Under the *Health Information Act* (HIA), custodians and their information managers must take reasonable steps to protect health information against threats to confidentiality or security in **electronic health record (EHR) systems**, including unauthorized access, use, disclosure, modification or loss of health information.

Purposes

This document is meant for custodians and their information managers (i.e. EHR service providers) to assess the safeguards in EHR systems.

Specifically, you may use this document for the following three purposes:

- To assess whether EHR systems comply with HIA and meet the OIPC's expectations for protecting health information with reasonable safeguards.
- To support the submission of a **Privacy Impact Assessment (PIA)** on an EHR system to the Office of the Information and Privacy Commissioner (OIPC). OIPC staff assigned to review a custodian's PIA may ask that a gap analysis against these guidelines be completed if further information is needed to complete a PIA review.
- To prepare PIA amendments or for continuous improvement to ensure upgrades or changes to systems comply with HIA requirements.

This guidance may be used voluntarily to assess your EHR. It does not replace the OIPC's PIA Requirements or Alberta Health's **Provincial Organizational Readiness Assessment** (pORA), which are both mandatory under HIA.

When using this guidance, you will likely need to work with your EHR service provider (i.e. information manager) to fully understand and complete an assessment.

This document is an administrative tool intended to assist custodians in understanding the *Health Information Act* (HIA). This document is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of HIA, please read the Act and its regulation in their entirety. This document is not binding on the Office of the Information and Privacy Commissioner of Alberta.

Assessment of System Safeguards

In the tables below, describe how you meet the HIA requirements using the sample practices as a guide. The samples are based on the OIPC's observations of successfully implemented EHR systems in Alberta's health sector.

Custodian:

Information Manager:

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
A brief description with applicable sections in HIA.	Examples of practices associated with the HIA requirement. You may take other reasonable steps to meet the requirement.	Steps you have taken to meet HIA requirements, such as technical, physical and/or administrative safeguards.

Privacy Accountability

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
This is a broad requirement that sets out privacy roles and accountability for the custodian. • HIA sections 62 and 63 • *Health Information Regulation* section 8	A governance and accountability structure is created that establishes: • A written access and privacy policy that sets out the custodian's direction on HIA compliance. • Who the custodian has made responsible for HIA compliance and the reporting relationship between that role and the custodian. • The duties and role of privacy/security officer. • How system users confirm their understanding and agreement with the custodian's policies and procedures related to the privacy and security of health information. • Privacy statements or reminders are included on system screens. • Training and awareness. • Response plans for privacy breaches. • The system provides reporting mechanisms for privacy management, such as audit and disclosure logs.	

Access to Health Information

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must respond to requests from individuals for access to their health information within the legislated timeframe. Custodians must be able to respond to reviews of their decisions regarding access. • HIA part 2 • *Health Information Regulation* section 10(1)	• A process is in place to determine if the system holds or controls information about the requestor. • Requests for access to information are recorded and tracked. • Processes are in place to assist custodians in preparing documents related to an access request for release, including providing fee estimates and any redaction.	

Correction Requests

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
HIA allows individuals to request corrections or amendments to health information held by the custodian. Custodians must decide whether to make the requested correction and be able to respond to reviews of their decisions. HIA imposes duties on custodians to make others aware of any corrections made. Individuals may opt to submit a statement of disagreement to be attached to the record in question. • HIA sections 13 and 14	• Processes are in place to allow individuals to request corrections to their health information. • Correction requests are logged and steps taken to address the request. • Date and time are recorded when changes to health information are made. • A statement of disagreement can be attached to records if required. • A record is kept when a request for correction was received and was not accepted by the custodian (i.e. no change was made). • Corrected or annotated records are permanently retained with the original records along with an explanation of why the record was changed.	

Training, Awareness and Sanctions

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
A custodian must ensure that all of its affiliates are aware of and adhere to the custodian's administrative, technical and physical safeguards in respect of health information. • *Health Information Regulation* section 8	• Regular training is provided to all system users. This training is reviewed and updated to reflect current legislative, regulatory, industry, and entity policy and procedure requirements. • Training is also provided when there are system changes and upgrades.	

Collection of Health Information Limitation

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Only essential health information must be collected whether under HIA or other relevant legislation. • HIA part 3	• The system is designed or configured to collect only the health information essential to meet the intended purpose. • Fields, drop down menus, etc. limit collection of health information to what is essential.	

Use of Health Information Limitation

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
The concept of use includes appropriate and controlled access to and sharing of health information within a custodian's organization. • HIA part 4	• The system is designed or configured to only allow access to the least amount of information essential to meet the intended purpose and such access should be based on a need-to-know (e.g. it could implement role-based access control, Personal Health Number-based access, white lists, black lists, etc.)	

Disclosures of Health Information and Expressed Wishes

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
An expressed wish is described in the HIA as follows: In deciding how much health information to disclose, a custodian must consider as an important factor any expressed wishes of the individual who is the subject of the information relating to disclosure of the information, together with any other factors the custodian considers relevant. • HIA section 58(2) Similar obligations are placed on authorized custodians prior to making information accessible in the Alberta EHR (i.e. Alberta Netcare). • HIA section 56.4	• The system allows for reduced access, view or disclosure capability based on the request of an individual. • The system implements technical controls to ensure the consideration of expressed wishes made by a patient to limit disclosure. • The system logs an individual's consent to disclose or expressed wish to limit the disclosure of his or her health information. • The system tracks the purpose for the disclosure and what information was disclosed and to whom. • The system retains disclosure information required under section 41(2) for 10 years.	

Maintaining Disclosure Information

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
HIA requires a custodian who is disclosing identifiable health information to make a notation of the disclosure. This notation must include the name of the person to whom the custodian discloses the information, the date and the purpose of the disclosure, and a description of the information disclosed. Section 41(1.1) allows this information to be recorded electronically. • HIA section 41 This disclosure information must be retained for 10 years. • HIA section 41(2) A custodian that discloses health information must make a reasonable effort to ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information. • HIA section 45	• The system allows for reduced access, view or disclosure capability based on the request of an individual. • The system implements technical controls to ensure the consideration of expressed wishes made by a patient to limit disclosure. • The system logs an individual's consent to disclose or expressed wish to limit the disclosure of his/her health information. • The system tracks the purpose for the disclosure and what information was disclosed and to whom. • The system retains disclosure information required under section 41(2) for 10 years.	

Research

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians may disclose health information to researchers in compliance with HIA. • HIA, part 5 division 3	• The system allows health information to be extracted and rendered non-identifying for research purposes (where required). • Requests from researchers to disclose health information are tracked. • Consents from research subjects are recorded. • Controls are in place to ensure agreements are properly executed before health information is disclosed to researchers.	

Information Managers (i.e. third party service providers, vendors, etc.)

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians are required to enter into an **information manager agreement** prior to disclosing health information to an information manager. Information managers must comply with HIA and its regulations as well as the agreement they enter into with the custodian. An information manager agreement must: • Identify the objectives of the agreement and the principles to guide the agreement. • Indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected. • Indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used. • Indicate whether or not the information	• The system has safeguards in place to prevent the information manager from collecting, using or disclosing health information beyond what is authorized in the information manager agreement. • The information manager agreement is compliant with section 7.2 and section 8.4 (if applicable) of the *Health Information Regulation*.	

manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed. • Describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself. • Describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself. • HIA section 66 • *Health Information Regulation* sections 7.2 and 8(4) Custodians must protect the confidentiality of health information that is to be stored in a jurisdiction outside of Alberta. • HIA section 60(1)(b)		

Privacy Impact Assessments

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must prepare PIAs to describe how proposed practices, including the implementation of a new system, relating to the collection, use or disclosure of health information may affect the privacy of the individual who is the subject of the information. A PIA identifies potential risks to health information as a result of data matching or being collected, used or disclosed in an electronic health record system. It also provides mitigation plans used by the custodian to prevent the loss, destruction, loss of integrity to or unauthorized use, modification or disclosure of the health information that is stored in the system. Custodians must periodically assess their safeguards that protect the confidentiality and security of health information. • HIA sections 64, 70 and 71 • *Health Information Regulation* section 8	• A PIA is submitted to the Commissioner for review and comment with enough lead time to consider comments and make system changes if necessary. • The actual implementation of a system is evaluated against assertions made in the custodian's PIA to ensure ongoing compliance. Evaluation should be conducted at regular, pre-defined intervals.	

Records Retention and Disposition

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Safeguards must be in place for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal. Custodians must not dispose of any records relating to an access request after it is received, even if the records are scheduled for destruction under an approved records retention and disposition schedule. • HIA section 60(2)(b)	• The system archives records in compliance with the custodian's records retention policies, as required by the HIA, professional regulatory body or other legislation. Deletions of records are also documented. • Systems or processes are in place to securely dispose of health information where authorized. • The custodian has a records retention and disposition policy in place. • Custodians belonging to regulatory bodies or working at hospitals may have additional records retention requirements.	

Information Classification

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
The collection, use or disclosure of health information is restricted if the health information is individually identifying. • HIA sections 19, 20, 26, 27, 32, 33, 34, 35, 36 and 37	Custodian has a process for classifying health information in order to: • Distinguish health information that is individually identifying from health information that is not. • Identify where an expressed wish applies to records.	

Risk Assessment

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
New risks to the confidentiality, integrity and availability of health information may arise over time as technology and business processes evolve. To detect these risks, the custodian needs a policy to conduct periodic risk assessments. • HIA section 60 • *Health Information Regulation* section 8	Custodian has a process to periodically identify and mitigate the risks to information in the EHR, which could include: • Third party privacy and security reviews/audits. • Penetration testing. • Internal quality improvement program that tracks privacy and security vulnerabilities, weaknesses and near-misses.	

Physical Security of Data and Equipment

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must maintain reasonable physical safeguards to protect health information. • HIA section 60 • *Health Information Regulation* section 8	Safeguards are in place to manage physical access to health information stored within the system, which could include: • Alarm systems. • Secured server rooms. • Secured routers and wireless access points. • Cables to lock mobile devices. • Maintaining backup and archival copies of health information in a secure off-site location. Measures to protect against environmental hazards (e.g. power loss, fire, flooding, etc.) are based on a **risk assessment**.	

Network and Communications Security

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must maintain reasonable technical safeguards to protect health information. • HIA section 60 • *Health Information Regulation* section 8	• The system and network are protected from unauthorized access through use of firewalls, anti-virus software, intrusion prevention and detection, and regular review of system logs. • Encryption over open networks used when transmitting identifying health information.	

Access Controls

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must have the ability to manage access to the health information in their custody or under their control. • HIA sections 24, 28, 43, and 58(1)	• The system is able to provide an appropriate level of access for each user based on the classification of the information and the user's need-to-know. • The system allows adding new users, modifying existing users, and promptly removing users who no longer require access. • The system has a timeout function that is a variable parameter and based on risk identified by the custodian. • The system is able to uniquely identify and authenticate each user prior to granting access to information. • Remote users log into the system using two factor authentication. • Remote users communicate with the system over an encrypted channel.	

Monitoring, Audit and Incident Response

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must protect the confidentiality of the health information in their custody or under their control against any reasonably anticipated threats to the security, integrity or loss of the health information, as well as its unauthorized use, disclosure or modification. Custodians are required to ensure their EHR system creates and maintains logs. Authorized custodians whose systems connect to Alberta Netcare must also meet certain criteria. The system must be able to log user activity including all accesses to and actions taken by a user. Audit logs should record the following activities. For systems considered part of the Alberta EHR (i.e. Alberta Netcare), these logs are mandatory: • User identification and application identification associated with an access. • Name of user and application that performs an access. • Role or job functions of user who performs an access. • Date of an access. • Time of an access. • Actions performed by a user during an access, including, without limitation, creating, viewing, editing and deleting information. • Name of facility or organization at which an access is performed. • Display screen number or reference. • Personal health number of the individual in respect of whom the access is performed • Other information required by the Minister.	• The system has audit logging functionality to verify the integrity of the system and to log and monitor access to health information. • The system generates logs to monitor user compliance and respond to access requests for logs. • Custodian knows how to retrieve and interpret audit logs. See *Access Controls and Privacy Accountability*. • Processes are in place for the management of privacy breaches and investigations of actual or attempted breaches. • Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis. • The custodian periodically reviews audit logs to determine whether all system activity is authorized.	

Custodians are also required to verify employees adhere to safeguards in place. Audit logging allows custodians to do this. • HIA section 60 • *Alberta Electronic Health Record Regulation* section 6(1) • *Health Information Regulation* section 8(6) Each custodian must establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information. • *Health Information Regulation* section 8(7)		

Business Continuity

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians must protect against reasonably anticipated threats to the security, integrity, or loss of health information. • HIA section 60(1)(c)	• Backup and restoration procedures, including the audit log information, are available at an offsite location. The system is able to archive records and maintain them in a permanently retrievable digital format. This is tested regularly. • To respond to a disaster or major service interruption, custodians should have a tested plan to resume EHR system operations within timeframes based on business needs, professional standards or regulatory requirements.	

Change Control

HIA Requirements	Sample Practices	Describe How You Meet the Requirement
Custodians or information managers may make changes to the system application or other components (e.g. the database, operating system, and network or access directory). The custodian or information manager must demonstrate that the impacts of a change have been identified and steps taken to address them. Custodians must take steps to protect against "reasonably anticipated" threats. Uncontrolled system changes can introduce threats to the security, confidentiality and integrity of health information. Change control allows custodians to test changes before implementation. This is a reasonable step to identify and mitigate privacy threats introduced though system changes. • HIA section 60	• The information manager has documented change management processes in place for upgrades to the hardware and software of the system and a process to inform custodians about changes. • The custodian has documented change management processes in place. • System changes are tested and approved and the change can be "rolled back" without loss of health information or of the integrity of the health information, including audit logs. The system can be restored to a point prior to a failed upgrade.	

Glossary of Terms

Electronic Health Record Information System: Defined in the *Alberta Electronic Health Record Regulation*, section 1(b), as "… the system used by an authorized custodian to collect, use and disclose health information about an individual."

Electronic Health Records: Defined in HIA, section 60(3), as "records of health information in electronic form."

Information Manager: Defined in section 66(1) of HIA as a person or body that:

(a) processes, stores, retrieves or disposes of health information,
(b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information, or
(c) provides information management or information technology services.

Information Manager Agreement: A mandatory agreement between a custodian and an information manager that describes the relationship between the parties. It must include all of the requirements set out in section 7.2 of the *Health Information Regulation* and must be signed by a custodian with authority to do so. An information manager agreement signed between the information manager and a person who is not a custodian does not meet the legislated requirements.

Privacy Impact Assessment (PIA): A due diligence exercise in which privacy risks that may occur in the course of operations are identified and addressed. Custodians must prepare a PIA and submit it to the OIPC for review and comment before implementing any proposed new administrative practice or information system that involves the collection, use or disclosure of health information. PIAs are required under section 64 of HIA.

Provincial Organizational Readiness Assessment (pORA): Refers to the security assessment criteria set by Alberta Health, as required under section 3(1)(c) of the *Alberta Electronic Health Record Regulation*. Completing a pORA is a pre-requisite to obtaining access to Alberta Netcare, the provincial Electronic Health Record.

Risk Assessment: Refers to the process of determining potential vulnerabilities in a given system or initiative. The vulnerabilities are then classified by the risk of harm that may occur as the result of the vulnerability. Similar to a PIA it should also include measures for mitigating the risk.

System: Refers to "electronic health records" and "electronic health records information system" as these terms are defined in HIA. Also refers to an "information system" as described in section 64 of HIA regarding PIAs.

More Information

You can find more information on this topic and the *Privacy Impact Assessment Requirements* guide at www.oipc.ab.ca.

This document is also compatible with *Getting Accountability Right with a Privacy Management Program* developed in partnership with the Office of the Privacy Commissioner of Canada and Office of the Information and Privacy Commissioner for British Columbia.

This document was developed with consideration of the following standards: ISO 27001, the American Institute of Professional Accountants (AICPA), Chartered Professional Accountants (CICA), and Generally Accepted Privacy Principles (GAPP 2009).