2.0 Requirements of privacy audits

2.1 The nature and scope of privacy audits will be determined in accordance with CIHI's Multi-Year Privacy Audit Plan. Privacy audits may include in-person visits (including remote site visits), inspections, document reviews and interviews, as CIHI sees fit.

2.2 The scope of third-party privacy audits will include the principal organization and the IT services organization(s), as applicable.

2.3 Privacy audits will be conducted by CIHI's Privacy and Legal Services staff or by staff contracted to perform the privacy audit, in collaboration with CIHI's Information Security department as required.

2.4 Privacy audits will be conducted in accordance with the audit schedule presented in CIHI's Multi-Year Privacy Audit Plan or on an ad hoc basis in response to emergent privacy and security risks (e.g., incident and breach response processes), or in response to external factors such as an investigation, recommendation or order from a privacy commissioner/ombudsperson.

3.0 Privacy audit process

3.1 Criteria considered in selecting the subject matter of internal privacy audits include assessment information arising from compliance with CIHI's *Privacy Impact Assessment Policy*, *Policy on Privacy and Security Risk Management* and *Privacy and Security Incident Management Protocol*, or from external factors such as an investigation, recommendation or order from a privacy commissioner/ombudsperson. Criteria considered in selecting the subject matter of third-party privacy audits will be described in CIHI's Multi-Year Privacy Audit Plan and will include, for example, proposed changes in the use of data disclosed to a third party, the complexity of project data management, disclosure of personal health information, and CIHI's assessment of sources of current and

3.3 Notification of a privacy audit will be issued in writing, in accordance with the associated agreement where applicable, and will include the policy or contractual basis for conducting the audit, the contact information of the CIHI staff conducting the audit, the nature and scope of the audit, potential participants to be included in any audit-related interviews or inspections, and the proposed timing for the audit.

3.4 Documentation will be created, received and maintained in the format required by the chief privacy officer as evidence of the administration and operations of CIHI's privacy audits and/or to support legal obligations. Such documentation will include lists of audit participants present for meetings, records of site visits and inspections, audit assessment questionnaires developed and utilized for the purpose of conducting the audit, documentation submitted or collected for the purpose of conducting the audit, written confirmations of acceptance and internal approval, the final audit report and recommendations arising from the audit.

3.5 CIHI staff conducting a privacy audit are responsible for completing privacy audit documentation as required. Privacy audit documentation is maintained by CIHI's Privacy and Legal Services department.

3.6 Upon completion of a privacy audit, an audit report in the format required by the chief privacy officer will be provided to the auditee. For internal privacy audits, an audit report will be provided to CIHI staff in the accountable area who are in a position of director or above. For third-party privacy audits, an audit report will be provided to an individual able to bind the principal organization and/or IT services organization(s).

4.0 Addressing recommendations arising from privacy audits

4.1 Staff conducting a privacy audit will identify the primary contact of the auditee who is responsible for addressing recommendations arising from the privacy audit, determine the associated timelines for addressing the recommendations and obtain confirmation in writing from the auditee of acceptance of the audit report and recommendations.

4.2 Staff conducting an internal privacy audit will obtain acceptance of the audit report and recommendations from an individual in a position of director or above. Once the recommendations are accepted, the Privacy and Legal Services department is responsible for ensuring all recommendations are entered into the Privacy Recommendation Log, and then into CIHI's Master Log of Action Plans. Internal owners of a recommendation are responsible for providing regular updates/presentations to CIHI's Senior Management Committee. These updates will be provided until the recommendations are fully implemented.