an auditable process for the receipt, protection, retention and disposal of PHI, regardless of format, it receives from external third parties; and promptly notify third party organizations from whom PHI is obtained about any likely or impending breach of a term or condition set out in a legal instrument.	Accepted as per recommendation Accepted as per recommendation Accepted as per recommendation	September 2019 September 2019 January 2020	October 26, 2018

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audits Completed
	4. Enhance its access management and back-up systems to ensure logs capture information about who and when folders and data files, for example, are accessed and deleted.	Accepted as per recommendation	September 2019	
	5. Store PHI in a separate location from staff's personal drive on the network, which would allow the organization to audit locations that contain PHI, only.	Accepted as per recommendation	September 2019	
	6. Provide additional training to its IT staff to ensure they are knowledgeable about the capabilities of access management and back-up systems, and processes.	Accepted as per recommendation	January 2019	
	7. Develop off-boarding (or transitioning) processes to address situations where significant changes are made to the roles and responsibilities of its employees, contractors, and agents who are engaged in research and use external third-party data obtained under a legal instrument; and communicate to those third parties when a change (e.g., change in employment status) to any provision set out in a legal instrument is required to ensure a written amendment is duly executed.	Accepted as per recommendation	September 2020	

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audits Completed
	8. Develop and implement administrative measures (e.g., supplementary instruction) and/or technical measures such as auditing of access logs in situations where cohort data (e.g., PHI from a third- party) is copied or downloaded from a server to a USB or other similar portable device.	Accepted as per recommendation	September 2019	
	9. An identified opportunity for improvement for CIHI resulted in a recommendation for CIHI to continue its practice of ensuring that the signatory to the legal instrument used for any future disclosure of PHI is made at a sufficiently senior level, such as a vice president of a hospital.	Accepted as per recommendation	No action required (existing practice)	

Fiscal Year: 2019-20

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audits Completed
A compliance audit of an external third party that received personal health information from CIHI to ensure the third-party is meeting or has met its contractual obligations, as set out in CIHI's research agreement.	While no non-conformities were identified through the audit, three opportunities for improvement were identified for the accountable organization to consideration.: 1. The accountable organization completed no systematic review or audit to validate and provide ongoing assurance that access provisioning and removal continues to perform as required under its policies. 2. The one instance of secure destruction completed by the accountable organization, as of the completion of the audit, was done so in compliance with the Agreement. However, there was no process in place to document this activity in a traceable way that would be available if CIHI requested such evidence. 3. The accountable organization does not appear to review its privacy and security policies on a routine basis to ensure the controls remain suitable, adequate, and effective.	Opportunities for improvement accepted and action will be considered Opportunities for improvement accepted and action taken Opportunities for improvement accepted and action will be considered	November 2019 September 2019 November 2019	November 1, 2019

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audits Completed
An internal privacy audit of CIHI's Access Management System to validate that access by both external clients and CIHI agents to CIHI's secure applications and tools containing personal health information is still required. Two audits were undertaken in 2019-20: • Your Health System (YHS): Insight – The YHS: Insight audit was comprised of a comprehensive operational review of how access is granted, and a detailed review of all external users. • Audit of CIHI employee access to environments where PHI may be present.	Two opportunities for improvement were identified because of the access audit of Your Health System (YHS): Insight: 1. An opportunity for improvement was identified to implement an on-going process to ensure access management processes and procedures are updated on a regular basis to ensure currency. 2. An opportunity for improvement was identified whereby all team members providing access should do an annual "recertification" where training is undertaken on an annual basis and their application of the materials is verified by someone else on the team. Two opportunities for improvement were identified because of the audit of CIHI employee access to environments where PHI may be present: 1. Internal employee access to tools and environments where PHI is present should be reviewed and confirmed on an annual basis.	Opportunities for improvement accepted and action taken Opportunities for improvement accepted and action taken	March 2020 December 2020 December 2019	March 2020 December 2019

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audits Completed
	2. Audit reporting capabilities for AMS need to allow for more specific reporting to target access where PHI may be suspected or known. **Note**: Effective February 2022, all access audits will be overseen by the Chief Information Security Officer, under CIHI's Security Audit Program, with audits reported in the associated sections of CIHI's Prescribed Entity Review reporting.		September 2020	

Fiscal Year: 2021-22

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audit Completed
A compliance survey audit of external third parties that received and continue to retain de-identified data and/or personal health information from CIHI to ensure the third parties continue to meet their contractual obligations, as set out in the agreement signed with CIHI. This compliance survey audit replaced the standard annual certification activity for 2021.	7 respondents were issued and have addressed, or are in the process of addressing, corrective measures recommended by CIHI to bring the organizations into compliance. Corrective measures implemented by accountable organizations: 1. The accountable organization elected to certify secure destruction all CIHI data received for the project. The accountable organization to complete, sign and return the CIHI-issued certificate of destruction. 2. The accountable organization elected to certify secure destruction all CIHI data received for the project. The accountable organization to complete, sign and return the CIHI-issued certificate of destruction. 3. The accountable organization to cease any access to CIHI data from any device not issued by and under control of the accountable organization. 4. The accountable organization to complete, sign and return a new	Accepted as per recommendations	November 2022 July 2022 December 2021 September 2022	December 2021

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audit Completed
	(updated) Information Security Form to CIHI, to confirm all administrative and technical controls comply with CIHI's minimum security requirements.			
	5. The accountable organization to upgrade VPN solution in compliance with CIHI's minimum security requirements, migrate projects into CIHI's Secure Access Environment, or cease work and certify secure destruction of all CIHI project data.		December 2022	
	6. The accountable organization elected to certify secure destruction all CIHI data received for the project. The accountable organization to complete, sign and return the CIHI-issued certificate of destruction.		January 2022	
	7. The accountable organization to complete and return an amendment form to CIHI, adding a new authorized person approved to access previously disclosed CIHI data.		December 2021	
	8. The accountable organization elected to certify secure destruction all CIHI data received for the project. The accountable		February 2022	

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audit Completed
	organization to complete, sign and return the CIHI-issued certificate of destruction			

Fiscal Year: 2022-23

Description of Audit	Recommendations	Manner Addressed	Date Recommendations Completed	Audit Completed
A compliance survey audit of external third parties that received and continue to retain de-identified data and/or personal health information from CIHI to ensure the third parties continue to meet their contractual obligations, as set out in the agreement signed with CIHI. This compliance survey audit replaced the standard annual certification activity for 2021. This is follow-up to the 2021 survey audit focusing on remote access to CIHI data.	In progress	—	—	—

Appendix F — IPC's 3-Year Statutory Review

Fiscal Year: 2020-21

Description of Review	Recommendations	Manner Addressed	Date Recommendation Completed	Review Completed
IPC/ON's mandatory 3-year review of CIHI's Prescribed Entity status.	1. It is recommended that CIHI develop and implement distinct policies and procedures in accordance with the policy structure and naming conventions set out in appendix A of the *Manual*. Doing so will better align CIHI's policies with the expectations set out in the *Manual* and thereby facilitate locating relevant content in any future review.	See CIHI Manual Cross Reference Tracking Chart	July 2022	Review completed October 31, 2020
	2. It is recommended that in developing distinct policies and procedures described above, CIHI ensure that each policy and procedure address compliance, audit, and enforcement as required under the *Manual*.	See CIHI Manual Cross Reference Tracking Chart	July 2022	
	3. It is recommended that CIHI amend its Privacy Policy to include a list of data holdings of personal health information it maintains and identify where an individual may obtain further information in relation to the purposes, data elements and data sources for each data holding of personal health information; and that the *Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information* be amended to address each requirement set out in the *Manual.*	See Appendix F-1 Supplementary Details to Appendix F	June 2022	
	4. It is recommended that CIHI amend its Privacy Policy to clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information, and to clearly	See Appendix F-1 Supplementary Details to Appendix F	June 2022	

Description of Review	Recommendations	Manner Addressed	Date Recommendation Completed	Review Completed
	distinguish between the use of personal health information for the purposes of section 45 of the *Act* and the use of personal health information for research purposes.			
	5. It is recommended that CIHI's *Policy on the Transparency of Privacy Policies, Procedures and Practices* be amended to address each requirement set out in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	6. It is recommended that CIHI's *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information* be amended to address each requirement set out in the *Manual* respecting the review and approval process and the conditions or restrictions on the approvals given.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	7. It is recommended that CIHI's *Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research* be amended to address each requirement set out in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	8. It is recommended that CIHI's *Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements* be amended to address each requirement set out in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	9. It is recommended that CIHI maintain the required logs of privacy impact assessments and logs of data holdings and that each log comply with the requirements set out in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	

Description of Review	Recommendations	Manner Addressed	Date Recommendation Completed	Review Completed
	10. It is recommended that CIHI complete its initiative to combine its various policies and procedures in respect of privacy audits into a single *Policy and Procedures in Respect of Privacy Audits* which addresses each requirement set out in the *Manual*.	-New Privacy Audit Policy approved - Also see Appendix F-1 Supplementary Details to Appendix F	September 2021	
	11. It is recommended that CIHI amend its *Policy and Procedures for Privacy Breach Management* and *Policy and Procedures for Information Security Breach Management* to clearly define "privacy breach" and "information security breach" and address each requirement set out in the *Manual*.	See Statement of Requested Exception in Exhibit A to the CEO Affidavit		
	12. It is recommended that CIHI's *Policy and Procedures for Secure Retention of Records of Personal Health Information* be amended to identify the agent(s) responsible for ensuring the secure retention of records of personal health information, require agents to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal and identify the reasonable steps that must be taken by agents as required in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	13. It is recommended that CIHI's *Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices* be amended to address each requirement set out in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	

Description of Review	Recommendations	Manner Addressed	Date Recommendation Completed	Review Completed
	14. It is recommended that CIHI's *Policy and Procedures for Secure Transfer of Records of Personal Health Information* be amended to address the manner of obtaining and recording acknowledgement of receipt of the records of personal health information transferred as required in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	15. It is recommended that CIHI's *Policy and Procedures for Secure Disposal of Records of Personal Health Information* be amended to address each requirement set out in the *Manual*.	See Appendix F-1 Supplementary Details to Appendix F	July 2022	
	16. It is recommended that CIHI ensure that all information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of personal health information as required by the *Manual* when adding or replacing information systems, technologies, applications and programs involving personal health information.	Over the past three years, all new business applications have been built on our legacy technology base (at the same level of compliance as our existing systems) and not on new technologies.	July 2022	
	17. It is recommended that CIHI ensure, and that its *Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs* require that its system control and audit logs are immutable.	See Appendix F-1 Supplementary Details to Appendix F	August 2021	
	18. It is recommended that CIHI's *Policy and Procedures for the Execution of Confidentiality Agreements by Agents* be amended to outline the process that must be followed where an executed confidentiality agreement is not received within a defined	See new Policy for the Execution of Confidentiality Agreements, s. 1.1	September 2021	

Description of Review	Recommendations	Manner Addressed	Date Recommendation Completed	Review Completed
	period as required by the *Manual*.	and 1.3, 2.1, 2.2 (also in appendix F-1)		
	19. It is recommended that CIHI's *Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship* be amended to provide a definition of "property" in compliance with the requirements of the *Manual*.	Definition of "property" included in Offboarding Checklist (also in appendix F-1)	April 2022	
	20. It is recommended that CIHI ensure that the Board of Directors is advised of the results of and any recommendations arising from investigations of any privacy breaches, information security breaches, and privacy complaints that are investigated, and the status of implementation of the recommendations.	Privacy and security breaches are reported to the Board (See P&S Incident Management Protocol); Investigations of privacy complaints are reported to the Present and CEO (Privacy Policy Procedures, s. 64.8)	June 2022	
	21. It is recommended that CIHI ensure that its reporting of indicators related to statements of purpose for data holdings containing personal health information and privacy impact assessments is provided in full compliance with the *Manual* at the start of the next review period.	Indicators updated to comply with this requirement	June 2022	
	22. It is recommended that CIHI ensure that its privacy impact assessments are reviewed annually, as required by CIHI's *Privacy Impact Assessment Policy*.	Indicators updated to comply with this requirement	June 2022	

Description of Review	Recommendations	Manner Addressed	Date Recommendation Completed	Review Completed

Appendix F-1 — Supplementary Details to Appendix F

The recommendations noted below have been satisfied. Below we have pinpointed exactly where in CIHI's practices and procedures each requirement is met.

Recommendation 3. It is recommended that CIHI amend its Privacy Policy to include a list of data holdings of personal health information it maintains and identify where an individual may obtain further information in relation to the purposes, data elements and data sources for each data holding of personal health information; and that the Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal Health Information be amended to address each requirement set out in the Manual.

CIHI Response:

3. Policy on the Transparency of Privacy Policies, Procedures and Practices	• must identify the information made available to the public and other stakeholders relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and that identifies the means by which such information is made available	Privacy and Security Framework- s. 2b
	• At a minimum, the policy must require the prescribed person or prescribed entity to make the following information available:	Privacy and Security Framework- s. 2b
	• Its Privacy Policy;	Privacy and Security Framework- s. 2b
	• Brochures or frequently asked questions related to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity;	Privacy and Security Framework- s. 2b

	• Documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information;	Privacy and Security Framework- s.2b
	• A list of the data holdings of personal health information maintained by the prescribed person or prescribed entity, including where an individual may obtain further information in relation to the purposes data elements and data sources for each data holding of personal health information.	Privacy and Security Framework- 2b
	• The name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the *Act* and its regulation may be directed.	Privacy and Security Framework- s.2b
	• It is recommended that privacy impact assessments or a summary of the privacy impact assessments conducted also be made available.	Privacy and Security Framework- s.2b
	• must set out the minimum content of the brochures or frequently asked questions described above	Privacy and Security Framework- s.2b
	• the brochures or frequently asked questions must describe the status of the prescribed person or prescribed entity under the Act, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information, including:	Privacy and Security Framework- s.2b
	• The types of personal health information collected and the persons or organizations from which this personal health information is typically collected;	Privacy and Security Framework- s.2b

	• The purposes for which personal health information is collected;	Privacy and Security Framework- s.2b
	• The purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used; and	Privacy and Security Framework- s.2b
	• The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed.	Privacy and Security Framework- s.2b
	• the brochures or frequently asked questions must also identify some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal	Privacy and Security Framework- s.2b
	• it is recommended that the brochures or frequently asked questions provide the name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its regulation may be directed	Privacy and Security Framework- s.2b
6. Policy and Procedures for Statements of Purpose for Data Holdings Containing Personal [Health] Information	• shall require the statements of purpose to set out the purpose of the data holding, the personal health information contained in the data holding, the source(s) of the personal health information and the need for the personal health information in relation to the identified purpose.	Privacy Impact Assessment Policy- s. 2
	• must identify the agent(s) responsible and the process that must be followed in completing the statements of purpose for the data holdings containing personal health information, including the agent(s) or other persons or organizations that must be consulted in completing the statements of purpose and the agent(s) responsible for approving the statements of purpose.	Privacy Impact Assessment Policy- Purpose
	• The role of the agent(s) that have been delegated day-to-day authority to manage the privacy program in respect of the statements of purpose shall also be specified.	Privacy Impact Assessment Policy- s. 4

	• must identify the persons and organizations that will be provided the statements of purpose. At a minimum, this should include the health information custodians or other persons or organizations from whom the personal health information in the data holding is collected.	Privacy Impact Assessment Policy –s. 5
	• shall require that the statements of purpose be reviewed on an ongoing basis in order to ensure their continued accuracy and in order to ensure that the personal health information collected for purposes of the data holding is still necessary for the identified purposes. In this regard, the frequency with which and the circumstances in which the statements of purpose are required to be reviewed must be identified.	Privacy Impact Assessment Policy- s. 12
	• must document the agent(s) responsible and the process that must be followed in reviewing the statements of purpose and in amending the statements of purpose, if necessary. This shall include the agent(s) or other persons or organizations that must be consulted in reviewing, and if necessary, amending the statements of purpose and the agent(s) responsible for approving the amended statements of purpose.	Privacy Impact Assessment Policy- s.12-14
	• must identify the persons and organizations that will be provided amended statements of purpose upon approval, including health information custodians or other persons or organizations from whom the personal health information in the data holding is collected.	Privacy Impact Assessment Policy- s. 5
	• The prescribed person or prescribed entity shall require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Privacy Impact Assessment Policy – Compliance, Audit and Enforcement
	• must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Privacy Impact Assessment Policy – Compliance, Audit and Enforcement
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Privacy Impact Assessment Policy – Compliance, Audit and Enforcement

Recommendation 4. It is recommended that CIHI amend its Privacy Policy to clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information, and to clearly distinguish between the use of personal health information for the purposes of section 45 of the Act and the use of personal health information for research purposes.

CIHI Response:

Use of Personal Health Information	
• The purposes for which the prescribed person or prescribed entity uses personal health information must be identified	Privacy Policy Procedures- s. 3.1 and 10.3
• must clearly distinguish between the use of personal health information and the use of de-identified and/or aggregate information and between the use of personal health information for purposes of subsection 39(1)(c) or section 45 of the Act, as the case may be, and the use of personal health information for research purposes	Privacy Policy Procedures- s. 7.1
• must ensure that each use of personal health information identified in the Privacy Policy is consistent with the uses of personal health information permitted by the Act and its regulation	Privacy Policy Procedures – s. 10.4.2
• must articulate a commitment by the prescribed person or prescribed entity not to use personal health information if other information will serve the purpose and not to use more personal health information than is reasonably necessary to meet the purpose and must identify some of the policies, procedures and practices implemented by the prescribed person or prescribed entity in this regard, including limits on the use of personal health information by agents	Privacy Policy- s. 3.
• should state that the prescribed person or prescribed entity remains responsible for personal health information used by its agents and should identify the policies, procedures and practices implemented to ensure that its agents only collect, use, disclose, retain and dispose of personal health information in compliance with the Act and its regulation and in compliance with the privacy and security policies, procedures and practices implemented.	Privacy Policy - s. 11

10. Policy and Procedures for the Use of Personal [Health] Information for Research	• must articulate a commitment by the prescribed person or prescribed entity not to use personal health information for research purposes if other information will serve the research purpose and not to use more personal health information than is reasonably necessary to meet the research purpose.	N/A- CIHI does not use personal health information for research purposes as contemplated by paragraph 37(1)(j) of the Act nor does CIHI use aggregate or de-identified data for research purposes.
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	N/A
	• must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Privacy Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	N/A
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of the policy or its procedures.	N/A
	Where the Use of Personal Health Information is Permitted for Research	
	• if the prescribed person or prescribed entity permits personal health information to be used for research purposes, the policy and procedures must set out the circumstances in which personal health information is permitted to be used for research purposes	N/A

	Distinction between the Use of Personal Health Information for Research and Other Purposes	
	• must clearly distinguish between the use of personal health information for research purposes and the use of personal health information for purposes of subsection 39(1)(c) or section 45 of the Act, as the case may be. The criteria that must be considered in determining when a use of personal health information is for research purposes and when a use is for purposes of subsection 39(1)(c) or section 45 of the Act, as well as the agent(s) responsible and the procedure to be followed in making this determination, must also be addressed.	N/A
	Review and Approval Process	
	• must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of personal health information for research purposes and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	N/A
	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request to use personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the Act and its regulation.	N/A
	• prior to any approval of the use of personal health information for research purposes, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to review the written research plan to ensure it complies with the requirements in the Act and its regulation, to ensure that the written research plan has been approved by a research ethics board and to ensure that the prescribed person or prescribed entity is in receipt of a copy of the decision of the research ethics board approving the written research plan.	N/A
	• prior to any approval of the use of personal health information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal health information being requested is consistent with the personal health	N/A

	information identified in the written research plan approved by the research ethics board. The responsible agent(s) must also be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.	
	• should set out the manner in which the decision approving or denying the request to use personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	N/A
	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions that will be imposed on the approval to use personal health information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.	N/A
	• in determining the conditions or restrictions that will be imposed, the policy and procedures shall have regard to the Act and its regulation.	N/A
	• At a minimum, the agent(s) granted approval to use personal health information for research purposes must be required to comply with subsections 44(6) (a) to (f) of the Act.	N/A
	• must identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of personal health information for research purposes are in fact being satisfied.	N/A
	Secure Retention	
	• must require the agent granted approval to use personal health information for research purposes to retain the records of personal health information in compliance with the written research plan approved by the research ethics board and in compliance with the Policy and Procedures for Secure Retention of Records of Personal Health Information.	N/A

	Secure Return or Disposal	
	• must address whether an agent granted approval to use personal health information for research purposes is required to securely return or securely dispose of the records of personal health information or is permitted to de-identify and retain the records following the retention period in the written research plan approved by the research ethics board.	N/A
	• if records of personal health information are required to be securely returned to the prescribed person or prescribed entity, the policy and procedures must stipulate the time frame following the retention period set out in the written research plan within which the records must be securely returned, the secure manner in which the records must be returned and the agent to whom the records must be securely returned.	N/A
	• if records of personal health information are required to be disposed of in a secure manner, the policy and procedures must require the records to be disposed of in accordance with the *Policy and Procedures for Secure Disposal of Records of Personal Health Information.*	N/A
	• must stipulate the time frame following the retention period in the written research plan within which the records must be securely disposed of, must require a certificate of destruction to be provided, must identify the agent of the prescribed person or prescribed entity to whom the certificate of destruction must be provided and must identify the time frame following secure disposal within which the certificate of destruction must be provided. The certificate of destruction confirming the secure disposal must be required to identify the records of personal health information securely disposed of and the date, time and method of secure disposal employed and must be required to bear the name and signature of the agent who performed the secure disposal.	N/A
	• if records of personal health information are required to be de-identified and retained by the agent rather than being securely returned or disposed of, the policy and procedures shall require the records of personal health information to be de-identified in compliance with the Policy and Procedures With Respect to De-Identification and Aggregation. The policy and procedures must further stipulate the time frame following the retention period set out in the written research plan within which the records must be de-identified.	N/A

	• must identify the agent(s) responsible for ensuring that records of personal health information used for research purposes are securely returned, securely disposed of or de-identified within the stipulated time frame following the retention period set out in the written research plan and the process to be followed in the event that the records of personal health information are not securely returned, a certificate of destruction is not received or the records of personal health information are not de-identified within the time frame identified.	N/A
	Tracking Approved Uses of Personal Health Information for Research	
	• must require that a log be maintained of the approved uses of personal health information for research purposes and must identify the agent(s) responsible for maintaining such a log.	N/A
	• recommended that the policy and procedures address where written research plans, copies of the decisions of research ethics boards, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the use of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.	N/A
	Where the Use if Personal Health Information is not Permitted for Research	
	• if the prescribed person or prescribed entity does not permit personal health information to be used for research purposes, the policy and procedures must expressly prohibit the use of personal health information for research purposes and must indicate whether or not de-identified and/or aggregate information may be used for research purposes.	Privacy Policy Procedures- s. 7.1
	Review and Approval Process	
	• if the prescribed person or prescribed entity permits de-identified and/or aggregate information to be used for research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the use of de-identified and/or aggregate information for research purposes and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or	N/A

	executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	
	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request to use de-identified and/or aggregate information for research purposes. At a minimum, the policy and procedures must require the de-identified and/or aggregate information to be reviewed prior to the approval and use of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	N/A
	• should set out the manner in which the decision approving or denying the request for the use of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	N/A
	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions that will be imposed on the approval to use de-identified and/or aggregate information for research purposes, including any documentation that must be completed, provided or executed and the agent(s) responsible for completing, providing or executing the documentation.	N/A
	• must prohibit an agent granted approval to use de-identified and/or aggregate information for research purposes from using that information, either alone or with other information, to identify an 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.	N/A
	• must identify the agent(s) responsible for ensuring that any conditions or restrictions imposed on the use of de-identified and/or aggregate information for research purposes are in fact being satisfied.	N/A

Recommendation 5. It is recommended that CIHI's Policy on the Transparency of Privacy Policies, Procedures and Practices be amended to address each requirement set out in the Manual.

CIHI response:

3. Policy on the Transparency of Privacy Policies, Procedures and Practices	• must identify the information made available to the public and other stakeholders relating to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and that identifies the means by which such information is made available	Privacy and Security Framework- s. 2b
	• At a minimum, the policy must require the prescribed person or prescribed entity to make the following information available:	Privacy and Security Framework- s. 2b
	• Its Privacy Policy;	Privacy and Security Framework- s. 2b
	• Brochures or frequently asked questions related to the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity;	Privacy and Security Framework- s. 2b
	• Documentation related to the review by the Information and Privacy Commissioner of Ontario of the policies, procedures and practices implemented by the prescribed person or prescribed entity to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information;	Privacy and Security Framework- s. 2b
	• A list of the data holdings of personal health information maintained by the prescribed person or prescribed entity; and	Privacy and Security Framework- s. 2b
	• The name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the *Act* and its regulation may be directed.	Privacy and Security Framework- s.2b
	• It is recommended that privacy impact assessments or a summary of the privacy impact assessments conducted also be made available.	Privacy and Security Framework- s.2b

	• must set out the minimum content of the brochures or frequently asked questions described above	Privacy and Security Framework- s.2b
	• the brochures or frequently asked questions must describe the status of the prescribed person or prescribed entity under the Act, the duties and responsibilities arising from this status and the privacy policies, procedures and practices implemented in respect of personal health information, including:	Privacy and Security Framework- s.2b
	• The types of personal health information collected and the persons or organizations from which this personal health information is typically collected;	Privacy and Security Framework- s.2b
	• The purposes for which personal health information is collected;	Privacy and Security Framework- s.2b
	• The purposes for which personal health information is used, and if identifiable information is not routinely used, the nature of the information that is used; and	Privacy and Security Framework- s.2b
	• The circumstances in which and the purposes for which personal health information is disclosed and the persons or organizations to which it is typically disclosed.	Privacy and Security Framework- s.2b
	• the brochures or frequently asked questions must also identify some of the administrative, technical and physical safeguards implemented to protect the privacy of individuals whose personal health information is received and to maintain the confidentiality of that information, including the steps taken to protect personal health information against theft, loss and unauthorized use or disclosure and to protect records of personal health information against unauthorized copying, modification or disposal	Privacy and Security Framework- s.2b
	• it is recommended that the brochures or frequently asked questions provide the name and/or title, mailing address and contact information of the agent(s) to whom inquiries, concerns or complaints regarding compliance with the privacy policies, procedures and practices implemented and regarding compliance with the Act and its regulation may be directed	Privacy and Security Framework- s.2b

Recommendation 6. It is recommended that CIHI's Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information be amended to address each requirement set out in the Manual respecting the review and approval process and the conditions or restrictions on the approvals given.

CIHI response:

8. Policy and Procedures for Limiting Agent Access to and Use of Personal [Health] Information	• must be developed and implemented to limit access to and use of personal health information by agents based on the "need to know" principle. The purpose of this policy and its procedures is to ensure that agents of the prescribed person or prescribed entity access and use both the least identifiable information and the minimum amount of identifiable information necessary for carrying out their day-to-day employment, contractual or other responsibilities.	Privacy Policy – s. 10
	• must identify the limited and narrowly defined purposes for which and circumstances in which agents are permitted to access and use personal health information and the levels of access to personal health information that may be granted.	Privacy Policy Procedures – s. 10.1 to 10.16 generally
	• The prescribed person or prescribed entity must ensure that the duties of agents with access to personal health information are segregated in order to avoid a concentration of privileges that would enable a single agent to compromise personal health information.	Privacy Policy Procedures – s. 10.1 to 10.16 generally
	• for all other purposes and in all other circumstances, the policy and procedures must require agents to access and use de-identified and/or aggregate information, as defined in the *Policy and Procedures with Respect to De-Identification and Aggregation*.	Privacy Policy Procedures – s. 10.1
	• must explicitly prohibit access to and use of personal health information if other information, such as de-identified and/or aggregate information, will serve the identified purpose and must prohibit access to or use of more personal health information than is reasonably necessary to meet the identified purpose.	Privacy Policy Procedures – s. 10.2 and 10.3

	• must prohibit agents from using de-identified and/or aggregate information, either alone or with other information, to identify an 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.	Privacy Policy Procedures – s. 3.2
	Review and Approval Process	
	• shall set out the agent(s) responsible and the process to be followed in receiving, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information, along with the various level(s) of access that may be granted by the prescribed person or prescribed entity.	Privacy Policy Procedures – s. 10.4 to 10.14 For each category of CIHI access, the agents are identified and the level of access that is granted is also identified (from the titles we can see whether it is access to General Use Data files, system applications or Network Drive, etc.).
	• must set out the requirements to be satisfied in requesting, reviewing and determining whether to approve or deny a request by an agent for access to and use of personal health information; the documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	Privacy Policy Procedures – s. 10.4 to 10.14

	• must set out the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for access to and use of personal health information and, if the request is approved, the criteria that must be considered in determining the appropriate level of access	Privacy Policy Procedures – s. 10.4 to 10.14
	• At a minimum, the agent(s) responsible for determining whether to approve or deny the request must be satisfied that:	
	▪ The agent making the request routinely requires access to and use of personal health information on an ongoing basis or for a specified period for his or her employment, contractual or other responsibilities;	Privacy Policy Procedures – 10.4.1
	▪ The identified purpose for which access to and use of personal health information is requested is permitted by the *Act* and its regulation;	Privacy Policy Procedures – 10.4.2
	▪ The identified purpose for which access to and use of personal health information is requested cannot reasonably be accomplished without personal health information;	Privacy Policy Procedures – 10.4.3
	▪ De-identified and/or aggregate information will not serve the identified purpose; and	Privacy Policy Procedures – 10.4.4
	▪ In approving the request, no more personal health information will be accessed and used than is reasonably necessary to meet the identified purpose.	Privacy Policy Procedures – 10.4.5
	• should set out the manner in which the decision approving or denying the request for access to and use of personal health information and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; to whom the decision will be communicated; any documentation that must be completed, provided and/or executed upon rendering the decision; the agent(s) responsible for	Privacy Policy Procedures – s. 10 generally

	completing, providing and/or executing the documentation; and the required content of the documentation.	
	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions imposed on an agent granted approval to access and use personal health information, such as read, create, update or delete limitations, and the circumstances in which the conditions or restrictions will be imposed.	Privacy Policy Procedures – s. 10 generally
	• in the event that an agent only requires access to and use of personal health information for a specified period, the policy and procedures must set out the process to be followed in ensuring that access to and use of the personal health information is permitted only for that specified time period.	Privacy Policy Procedures – ss. 10.17-10.21
	• recommended that all approved accesses and uses of personal health information be subject to an automatic expiry, following which an agent is again required to request approval to access and use personal health information in accordance with the policy and its procedures. At a minimum, it is recommended that the expiry date be one year from the date approval is granted.	Privacy Policy Procedures – s. 10.21.3 – 10.21.4
	• must prohibit an agent granted approval to access and use personal health information from accessing and using personal health information except as necessary for his or her employment, contractual or other responsibilities; from accessing and using personal health information if other information will serve the identified purpose; and from accessing and using more personal health information than is reasonably necessary to meet the identified purpose.	Privacy Policy Procedures - s. 10.1 – 10.3
	• The prescribed person or prescribed entity also ensure that all accesses to and uses of personal health information are permitted by the Act and its regulation.	Privacy Policy – s. 7

	• must impose conditions or restrictions on the purposes for which and the circumstances in which an agent granted approval to access and use personal health information is permitted to disclose that personal health information. The prescribed person or prescribed entity must ensure that any such disclosures are permitted by the Act and its regulation.	Privacy Policy and Privacy Policy Procedures – All provisions related to disclosure of PHI in general (s. 37 to 57)
	Notification and Termination of Access and Use	
	• must require an agent granted approval to access and use personal health information, as well as his or her supervisor, to notify the prescribed person or prescribed entity when the agent is no longer employed or retained by the prescribed person or prescribed entity or no longer requires access to or use of the personal health information.	Privacy Policy Procedures - s. 10.17 – 10.20
	• must identify the procedure to be followed in providing the notification. In particular, the policy and procedures must identify the agent(s) to whom this notification must be provided; the time frame within which this notification must be provided; the format of the notification; the documentation that must be completed, provided and/or executed, if any; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom the documentation must be provided; and the required content of the documentation.	Privacy Policy Procedures - s. 10.17 – 10.20
	• must identify the agent(s) responsible for terminating access to and use of the personal health information, the procedure to be followed in terminating access to and use of the personal health information and the time frame within which access to and use of the personal health information must be terminated.	Privacy Policy Procedures -10.17 – 10.20
	• The prescribed person or prescribed entity must ensure that the procedures implemented in this regard are consistent with the Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship.	Yes – they are consistent

	Secure Retention	
	• must require an agent granted approval to access and use personal health information to securely retain the records of personal health information in compliance with the Policy and Procedures for Secure Retention of Records of Personal Health Information.	Privacy Policy Procedures - s. 10.5 (Ref. Secure Information Storage Standard)
	Secure Disposal	
	• must require an agent granted approval to access and use personal health information to securely dispose of the records of personal health information in compliance with the Policy and Procedures for Secure Disposal of Records of Personal Health Information.	Privacy Policy Procedures - s. 10.5 (Ref. Secure Destruction Standard)
	Tracking Approved Access to and Use of Personal Health Information	
	• must require that a log be maintained of agents granted approval to access and use personal health information and must identify the agent(s) responsible for maintaining such a log.	Privacy Policy Procedures - s. 10.21.2
	• recommended that the policy and procedures address where documentation related to the receipt, review, approval, denial or termination of access to and use of personal health information is to be retained and the agent(s) responsible for retaining this documentation.	Privacy Policy Procedures – s. 10.21.2
	Compliance, Audit and Enforcement	
	• The prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Privacy Policy- Page 3: Compliance, Audit and Enforcement

	• In the event that there is no automatic expiry date on the approval to access and use personal health information, regular audits of agents granted approval to access and use personal health information must be conducted in accordance with the Policy and Procedures In Respect of Privacy Audits. The purpose of the audit is to ensure that agents granted such approval continue to be employed or retained by the prescribed person or prescribed entity and continue to require access to the same amount and type of personal health information. In this regard, the policy and procedures must identify the agent(s) responsible for conducting the audits and for ensuring compliance with the policy and its procedures and the frequency with which the audits must be conducted. At a minimum, audits must be conducted on an annual basis.	Privacy Policy Procedures - s. 10.21.5
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Privacy Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Privacy Policy- Page 3: Notification of Breach

Recommendation 7: It is recommended that CIHI's Policy and Procedures for Disclosure of Personal Health Information for Purposes Other Than Research be amended to address each requirement set out in the Manual.

CIHI response:

12. Policy and Procedures for Disclosure of Personal [Health] Information for Purposes Other Than Research	• A policy and procedures must be developed and implemented to identify whether and in what circumstances, if any, personal health information is permitted to be disclosed for purposes other than research.	Privacy Policy s. 37, 40 and 42
	• must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information if other information will serve the purpose and not to disclose more personal health information than is reasonably necessary to meet the purpose.	Privacy Policy- s. 40
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Privacy Policy-Page 3: Compliance, Audit and Enforcement
	• must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Privacy Policy- Page 3: Compliance, Audit and Enforcement
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy* Breach *Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Privacy Policy- Page 3: Notification of Breach
	Where the Disclosure of Personal Health Information is Permitted	
	• if the prescribed person or prescribed entity permits personal health information to be disclosed for purposes other than research, the policy and procedures must set out the purposes for which and the circumstances in which the disclosure of personal health information is permitted.	Privacy Policy- s. 37, s.38, s. 40
	• must require that all disclosures of personal health information comply with the *Act* and its regulation.	Privacy Policy Procedures- s. 38.5

	Review and Approval Process	
	• must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for purposes other than research and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	Privacy Policy Procedures- s. 42.1 - 42.8
	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for purposes other than research. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.	Privacy Policy Procedures- s. 42.1 and 42.2
	• The agent(s) responsible for determining whether to approve or deny the request for the disclosure of personal health information for purposes other than research must be required to ensure that the disclosure is permitted by the *Act* and its regulation and that any and all conditions or restrictions set out in the *Act* and its regulation have been satisfied. For example, if a prescribed entity is requested to disclose personal health information to a health information custodian who provided the personal health information directly or indirectly to the prescribed entity, the prescribed entity must ensure that the personal health information does not contain any additional identifying information.	Privacy Policy Procedures- s. 42.2 and s. 35
	• The criteria must require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose of the disclosure and that no more personal health information is being requested than is reasonably necessary to meet the identified purpose.	Privacy Policy Procedures- 42.1
	• should set out the manner in which the decision approving or denying the request for the disclosure of personal health information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	Privacy Policy Procedures- s. 42.1 – 42.8

	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for purposes other than research, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.	Privacy Policy Procedures- s. 42.4
	• must require a Data Sharing Agreement to be executed in accordance with the *Policy and Procedures for the Execution of Data Sharing Agreements* and the *Template Data Sharing* Agreement *p*rior to any disclosure of personal health information for purposes other than research.	Privacy Policy Procedures- 42.4
	• must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information have in fact been satisfied, including the execution of a Data Sharing Agreement.	Privacy Policy Procedures- s. 42.1 – 42.8
	Secure Transfer	
	• must require records of personal health information to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.	Privacy Policy Procedures- s. 42.5 (Ref. Secure Information Transfer Standard)
	Secure Return or Disposal	
	• must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a person or organization for purposes other than research are either securely returned or securely disposed of, as the case may be, following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement.	Privacy Policy Procedures- s. 42.7

	• must address the process to be followed where records of personal health information are not securely returned or a certificate of destruction is not received within a reasonable period of time following the retention period in the Data Sharing Agreement or the date of termination of the Data Sharing Agreement. This shall include the agent(s) responsible for implementing this process and the stipulated time frame following the retention period or the date of termination within which this process must be implemented.	Privacy Policy Procedures- s. 42.8
	Documentation Related to Approved Disclosures of Personal Health Information	
	• it is recommended that the policy and procedures address where documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for purposes other than research will be retained and the agent(s) responsible for retaining this documentation.	Privacy Policy Procedures- s. 42.4
	Where the Disclosure of Personal Health Information is not Permitted	
	• if the prescribed person or prescribed entity does not permit personal health information to be disclosed in these circumstances, the policy and procedures must expressly prohibit the disclosure of personal health information for non-research purposes, except where required by law, and must indicate whether or not de-identified and/or aggregate information may be disclosed.	N/A as CIHI permits PHI to be disclosed for non-research purposes
	Review and Approval Process	
	• if the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for non-research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information and the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed; the agent(s) or other persons or organizations responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	Privacy Policy Procedures- s. 48.1 – 48.5 (for de-identified data) PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"

	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for purposes other than research.	Privacy Policy Procedures- s. 37, s. 48.1, 48.3 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• must require the de-identified and/or aggregate information to be reviewed prior to the disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	Privacy Policy Procedures- s. 48.2 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Roles and Responsibilities"
	• should set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for purposes other than research and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	Privacy Policy Procedures- s. 48.1, 48.3 – 48.5 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"

	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for non-research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or other persons or organizations responsible for completing, providing or executing the documentation and/or agreements.	Privacy Policy Procedures- s. 48.1 – 48.4. 48.5, 45.8 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• The prescribed person or prescribed entity must require the person or organization to which the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the person or organization will not use the de-identified and/or aggregate information, either alone or with other information, to identify an 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.	Privacy Policy and Privacy Policy Procedures- s. 48.3 CIHI has included this wording in all agreements, including the licensing agreement for disclosure of aggregate information.
	• must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement.	Privacy Policy Procedures- s. 48.1, 48.2, 48.3 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"

	• must require the responsible agent(s) to track receipt of the executed written acknowledgments and must set out the procedure that must be followed and the documentation that must be maintained in this regard.	Privacy Policy Procedures- s. 48.1 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"

Recommendation 8: It is recommended that CIHI's Policy and Procedures for Disclosure of Personal Health Information for Research Purposes and the Execution of Research Agreements be amended to address each requirement set out in the Manual.

CIHI Response:

13. Policy and Procedures for Disclosure of Personal [Health] Information for Research Purposes and the Execution	• must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes.	Privacy Policy - s. 37 and 43
	• must articulate a commitment by the prescribed person or prescribed entity not to disclose personal health information for research purposes if other information will serve the research purpose and not to disclose more personal health information than is reasonably necessary to meet the research purpose.	Privacy Policy- s. 40
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Privacy Policy- Page 3: Compliance, Audit and Enforcement
	• must stipulate that compliance will be audited in accordance with the *Policy and Procedures In Respect of Privacy Audits*, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Privacy Policy- Page 3: Compliance, Audit and Enforcement

of Research Agreements	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the *Policy and Procedures for Privacy Breach Management*, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Privacy Policy- Page 3: Notification of Breach
	Where the Disclosure of Personal Health Information is Permitted for Research	
	• If the prescribed person or prescribed entity permits personal health information to be disclosed for research purposes, the policy and procedures must set out the circumstances in which personal health information is permitted to be disclosed for research purposes.	Privacy Policy- s. 37(c)&(d) and s. 40 Privacy Policy Procedures – s. 40.1 and 40.3, 43.2
	Review and Approval Process	
	• must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of personal health information for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by the researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	Privacy Policy Procedures- s. 43.1 and 43.2 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve the request for the disclosure of personal health information for research purposes. In identifying the requirements that must be satisfied and the criteria that must be considered, the policy and procedures shall have regard to the *Act* and its regulation.	Privacy Policy- s. 43; Privacy Policy Procedures- s. 43.3 and 43.4

	• prior to any approval of the disclosure of personal health information for research purposes, must require the agent(s) responsible for determining whether to approve or deny the request to ensure that the prescribed person or prescribed entity is in receipt of a written application, a written research plan and a copy of the decision of the research ethics board approving the written research plan and that the written research plan complies with the requirements in the *Act* and its regulation.	Privacy Policy Procedures- s. 43.3 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• prior to any approval of the disclosure of personal health information for research purposes, the agent(s) responsible for determining whether to approve or deny the request must be required to ensure that the personal health information being requested is consistent with the personal health information identified in the written research plan approved by the research ethics board.	Privacy Policy Procedures- s. 43.3 (iii) PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• the responsible agent(s) must be required to ensure that other information, namely de-identified and/or aggregate information, will not serve the research purpose and that no more personal health information is being requested than is reasonably necessary to meet the research purpose.	Privacy Policy- s. 40 Privacy Policy Procedures - s. 43.3 (iii)
	• should also set out the manner in which the decision approving or denying the request for the disclosure of personal health information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	Privacy Policy Procedures- s. 43.6 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Roles and Responsibilities"

	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of personal health information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.	Privacy Policy Procedures - s. 43.1 – 43.8 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• must require that a Research Agreement be executed in accordance with the *Template Research Agreement* prior to the disclosure of personal health information for research purposes.	Privacy Policy Procedures – s. 43.6
	• must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of personal health information for research purposes have in fact been satisfied, including the execution of a Research Agreement.	Privacy Policy Procedures- s. 43.1 – 43.8 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"

	Secure Transfer	
	• The policy and procedures shall require the records of personal health information disclosed for research purposes to be transferred in a secure manner in compliance with the *Policy and Procedures for Secure Transfer of Records of Personal Health Information*.	Privacy Policy Procedures - 43.2 (Ref. Secure Information Transfer Standard)
	Secure Return or Disposal	
	• must identify the agent(s) responsible for ensuring that records of personal health information disclosed to a researcher for research purposes are either securely returned, securely disposed of or de-identified, as the case may be, following the retention period set out in the Research Agreement.	Privacy Policy Procedures- s. 43.7
	• must address the process to be followed by the responsible agent(s) where records of personal health information are not securely returned, a certificate of destruction is not received or written confirmation of de- identification is not received within the time set out in the Research Agreement.	Privacy Policy Procedures – 43.8
	Documentation Related to Approved Disclosures of Personal Health Information for Research	
	• it is recommended that the policy and procedures also address where written applications, written research plans, copies of the decisions of research ethics boards, Research Agreements, certificates of destruction and other documentation related to the receipt, review, approval or denial of requests for the disclosure of personal health information for research purposes will be retained and the agent(s) responsible for retaining this documentation.	Privacy Policy Procedures – 43.3 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under “Roles and Responsibilities”

	Where the Disclosure of Personal Health Information is not Permitted for Research	
	• if the prescribed person or prescribed entity does not permit personal health information to be disclosed for research purposes, the policy and procedures must expressly prohibit the disclosure of personal health information for research purposes and must indicate whether or not de- identified and/or aggregate information may be disclosed for research purposes.	N/A as CIHI permits PHI to be disclosed for research purposes
	Review and Approval Process	
	• if the prescribed person or prescribed entity permits de-identified and/or aggregate information to be disclosed for research purposes, the policy and procedures must identify the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the disclosure of de-identified and/or aggregate information for research purposes, as well as the process that must be followed in this regard. This shall include a discussion of the documentation that must be completed, provided and/or executed by agent(s) of the prescribed person or prescribed entity or by a researcher; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	Privacy Policy Procedures- s. 48.1 – 48.5 (for de-identified data) PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• for example, the policy and procedures should address whether the prescribed person or prescribed entity requires the preparation of a written research plan in accordance with the *Act* and its regulation and/or requires research ethics board approval of the written research plan prior to the disclosure of de-identified and/or aggregate information for research purposes.	PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny the request for the disclosure of de-identified and/or aggregate information for research purposes.	PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and

		"Roles and Responsibilities"
	• must require the de-identified and/or aggregate information to be reviewed prior to the approval and disclosure of the de-identified and/or aggregate information in order to ensure that the information does not identify an individual and that it is not reasonably foreseeable in the circumstances that the information could be utilized, either alone or with other information, to identify an individual. The agent(s) responsible for undertaking this review shall also be identified.	Privacy Policy Procedures – s. 48.1 and 48.2 PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Roles and Responsibilities"
	• should also set out the manner in which the decision approving or denying the request for the disclosure of de-identified and/or aggregate information for research purposes and the reasons for the decision are documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"
	Conditions or Restrictions on the Approval	
	• must identify the conditions or restrictions that are required to be satisfied prior to the disclosure of de-identified and/or aggregate information for research purposes, including any documentation and/or agreements that must be completed, provided or executed and the agent(s) or researcher responsible for completing, providing or executing the documentation and/or agreements.	PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Procedures" and "Roles and Responsibilities"

	• the prescribed person or prescribed entity must require the researcher to whom the de-identified and/or aggregate information will be disclosed to acknowledge and agree, in writing, that the researcher will not use the de-identified and/or aggregate information, either alone or with other information, to identify an 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.	Privacy Policy and Privacy Policy Procedures- ss. 48.6 and 48.7 CIHI will ensure that this wording is included in the licensing agreement for disclosure of aggregate information.
	• must identify the agent(s) responsible for ensuring that any conditions or restrictions that must be satisfied prior to the disclosure of the de-identified and/or aggregate information have in fact been satisfied, including the execution of the written acknowledgement.	PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Roles and Responsibilities"
	• must require the responsible agent(s) to track receipt of the executed written acknowledgments and set out the procedure that must be followed and the documentation that must be maintained in this regard.	PROCEDURE: Data Disclosure to Third Party Data Requestors via CIHI Data Request Program, under "Roles and Responsibilities"

Recommendation 9: It is recommended that CIHI maintain the required logs of privacy impact assessments and logs of data holdings and that each log comply with the requirements set out in the Manual.

CIHI Response:

• must require that a log be maintained of privacy impact assessments that have been completed; that have been undertaken but that have not been completed; and that have not been undertaken. The policy and procedures must also identify the agent(s) responsible for maintaining such a log.	Privacy Impact Assessment Policy- s.10

Recommendation 10: It is recommended that CIHI complete its initiative to combine its various policies and procedures in respect of privacy audits into a single Policy and Procedures in Respect of Privacy Audits which addresses each requirement set out in the Manual.

CIHI Response: New Privacy Audit Policy approved September 2021

27. Policy and Procedures in Respect of Privacy Audits	• must be developed and implemented that sets out the types of privacy audits that are required to be conducted.	Privacy Audit Policy- Purpose
	• the audits required to be conducted shall include audits to assess compliance with the privacy policies, procedures and practices implemented by the prescribed person or prescribed entity and audits of the agent(s) permitted to access and use personal health information pursuant to *Policy and Procedures for Limiting Agent Access to and Use of Personal Health Information*.	Privacy Audit Policy- s. 1
	• with respect to each privacy audit that is required to be conducted, the policy and procedures must set out the purposes of the privacy audit; the nature and scope of the privacy audit (i.e. document reviews, interviews, site visits, inspections); the agent(s) responsible for conducting the privacy audit; and the frequency with which and the circumstances in which each privacy audit is required to be conducted.	Privacy Audit Policy- s. 1.3 and 1.4
	• shall require a privacy audit schedule to be developed and shall identify the agent(s) responsible for developing the privacy audit schedule.	Privacy Audit Policy- s. 1.2

	• for each type of privacy audit that is required to be conducted, the policy and procedures shall also set out the process to be followed in conducting the audit. This is to include the criteria that must be considered in selecting the subject matter of the audit and whether or not notification will be provided of the audit, and if so, the nature and content of the notification and to whom the notification must be provided.	Privacy Audit Policy- s. 3.1, 3.2, 3.3.
	• must further discuss the documentation that must be completed, provided and/or executed in undertaking each privacy audit; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	Privacy Audit Policy- s. 3.4, 3.5, 3.6,
	• the role of agent(s) that have been delegated day-to-day authority to manage the privacy program and the security program shall also be identified.	Privacy Audit Policy- s. 1.1
	• shall set out the process that must be followed in addressing the recommendations arising from privacy audits, including the agent(s) responsible for assigning other agent(s) to address the recommendations, for establishing timelines to address the recommendations, for addressing the recommendations and for monitoring and ensuring the implementation of the recommendations.	Privacy Audit Policy- s. 4.1, 4.2
	• must set out the nature of the documentation that must be completed, provided and/or executed at the conclusion of the privacy audit, including the agent(s) responsible for completing, providing and/or executing the documentation, the agent(s) to whom the documentation must be provided and the required content of the documentation.	Privacy Audit Policy- s. 5.1, 5.2
	• must address the manner and format in which the findings of privacy audits, including the recommendations arising from the privacy audits and the status of addressing the recommendations, are communicated. This shall include a discussion of the agent(s) responsible for communicating the findings of the privacy audit; the mechanism and format for communicating the findings of the privacy audit; the time frame within which the findings of the privacy audit must be communicated; and to whom the findings of the privacy audit will be communicated, including the Chief Executive Officer or the Executive Director.	Privacy Audit Policy- s. 6.1, 6.2, 6.3, 6.4
	• must further require that a log be maintained of privacy audits and must identify the agent(s) responsible for maintaining the log and for tracking that the recommendations arising from the privacy audits are addressed within the identified time frame. They should further address where documentation	Privacy Audit Policy- s. 7.1, 7.2

	related to privacy audits will be retained and the agent(s) responsible for retaining this documentation.	
	• must require the agent(s) responsible for conducting the privacy audit to notify the prescribed person or prescribed entity, at the first reasonable opportunity, of a privacy breach or suspected privacy breach in accordance with the *Policy and Procedures for Privacy Breach Management* and of an information security breach or suspected information security breach in accordance with the *Policy and Procedures for Information Security Breach Management.*	Privacy Audit Policy- s. 8.1

Recommendation 11: It is recommended that CIHI amend its Policy and Procedures for Privacy Breach Management and Policy and Procedures for Information Security Breach Management to clearly define "privacy breach" and "information security breach" and address each requirement set out in the Manual.

(To be addressed separately)

Recommendation 12: It is recommended that CIHI's Policy and Procedures for Secure Retention of Records of Personal Health Information be amended to identify the agent(s) responsible for ensuring the secure retention of records of personal health information, require agents to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal and identify the reasonable steps that must be taken by agents as required in the Manual.

CIHI Response:

5. Policy and Procedures for Secure Retention of Records of Personal	• must be developed and implemented with respect to the secure retention of records of personal health information in paper and electronic format.	Standard: Secure Information Storage
	• must identify the retention period for records of personal health information in both paper and electronic format, including various categories thereof. For records of personal health information used for research purposes, the prescribed person or prescribed entity must ensure that the records of personal health information are not being retained for a period longer than	Privacy Policy- s.6; Privacy and Security Framework- s. 4d

Health Information	that set out in the written research plan approved by a research ethics board. For records of personal health information collected pursuant to a Data Sharing Agreement, the policy and procedures must prohibit the records from being retained for a period longer than that set out in the Data Sharing Agreement. In any event, the policy and procedures must mandate that records of personal health information be retained for only as long as necessary to fulfill the purposes for which the personal health information was collected.	
	• must require the records of personal health information to be retained in a secure manner and must identify the agent(s) responsible for ensuring the secure retention of these records. In this regard, the policy and procedures must identify the precise methods by which records of personal health information in paper and electronic format are to be securely retained, including records retained on various media.	Standard: Secure Information Storage- Definition of "Staff" + rest of document ss. 2.0, 5.0, 6.0
	• must require agents of the prescribed person or prescribed entity to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure and to ensure that records of personal health information are protected against unauthorized copying, modification or disposal. The reasonable steps that must be taken by agents shall also be outlined in the policy and procedures.	Standard: Secure Information Storage- s. 2.1
	• if a third party service provider is contracted to retain records of personal health information on behalf of the prescribed person or prescribed entity, the policy and procedures must also address the following additional matters:	Competitive and Non Competitive Procurement Procedure- s. 7
	• must address the circumstances in which and the purposes for which records of personal health information will be transferred to the third party service provider for secure retention. They must detail the procedure to be followed in securely transferring the records of personal health information to the third party service provider and in securely retrieving the records from the third party service provider, including the secure manner in which the records will be transferred and retrieved, the conditions pursuant to which the records will be transferred and retrieved and the agent(s) responsible for ensuring the secure transfer and retrieval of the records. In this regard, the procedures shall comply with	Competitive and Non Competitive Procurement Procedure- s. 7

	the Policy and Procedures for Secure Transfer of Records of Personal Health Information.	
	• must address the documentation that is required to be maintained in relation to the transfer of records of personal health information to the third party service provider for secure retention. In particular, the policy and procedures must require the agent(s) responsible for ensuring the secure transfer to document the date, time and mode of transfer and to maintain a repository of written confirmations received from the third party service provider upon receipt of the records of personal health information.	Competitive and Non Competitive Procrement Procedure- s. 7
	• must require a detailed inventory to be maintained of records of personal health information being securely retained by the third party service provider and of records of personal health information retrieved by the prescribed person or prescribed entity and must identify the agent(s) responsible for maintaining the detailed inventory.	Standard: Secure Information Storage s. 3.3- See comment s. 1.0
	• where a third party service provider is contracted to retain records of personal health information, the policy and procedures must require that a written agreement be executed with the third party service provider containing the relevant language from the Template Agreement For All Third Party Service Providers, and must identify the agent(s) responsible for ensuring that the agreement has been executed prior to transferring the records of personal health information for secure retention.	Competitive and Non Competitive Procurement Procedure- s. 7
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Standard: Secure Information Storage- s.7
	• must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Standard: Secure Information Storage- s. 7
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures	Standard: Secure Information Storage- s. 7

	for Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	

Recommendation 13: It is recommended that CIHI's Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices be amended to address each requirement set out in the Manual.

CIHI Response:

6. Policy and Procedures for Secure Retention of Records of Personal Health Information on Mobile Devices	• must be developed and implemented to identify whether and in what circumstances, if any, the prescribed person or prescribed entity permits personal health information to be retained on a mobile device. In this regard, the policy and procedures shall provide a definition of "mobile device."	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- "Definitions" at page 2
	• in drafting, it is recommended that the prescribed person or prescribed entity have regard to orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-004 and Order HO-007; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 12: Encrypting Personal Health Information on Mobile Devices, Fact Sheet 14: Wireless Communication Technologies: Safeguarding Privacy and Security and Safeguarding Privacy in a Mobile Workplace.	Privacy and Security Framework – s. 4a.
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- s. 4
	• must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- s. 4
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for	Policy on the Security of Confidential Information and

	Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Use of Mobile Devices/ Removable Media- s. 4
	Where Personal Health Information is Permitted to be Retained on a Mobile Device	
	• if the prescribed person or prescribed entity permits personal health information to be retained on a mobile device, the policy and procedures must set out the circumstances in which this is permitted.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- ss. 2.0 – 3.0 CIHI prohibits the retention of personal health information, health workforce personal information and de-identified data on mobile devices.
	Approval Process	
	• must state whether approval is required prior to retaining personal health information on a mobile device.	N/A
	• if approval is required, the policy and procedures must identify the process that must be followed and the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for the retention of personal health information on a mobile device. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	N/A
	• must further address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for the retention of personal health information on a mobile device.	N/A
	• prior to any approval of a request to retain personal health information on a mobile device, the policy and procedures must require the agent(s)	N/A

	responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose. The policy and procedures must also require the agent(s) responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to the Policy and Procedures for Limiting Agent Access to Personal Health Information.	
	• should set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	N/A
	Conditions or Restrictions on the Retention of Personal Health Information on a Mobile Device	
	• must require mobile devices containing personal health information to be encrypted as well as password-protected using strong and complex passwords that are in compliance with the Policy and Procedures Relating to Passwords.	N/A
	• Where mobile devices have display screens, the policy and procedures must further require that a mandatory standardized password-protected screen saver be enabled after a defined period of inactivity. The agent(s) responsible for encrypting mobile devices and for ensuring that the mandatory standardized password-protected screen saver is enabled shall also be identified.	N/A
	• must identify the conditions or restrictions with which agents granted approval to retain personal health information on a mobile device must comply. At a minimum, the agents must:	N/A
	• be prohibited from retaining personal health information on a mobile device if other information, such as de-identified and/or aggregate information, will serve the purpose;	N/A

	• de-identify the personal health information to the fullest extent possible;	N/A
	• be prohibited from retaining more personal health information on a mobile device than is reasonably necessary for the identified purpose;	N/A
	• be prohibited from retaining personal health information on a mobile device for longer than necessary to meet the identified purpose;	N/A
	• ensure that the strong and complex password for the mobile device is different from the strong and complex passwords for the files containing the personal health information and that the password is supported by "defence in depth" measures.	N/A
	• must detail the steps that must be taken by agents to protect the personal health information retained on a mobile device against theft, loss and unauthorized use or disclosure and to protect the records of personal health information retained on a mobile device against unauthorized copying, modification or disposal.	N/A
	• must require agents to retain the personal health information on a mobile device in compliance with the Policy and Procedures for Secure Retention of Records of Personal Health Information and to securely delete personal health information retained on a mobile device in accordance with the process and in compliance with the time frame outlined in the policy and procedures.	N/A
	Where Personal Health Information is not Permitted to be Retained on a Mobile Device	
	• if the prescribed person or prescribed entity does not permit personal health information to be retained on a mobile device, the policy and procedures must expressly prohibit the retention of personal health information on a mobile device and must indicate whether or not personal health information may be accessed remotely through a secure connection or virtual private network.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- ss. 2.0 – 3.0

	• if the prescribed person or prescribed entity permits personal health information to be accessed remotely, the policy and procedures must set out the circumstances in which this is permitted.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- s. 3.0
	Approval Process	
	• must identify whether approval is required prior to accessing personal health information remotely through a secure connection or virtual private network.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- s. 3.0
	• if approval is required, must identify the process that must be followed and the agent(s) responsible for receiving, reviewing and determining whether to approve or deny a request for remote access to personal health information. This shall include a discussion of any documentation that must be completed, provided and/or executed; the agent(s) responsible for completing, providing and/or executing the documentation; the agent(s) to whom this documentation must be provided; and the required content of the documentation.	N/A – approval not required
	• must address the requirements that must be satisfied and the criteria that must be considered by the agent(s) responsible for determining whether to approve or deny a request for the retention of personal health information on a mobile device.	N/A – approval not required
	• prior to any approval of a request to retain personal health information on a mobile device, the policy and procedures must require the agent(s) responsible for determining whether to approve or deny the request to ensure that other information, namely de-identified and/or aggregate information, will not serve the identified purpose and that no more personal health information will be retained on the mobile device than is reasonably necessary to meet the identified purpose.	N/A – approval not required
	• must also require the agent(s) responsible for determining whether to approve or deny the request to ensure that the use of the personal health information has been approved pursuant to the Policy and Procedures for Limiting Agent Access to Personal Health Information.	N/A – approval not required

	• should set out the manner in which the decision approving or denying the request is documented; the method by which and the format in which the decision will be communicated; and to whom the decision will be communicated.	N/A – approval not required
	Conditions or Restrictions on the Remote Access to Personal Health Information	
	• must identify the conditions or restrictions with which agents granted approval to access personal health information remotely must comply. At a minimum, the agents must be prohibited from remotely accessing personal health information if other information, such as de-identified and/or aggregate information, will serve the purpose and from remotely accessing more personal health information than is reasonably necessary for the identified purpose. The policy and procedures must also set out the administrative, technical and physical safeguards that must be implemented by agents in remotely accessing personal health information.	Policy on the Security of Confidential Information and Use of Mobile Devices/ Removable Media- s. 3.0

Recommendation 14: It is recommended that CIHI's Policy and Procedures for Secure Transfer of Records of Personal Health Information be amended to address the manner of obtaining and recording acknowledgement of receipt of the records of personal health information transferred as required in the Manual.

CIHI response:

7. Policy and Procedures for Secure Transfer of Records of Personal Health Information	• must be developed and implemented with respect to the secure transfer of records of personal health information in paper and electronic format.	Secure Information Transfer Standard
	• shall require records of personal health information to be transferred in a secure manner and shall set out the secure methods of transferring records of personal health information in paper and electronic format that have been approved by the prescribed person or prescribed entity.	Secure Information Transfer Standard- pg. 3
	• shall require agents to use the approved methods of transferring records of personal health information and shall prohibit all other methods.	Secure Information Transfer Standard- pg. 3
	• procedures that must be followed in transferring records of personal health information through each of the approved methods must also be outlined. This shall include a discussion of the conditions pursuant to which records of personal health information will be transferred; the agent(s) responsible for ensuring the secure transfer; any documentation that is required to be completed, provided and/or executed in relation to the secure transfer; the agent(s) responsible for completing, providing and/or executing the documentation; and the required content of the documentation.	Secure Information Transfer Standard- pg. 3-4
	• must address whether the agent transferring records of personal health information is required to document the date, time and mode of transfer; the recipient of the records of personal health information; and the nature of the records of personal health information transferred. Further, the policy and procedures must address whether confirmation of receipt of the records of personal health information is required from the recipient, and if so, the manner of obtaining and recording acknowledgement of receipt of the records of personal health information and the agent(s) responsible for doing so.	Secure Information Transfer Standard- pg. 4
	• the administrative, technical and physical safeguards that must be implemented by agents in transferring records of personal health information through each of the approved methods must also be outlined in order to	Secure Information Transfer Standard- pg. 3-4

	ensure that the records of personal health information are transferred in a secure manner.	
	• the prescribed person or prescribed entity must ensure that the approved methods of securely transferring records of personal health information and the procedures and safeguards that are required to be implemented in respect of the secure transfer of records of personal health information are consistent with:	Privacy and Security Framework, s. 4a.
	• orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including but not limited to Order HO-004 and Order HO-007;	
	• guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario, including Privacy Protection Principles for Electronic Mail Systems and Guidelines on Facsimile Transmission Security; and	
	• evolving privacy and security standards and best practices.	
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Secure Information Transfer Standard- pg. 6, Compliance Audit and Enforcment
	• must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Secure Information Transfer Standard- pg. 6, Compliance Audit and Enforcment
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Secure Information Transfer Standard- pg. 6, Compliance Audit and Enforcment

Recommendation 15: It is recommended that CIHI's Policy and Procedures for Secure Disposal of Records of Personal Health Information be amended to address each requirement set out in the Manual.

CIHI Response:

8. Policy and Procedures for Secure Disposal of Records of Personal Health Information	• must be developed and implemented with respect to the secure disposal of records of personal health information in both paper and electronic format in order to ensure that reconstruction of these records is not reasonably foreseeable in the circumstances.	Secure Destruction Policy, Scope, s. 1.1
	• must require records of personal health information to be disposed of in a secure manner and must provide a definition of secure disposal that is consistent with the Act and its regulation.	Secure Destruction Policy, Scope, s. 1.1
	• must identify the precise method by which records of personal health information in paper format are required to be securely disposed of and the precise method by which records of personal health information in electronic format, including records retained on various media, are required to be securely disposed of.	Secure Destruction Standard, s. 7.0
	• in addressing the precise method by which records of personal health information in paper and electronic format must be securely disposed of, the prescribed person or prescribed entity must ensure that the method of secure disposal adopted is consistent with the Act and its regulation; with orders issued by the Information and Privacy Commissioner of Ontario under the Act and its regulation, including Order HO-001 and Order HO-006; and with guidelines, fact sheets and best practices issued by the Information and Privacy Commissioner of Ontario pursuant to the Act and its regulation, including Fact Sheet 10: Secure Destruction of Personal Information.	Privacy and Security Framework, s. 4a.
	• must address the secure retention of records of personal health information pending their secure disposal in accordance with the Policy and Procedures for Secure Retention of Records of Personal Health Information.	Secure Destruction Policy- s. 4.0
	• must require the physical segregation of records of personal health information intended for secure disposal from other records intended for recycling, must require that an area be designated for the secure retention of records of personal health information pending their secure disposal and must require the records of personal health information to be retained in a	Secure Destruction Policy- s. 5.0

	clearly marked and locked container pending their secure disposal. The policy and procedures must also identify the agent(s) responsible for ensuring the secure retention of records of personal health information pending their secure disposal.	
	• in the event that records of personal health information or certain categories of records of personal health information will be securely disposed of by a designated agent, who is not a third party service provider, the policy and procedures must identify the designated agent responsible for securely disposing of the records of personal health information; the responsibilities of the designated agent in securely disposing of the records; and the time frame within which, the circumstances in which and the conditions pursuant to which the records of personal health information must be securely disposed of. The policy and procedures must also require the designated agent to provide a certificate of destruction:	Secure Destruction Policy- s. 2.0 and 3.0
	• identifying the records of personal health information to be securely disposed of;	Secure Information Destruction Standard – s.9.0
	• confirming the secure disposal of the records of personal health information;	Secure Information Destruction Standard – s.9.0
	• setting out the date, time and method of secure disposal employed; and	Secure Information Destruction Standard - s.9.1
	• bearing the name and signature of the agent(s) who performed the secure disposal.	Secure Information Destruction Standard - s.9.1
	• the time frame within which and the agent(s) to whom certificates of destruction must be provided following the secure disposal of the records of personal health information must also be addressed in the policy and procedures.	Secure Information Destruction Standard – s.9.4
	• in the event that records of personal health information or certain categories of records of personal health information will be securely disposed of by an agent that is a third party service provider, the policy and procedures must address the following additional matters:	Secure Destruction Policy- s. 6.0

	• must detail the procedure to be followed by the prescribed person or prescribed entity in securely transferring the records of personal health information to the third party service provider for secure disposal. At a minimum, the policy and procedures must identify the secure manner in which the records of personal health information will be transferred to the third party service provider, the conditions pursuant to which the records will be transferred and the agent(s) responsible for ensuring the secure transfer of the records. In this regard, the policy and procedures shall comply with the Policy and Procedures for Secure Transfer of Records of Personal Health Information.	Secure Information Destruction Standard N/A see section 10.1
	• must require the agent(s) responsible for ensuring the secure transfer of records of personal health information to document the date, time and mode of transfer of the records of personal health information and to maintain a repository of written confirmations received from the third party service provider evidencing receipt of the records of personal health information. A detailed inventory related to the records of personal health information transferred to the third party service provider for secure disposal must also be maintained and the policy and procedures must identify the agent(s) responsible for maintaining this inventory.	Secure Information Destruction Standard N/A see section 10.1
	• where a third party service provider is retained to securely dispose of records of personal health information, the policy and procedures must require that a written agreement be executed with the third party service provider containing the relevant language from the Template Agreement For All Third Party Service Providers, and must identify the agent(s) responsible for ensuring that the agreement has been executed prior to the transfer of records of personal health information for secure disposal.	Secure Destruction Policy See section 6.0 Requirements for External Parties Contracted by CIHI in CIHI's Secure Destruction Policy
	• must outline the procedure to be followed in tracking the dates that records of personal health information are transferred for secure disposal and the dates that certificates of destruction are received, whether from the third party service provider or from the designated agent that is not a third party service provider, and the agent(s) responsible for conducting such tracking. Further, the policy and procedures must outline the process to be followed where a certificate of destruction is not received within the time set out in the policy and its procedures or within the time set out in the agreement with the third party service provider and the agent(s) responsible for implementing this process.	Secure Information Destruction Standard See sections 9 and 10

	• recommended that the policy and procedures address where certificates of destruction will be retained and the agent(s) responsible for retaining the certificates of destruction.	Standard Information Destruction Standard See section 9.2 Certificates of destruction are to be maintained as an official record of CIHI on the ISMS site and retained accordingly in CIHI's Secure Information Destruction Standard
	• the prescribed person or prescribed entity must require agents to comply with the policy and its procedures and must address how and by whom compliance will be enforced and the consequences of breach.	Secure Destruction Policy- s. 7.0
	• must stipulate that compliance will be audited in accordance with the Policy and Procedures In Respect of Security Audits, must set out the frequency with which the policy and procedures will be audited and must identify the agent(s) responsible for conducting the audit and for ensuring compliance with the policy and its procedures.	Secure Destruction Policy- s.7.0
	• must require agents to notify the prescribed person or prescribed entity at the first reasonable opportunity, in accordance with the Policy and Procedures for Information Security Breach Management, if an agent breaches or believes there may have been a breach of this policy or its procedures.	Secure Destruction Policy- s.7.0

Recommendation 16: It is recommended that CIHI ensure that all information systems, technologies, applications and programs involving personal health information have the functionality to log access, use, modification and disclosure of personal health information as required by the Manual when adding or replacing information systems, technologies, applications and programs involving personal health information.

CIHI Response: Over the past three years, all new business applications have been built on our legacy technology base (at the same level of compliance as our existing systems) and not on new technologies.

Recommendation 17: It is recommended that CIHI ensure, and that its Policy and Procedure for Maintaining and Reviewing System Control and Audit Logs require that its system control and audit logs are immutable.

CIHI Response:

• must require the system control and audit logs to be immutable, that is, the prescribed person or prescribed entity must be required to ensure that the system control and audit logs cannot be accessed by unauthorized persons or amended or deleted in any way.	Policy on the Maintenance of System Control and Audit Logs- s. 1.5, 1.6

Recommendation 18: It is recommended that CIHI's Policy and Procedures for the Execution of Confidentiality Agreements by Agents be amended to outline the process that must be followed where an executed confidentiality agreement is not received within a defined period as required by the Manual.

CIHI Response: See new Policy for the Execution of Confidentiality Agreements, s. 1.1 and 1.3, 2.1, 2.2

Recommendation 19: It is recommended that CIHI's Policy and Procedures for Termination or Cessation of the Employment or Contractual Relationship be amended to provide a definition of "property" in compliance with the requirements of the Manual.

CIHI Response: Definition of "property" included in Offboarding Checklist

Recommendation 20: It is recommended that CIHI ensure that the Board of Directors is advised of the results of and any recommendations arising from investigations of any privacy breaches, information security breaches, and privacy complaints that are investigated, and the status of implementation of the recommendations.

CIHI response:

The Board of Directors is advised of any privacy breaches, information security breaches and privacy complaints that were investigated, including the results of and any recommendations arising from these investigations and the status of

implementation of the recommendations. See section xx of the Privacy and Security Incident Management Protocol and section 64.8 of the Privacy Policy Procedures.

Recommendation 21: It is recommended that CIHI ensure that its reporting of indicators related to statements of purpose for data holdings containing personal health information and privacy impact assessments is provided in full compliance with the Manual at the start of the next review period.

CIHI response: Indicators updated to comply with this requirement

Recommendation 22: It is recommended that CIHI ensure that its privacy impact assessments are reviewed annually, as required by CIHI's Privacy Impact Assessment Policy.

CIHI response: Indicators updated to comply with this requirement

Appendix G — CIHI'S Security Audit Program

Fiscal Year: 2020-2021

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third-Party Vulnerability Assessment and Penetration Test Through external internet penetration testing and internal system vulnerability testing (DMZ perimeter and internal LAN), ensure: • CIHI's security architecture is well designed and provides protection from external intruders, • CIHI's security infrastructure guarding CIHI's LAN/WAN network provides protection and robust security and, The confidentiality, integrity and availability of CIHI's electronic information assets are protected. **Key activities – External:** • Perform exploratory vulnerability scanning across multiple "Class C" CIHI addresses • Penetration test of up to 12 targeted IPs **Key activities – Internal:** • Assessment of 250 servers and 1000 workstations Conducted November 2020	**External Penetration Test:** • 12 recommendations **Network Vulnerability Scan** • 1 recommendation **Social Engineering** • 2 recommendations **Network Security Assessment** • 24 recommendations Due to the sensitive nature of the recommendations, they will not be articulated in this report.	Addressed/Completed or In-Progress	External Pen Test: • Feb 2021 • Jan 2022 • Nov 2020 • Nov 2020 • June 2021 • March 2023 • April 2021 • Nov 2020 • Dec 2020 • Nov 2020 • March 2023 Network Security Assessment • Dec 2020 • Dec 2020 • April 2021 • Nov 2021 • Jan 2021 • Nov 2020 • Jan 2021 • Nov 2020 • Jan 2021 • Dec 2020- • Dec 2020 • June 2021 • Dec 2020 • Nov 2020 • Nov 2020 • Dec 2021 • Nov 2020 • Nov 2020 • Dec 2021 • Dec 2021 • Nov 2021 • Jan 2021 • Jan 2021 • Nov 2021

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
			Network Vulnerability Scan • Dec 2020 Social Engineering • Jan 2021 • Jan 2021

Fiscal Year: 2021-2022

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
External Third Party Vulnerability Assessment and Penetration Test Through external internet penetration testing and internal system vulnerability testing (DMZ perimeter and internal LAN), ensure: • CIHI's security architecture is well designed and provides protection from external intruders, • CIHI's security infrastructure guarding CIHI's LAN/WAN network provides protection and robust security and, The confidentiality, integrity and availability of CIHI's electronic information assets are protected. **Key activities – External:** • Perform exploratory vulnerability scanning across multiple "Class C" CIHI addresses • Penetration test of up to 12 targeted IPs **Key activities – Internal:** • Assessment of 250 servers and 1000 workstations Conducted October 2021	Internal/External Assessment Report: • 33 recommendations Social Engineering • 1 recommendation Due to the sensitive nature of the recommendations, they will not be articulated in this report.	Addressed/Completed	Internal/External Assessment: 1. Jan 2022 2. March 2022 3. Jan 2022 4. Feb 2022 5. June 2022 6. Feb 2022 7. March 2023 8. March 2022 9. Jan 2022 10. May 2022 11. Dec 2021 12. Jan 2022 13. Jan 2022 14. Feb 2022 15. March 2023 16. Jan 2022 17. Jan 2022 18. Jan 2022 19. March 2023 20. Dec 2021 21. Dec 2021 22. Dec 2021 23. Dec 2021 24. March 2023 25. March 2023 26. March 2022 27. Dec 2021 28. Jan 2022 29. June 2022 30. March 2023 31. May 2022 32. June 2022 33. March 2022 Social Engineering 1. Jan 2022

Fiscal Year: Ongoing regular audits

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
Database Security Audit Monthly database security audit to examine all instances of inappropriate sharing of accounts and excessive failed login attempts to CIHI databases for potential security threats. The audit also examines all the current database connections for any potential security implications.	N/A	N/A	N/A
Yearly Internal Data Access Audit Yearly internal data access audit to ensure only authorized staff have access to PHI in CIHI's analytical environment. The audit identifies all individuals who have access to data in CIHI's analytical environment and requires management to formally request continued access or removal for each employee, as appropriate. Completed: 2020 – Feb to April 2021 – Feb to April 2022 – Feb to April	N/A	N/A	N/A
Local Administrator Audit Internal audit of local administrator user access to desktop and laptop computers. For any unapproved administrator rights that are discovered, an Incident is opened and the administrator privileges are removed.	N/A	N/A	N/A

Description of Audit	Description of Recommendation	Manner Addressed	Completion Date
ISO/IEC 27001:2013 Surveillance / Recertification Audit The ISO/IEC 27001:2013 is conducted on an annual basis as required by the standard. The purpose of this audit is to ensure CIHI continues to meet the requirements of the Standard and continues to maintain its certification. Conducted in July of each fiscal year.	2020-2021 Audit - 2 Findings 2021-2022 Audit - 3 Findings 2022-2023 Audit - 2 Findings	Completed/Addressed	2020-2021 1. June 2020 2. June 2020 2021-2022 1. October 2021 2. August 2021 3. August 2021 2022-2023 All findings to be addressed June 2023
ISMS Internal Audit The ISMS Internal Audit is conducted on an annual basis as required by the ISO/IEC 27001:2013 standard. An external party is procured to execute this audit on behalf of CIHI. The purpose of the ISMS Internal Audit is to ensure that CIHI's ISMS conforms to the requirements of the ISO/IEC 27001:2013 standard and that it is effectively implemented and maintained. Conducted in May of each fiscal year.	2020-2021 Audit – 5 2021-2022 Audit – 7 2022-2023 Audit – 8	Completed/Addressed	2020-2021 1. July 2020 2. September 2020 3. September 2020 4. May 2020 5. August 2020 2021-2022 1. August 2021 2. September 2021 3. November 2021 4. June 2021 5. August 2021 6. September 2021 7. October 2023 – **Proposed completion date** 2022-2023 1. December 2023-**Proposed completion date** 2. June 2023 – **Proposed completion date** 3. December 2022 4. December 2022 5. December 2022 6. December 2022 7. December 2022 8. December 2022

Appendix H — InfoSec Staff Awareness, Education and Communication Log

Date	Provider	Attendees	Subject
2020-01-06	Internal	All CIHI Staff	January is Privacy Awareness Month
2020-01-30	CISO & PLS	All CIHI Staff	Privacy and Security by Design (PSbD)
2020-02-10	CISO	All CIHI Staff	Phishing email
2020-03-18	CISO	All CIHI Staff	Important information about maintaining Privacy and Security while working from home
2020-05-15	Cal Marcoux & Rhonda Wing	All CIHI Staff	Important Privacy and Security information about Microsoft Teams
2020-05-21	InfoSec and PLS	All CIHI Staff	Privacy and Security Phishing Awareness Challenge
2020-06-19	CISO & PLS	All CIHI Staff	COVID-19 Contact Tracing App Email
2020-08-31	CISO	All CIHI Staff	Information Security Awareness Month – Opening Article
2020-09-07	CISO	All CIHI Staff	Information Security Awareness Month – Article 2 on Records Management During Changing Times
2020-09-14	CISO	All CIHI Staff	Information Security Awareness Month – Article 3 on Privacy and Security When Working from Home
2020-09-21	CISO	All CIHI Staff	Information Security Awareness Month – Article 4 on Awareness on testing accounts from CES team
2020-09-22	CISO	All CIHI Staff	Employee Session – One-hour Teams Live Session on Working from Home
2020-09-28	CISO	All CIHI Staff	Information Security Awareness Month – Closing Article
2020-09-28	CISO	To first 150 requests	Kaspersky Licenses

Date	Provider	Attendees	Subject
2020-11-19	InfoSec	Security Group	Using the same password for your regular and admin account
2021-01-04	Internal	All CIHI Staff	January is Privacy Awareness Month
2021-04-12	PLS & CISO	ITSPD	Discuss Privacy and Security Framework
2021-06-21	InfoSec	All CIHI Staff	Phishing Article
2021-09-01	InfoSec	All CIHI Staff	Information Security Month
September 2021	CISO & PLS	All CIHI Staff	Demonstrable Accountability Sessions
2021-12-13	CISO	All Managers, Directors and Executives	Cybersecurity threat unfolding emails
2022-01-12	CPO/CISO	DL - All Staff	Privacy Awareness Campaign: Privacy and Security guidance related to working from home
2022-01-03	Internal	All CIHI Staff	January is Privacy Awareness Month
2022-01-10	Internal	All CIHI Staff	Privacy Awareness Month – Training Instructions
2022-01-17	Internal	All CIHI Staff	Privacy Awareness Month – PTA Spotlight: Pause
2022-01-17	Internal	All CIHI Staff	Privacy Awareness Month – Requirements when sharing externally with OneDrive
2022-01-24	Internal	All CIHI Staff	Privacy Awareness Month – Protecting your own confidential information
2022-01-24	Internal	All CIHI Staff	Privacy Awareness Month – PTA Spotlight: Think
2022-01-31	Internal	All CIHI Staff	Privacy Awareness Month – PTA Spotlight: Act
2022-02-07	Internal	All CIHI Staff	Homewood Health Privacy Incident
2022-02-07	Internal	All CIHI Staff	Be aware: The hang-up delay scan could cost you!
2022-02-07	Internal	All CIHI Staff	Another successful Privacy Awareness Month!

Date	Provider	Attendees	Subject
2022-05-09	InfoSec	All CIHI Staff	New Security Applications upgrade
2022-05-30	InfoSec	All CIHI Staff	Endpoint security software upgrade