A Physician’s Guide to the Information Sharing Framework
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>4</td>
</tr>
<tr>
<td>Information Sharing Framework</td>
<td>5</td>
</tr>
<tr>
<td>The Shared EMRs</td>
<td>9</td>
</tr>
<tr>
<td>Professional Obligations</td>
<td>10</td>
</tr>
<tr>
<td>Participation in the Information Sharing Framework</td>
<td>11</td>
</tr>
<tr>
<td>Benefits</td>
<td>12</td>
</tr>
<tr>
<td>Risks</td>
<td>12</td>
</tr>
<tr>
<td>Access, Correction, Use, and Disclosure of Information</td>
<td>13</td>
</tr>
<tr>
<td>Research</td>
<td>20</td>
</tr>
<tr>
<td>Appropriate Use – Self/Family</td>
<td>22</td>
</tr>
<tr>
<td>Privacy Features</td>
<td>23</td>
</tr>
<tr>
<td>Security</td>
<td>27</td>
</tr>
<tr>
<td>Auditing</td>
<td>28</td>
</tr>
<tr>
<td>Training</td>
<td>29</td>
</tr>
<tr>
<td>Questions &amp; Answers</td>
<td>30</td>
</tr>
</tbody>
</table>
Colleagues,

The Information Sharing Framework (ISF) marks an important milestone in the development of shared electronic medical solutions. For the first time, governance, responsibility and accountability for a single zonal ambulatory patient record is shared by Alberta Health Services (AHS) and participating physicians.

The ISF reflects over two years of negotiation between AHS and the Alberta Medical Association (AMA) on behalf of participating physicians. It ensures that decisions about the use, disclosure and protection of information in a designated shared EMR are made not by a single party, but rather by a governance body that reflects the interests of all EMR Custodians. It also creates a neutral Information Stewardship Office that is tasked with monitoring compliance and supporting positive privacy practices.

The ISF provides mechanisms through which participating physicians can meet their legal and professional obligations. The ISF, which was vetted by the OIPC and CPSA during development, contains the information management agreements and information sharing agreements required under both the Health Information Act and CPSA Standards of Practice.

Finally, the ISF allows us to meet important ethical obligations to our patients and our colleagues. It establishes a framework where the enhanced risks we all share in making additional health information available through a shared EMR are assessed and mitigated.

We welcome your participation in the ISF and encourage you to contact either of us with your questions and comments.

Regards,

Dr. Tim Graham  
ISF GC Co-Chair, AHS

Dr. Steve Edworthy  
ISF GC Co-Chair, AMA
Background

In 2008, Alberta Health Services (AHS) expanded use of designated ambulatory electronic medical record (EMR) systems to include use in ambulatory/outpatient clinics, primary care networks and community physician practices. This change necessitated the development of legal agreements required in order for health information to be shared, and a governance structure that would ensure that no single party to the agreements exercises exclusive control of the information stored in the shared EMRs.

In 2009, AHS and the Alberta Medical Association (AMA) undertook development of the Information Sharing Framework (ISF) to address the growing needs for information governance and risk management in a shared EMR. This process involved significant consultation with other health system stakeholders, including Faculties of Medicine, Covenant Health, the College of Physicians and Surgeons of Alberta, Alberta Health, the Canadian Medical Protective Association and the Office of the Information and Privacy Commissioner of Alberta.

The ISF was signed into effect in March 2012. It consists of:

- A Memorandum of Understanding between AHS and the AMA on behalf of participating physicians (the MOU)
- An Information Sharing Agreement (the ISA)
- An Information Management Agreement (the IMA)
- An EMR Information Exchange Protocol (the EMR IEP)
- A Physician Participation Agreement (PPA)
- A Physician Notice of Termination
- Terms of Reference for the ISF Governance Structure

Currently, over 1000 physicians are using an AHS operated shared EMR solution that is regulated under the ISF. Alberta Health Services and Covenant Health are also EMR Custodians. The ISF establishes a co-custodial model of information sharing; one where all participants contribute information to and use information from a shared information system in support of patient care.

This document is intended to provide participating physicians and other interested parties with a general overview of the ISF and specific information about the use and disclosure of information stored within the shared EMRs. The document also includes information on privacy functionality that is specific to the shared EMRs where such information is required by physicians to meet an obligation that has been placed upon them under the ISF.
Information Sharing Framework

The Information Sharing Framework (ISF) establishes a governance model that supports shared control of health information stored in a designated AHS operated EMR system. It ensures that all custodians that contribute to the shared EMRs, referred to as “EMR Custodians” under the agreements, have an equal voice in determining how health information in these systems is used, disclosed and protected. The primary governance body for the ISF, the Information Sharing Framework Governance Committee (ISF GC), is the only entity that can modify the legal agreements that underpin the ISF.

The governance model also describes relationships between the ISF GC and other governance/advisory bodies.
ISF Governance Committee (ISF GC)

The ISF GC includes voting members from AHS, the AMA and Covenant Health and non-voting members from the Faculties of Medicine, Alberta Health, the Canadian Medical Protective Association (CMPA), the College of Physicians, and Surgeons of Alberta (CPSA) and a member of the public. Its mandate includes:

- Maintaining the information sharing agreements and EMR Information Exchange Protocol (EMR IEP)
- Establishing policy and monitoring use and disclosure of EMR information
- Overseeing privacy and security issues
- Resolving disputes between AHS and participating physicians

Information Stewardship Office (ISO)

The ISO is a neutral office created under the ISF reporting to the ISF GC. The ISO supports the ISF GC and exercises a number of its operational functions, including:

- Developing privacy and security policies for the shared EMR
- Notifying the ISF GC of audits and investigations
- Providing recommendations should a breach of privacy or security involving the shared EMR occur
- Mediating disputes related to access, use and disclosure of the shared EMR
- Coordinating secondary use and research requests
- Monitoring the Information Manager’s compliance with the Information Management Agreement and the EMR Information Exchange Protocol

Local Data Stewardship Committee (Local DSC)

The Local DSC is a platform based committee responsible for developing recommendations and advising the ISF GC on data stewardship issues that relate to their respective local shared EMR. The Local DSC does not provide direct recommendation or guidance to other parties, such as the Information Manager (see below), custodians, or EMR end users.
Information Sharing Framework Workgroup (ISF WG)

The ISF WG is a sub-committee established by the ISF GC, including members from the AMA, ISO, AHS, University of Calgary (U of C), University of Alberta (U of A), and Covenant Health. The ISF WG is responsible for:

- Overseeing the development of shared EMR operational policies and procedures
- Directing, managing, and supporting the development and expansion of the ISF
- Performing duties as directed by the ISF GC

Information Manager (IM)

In addition to its role as an EMR Custodian, AHS is also the Information Manager for the shared EMRs. In its role as IM, AHS is contractually bound to provide the following services to other EMR Custodians:

- Processing, storing, retrieving and disposing of information in accordance with the ISF agreements
- Providing information management and information technology services
- Implementing and maintaining safeguards to ensure health information is protected
- Auditing for inappropriate use, access and disclosure of EMR information and reporting findings to the ISO
- Educating on privacy and appropriate access, use, and disclosure of EMR information
- Completing regular Privacy Impact Assessments on the shared EMR

Co-Custodians

Participating physicians, AHS and Covenant Health are co-custodians of the information stored in the shared EMR. Co-custodians are required to:

- Act in accordance with the Health Information Act and the EMR Information Exchange Protocol (EMR IEP) when accessing, using and disclosing health information stored in the shared EMR
- Take reasonable steps to protect health information, either directly or through the services provided by AHS as the Information Manager
- Report any suspected unauthorized access to or use and disclosure of health information in the shared EMR to AHS as the Information Manager
➢ Use reasonable efforts to ensure health information they enter into the shared EMR is correct and correct errors where possible after discovery
➢ Participate in any investigation struck under the ISF
➢ Agree to be subject to the decisions of the ISF GC
➢ Obtain patient consent for the use and disclosure of health information where consent required by law or under the ISF

Affiliates

An EMR affiliate is an employee of a participating custodian or a person providing a service on behalf of an EMR custodian, permitted by the custodian to access, use or disclose shared EMR information on his/her behalf.

Custodians are responsible and accountable for the actions of their affiliates as it relates to their access to the shared EMR. Custodians must take reasonable steps to ensure that their affiliates understand appropriate use of the shared EMR. They must also take reasonable steps to ensure their affiliates are aware of any applicable organizational policies and procedures related to the privacy, security or protection of health information.

EMR Custodians may contact the Information Stewardship Office at any time to request guidance or direction on the steps they can take to protect health information in the shared EMR or manage the risks associated with providing an affiliate with access to the system.
The Shared EMRs

The ISF applies to designated AHS operated shared EMR systems.

Currently, only eCLINICIAN is designated as a shared EMR under the ISF although the agreements recognize the potential to bring other EMRs under the framework as needed.

**eCLINICIAN**

eCLINICIAN is an AHS operated shared Electronic Medical Record (EMR) system, used in the Edmonton area, for ambulatory care physicians to schedule and manage patient appointments, initiate or accept referrals, store patient electronic health records and bill for healthcare services.

Participating physicians, along with AHS and Covenant Health, are co-custodians of the health information stored in eCLINICIAN. AHS is also the Information Manager to participating physicians and Covenant Health as it relates to their storage of health information in eCLINICIAN.

Information about health services provided at these clinics is accessible by authorized eCLINICIAN users. The following clinics are using eCLINICIAN.
Professional Obligations

Physicians must have an Information Management Agreement (IMA) and Information Sharing Agreement (ISA) in place prior to submitting patient information to a shared EMR system.

College of Physicians and Surgeons (CPSA) Standards of Practice #21

Where a physician places patient information into an electronic record which is not under his or her direct custody or control, there must be in place:

- A written information management agreement
- A written information sharing agreement which manages issues related to access, secondary use and disclosure of patient information

*Health Information Act (HIA) Sections 66 (1) and (2)*

A custodian must enter into a written agreement with the information manager in accordance with the regulations for the provision of any or all services below:

- Processes, stores, retrieves or disposes of health information
- Provides information management or information technology services.

The ISF includes a detailed IMA that describes the services that AHS will provide to participants and an ISA that describes how health information can be used for primary and secondary purposes and how health information can be disclosed. It further details these rules in an EMR Information Exchange Protocol (EMR IEP). The ISO monitors compliance with these agreements on behalf of all participants and reports to the ISF GC.

The IMA, ISA and EMR IEP provide physicians with the ability to meet the their legal and professional obligations to have an IMA and ISA in place when storing health information in a shared EMRs.

Both the CPSA and the Information and Privacy Commissioner’s Office were involved in the drafting of the ISF and recognize the ISF as a viable mechanism through which physicians can meet their obligations under the *Health Information Act* and CPSA Standards of Practice.
Participation in the Information Sharing Framework

Before storing health information in a shared EMR system, each physician must ensure that they have the appropriate legal documentation in place.

<table>
<thead>
<tr>
<th></th>
<th>Physician Participation Agreement (PPA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physicians become party to the ISF by signing a Physician Participation Agreement, which binds them to the other documents in the ISF, including the IMA and ISA.</td>
</tr>
<tr>
<td></td>
<td>Under the PPA, physicians become co-custodians of the shared EMR data and submit their information to the EMR system. They designate AHS as their Information Manager for information contributed to the shared EMR. By signing this agreement, physicians agree to the terms outlined in the IMA and ISA.</td>
</tr>
<tr>
<td></td>
<td>Physicians must sign the PPA before health information about their patients can be stored in the shared EMR.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Organizational Readiness Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>AHS, in its role as Information Manager for the shared EMRs, will assist a clinic in describing and assessing its privacy and security environment during deployment planning. The report generated as part of this assessment will be provided to the ISO, which can make recommendations that additional privacy and security measures be put in place.</td>
</tr>
<tr>
<td></td>
<td>The purpose of this assessment is to determine if a clinic has adequate privacy and security practices, policies and procedures to protect health information. Given the nature of a shared EMR, all EMR Custodians must meet a minimum level of privacy and security readiness.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Privacy Impact Assessment (PIA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Each clinic or organization must have a PIA completed and approved for their use of the shared EMR. The PIA will include data security, privacy and risk assessments to ensure that the privacy rights of the patient and EMR Custodians within the shared EMR are protected at all times. The ISO has developed materials to assist physicians in meeting this provincial requirement.</td>
</tr>
</tbody>
</table>
Benefits of ISF Participation

Becoming part of the Information Sharing Framework holds many benefits for both participating physician and the patients they care for.

✔ Upon joining the Information Sharing Framework, physicians become co-custodians of shared EMR data.

✔ Participating physicians can access, use, and disclose information as set out in the EMR Information Exchange Protocol (EMR IEP), including broad abilities to access enterprise EMR data for patients under their care.

✔ Physicians have the right to request and receive copies of patient records if they decide to move to a clinic outside of the shared EMR environment.

✔ The ISF respects physicians’ interest in the information they contribute to the shared EMR. AHS is limited to using information about a health services provider contained within the shared EMR for purposes expressly laid out in the Information Management Agreement and in accordance with the EMR IEP.

✔ The Information Stewardship Office, a neutral body, represents physicians and all other participating custodians of the shared EMR. The ISO monitors the Information Manager’s compliance with the Information Management Agreement, as well as the other participating custodian’s compliance with the Information Sharing Agreement.

✔ By means of AMA representation on the ISF GC, participating physicians have a voice in governance issues related to the collection, access, use and disclosure of shared EMR information.

Risks of ISF Participation

✗ Information entered into the shared EMR can be seen by other authorized users. The ISF establishes controls to mitigate against this risk. These controls are described in the following pages.
Access, Correction, Use and Disclosure of Information

**ISF FOUNDING PRINCIPLE**

Patient care guides the access, use and disclosure of EMR information, at all times adhering to the EMR Information Exchange Protocol (EMR IEP) and the Health Information Act (HIA)

**Access**

The ISF respects a patient’s right of access to health information as established under the HIA.

Individuals may request access to their own health information or the health information of any person for whom they are an authorized representative under the HIA (ex – parents/guardians of a minor child, personal representative after death for the purpose of administration of an estate, etc).

On receipt of a request from an individual, a participating physician may provide a patient with any information related directly to health services provided by the custodian that is stored in the shared EMR. In other words, a physician can provide a patient with a copy of chart notes, lab or other reports, referral/consultation letters, etc provided these documents relate to health services that the physician or his/her affiliates provided to the patient.

If participating physicians receive a request for information that cannot be related to services they or their staff provided to a patient (i.e. patient requests a copy of their entire shared EMR record) or a request for information contributed by another co-custodian, the request should be forwarded to the ISO. The ISO will direct AHS to process the request as the Information Manager for the shared EMR. In these cases, AHS will advise all involved participating physicians of the request and its decision to release or refuse to release shared EMR information contributed by the physician. AHS will apply the provisions of the Health Information Act in making its decisions.

The centralized access and disclosure service provided by AHS is an Information Manager service and is monitored by the ISO on behalf of all EMR Custodians.
References:

**EMR IEP 3.1.1** Subject to the exceptions set out in the *HIA*, an individual has the **right of access** to that individual's EMR information.

**EMR IEP 3.1.2 and 3.1.7** An individual may request his/her EMR information from his/her EMR custodian. The EMR custodian will respond to requests for access to records that relate **directly** to health services provided by that EMR custodian. Broader requests for access (from more than one custodian) should be referred to the ISO. Requests must be in writing.

**EMR IEP 3.1.9** An individual may be required to **pay a fee** stipulated by the EMR custodian or Information Manager prior to receipt of the requested EMR information.

**HIA Sections 11(1), (2)** The custodian has the **right to refuse access** to a health information disclosure request on the basis that:
- the disclosure poses a threat to the applicant’s mental or physical health
- the disclosure identifies a person who provided health information to the custodian in confidence
- the health information is about an individual other than the applicant
- the disclosure is prohibited by another enactment of Alberta

**Correction**

When a patient believes there is an error in fact or an omission in their health information, the patient may request their health information be corrected in the shared EMR.

Patients must make a request for correction of health information in writing to the custodian that entered the information into the shared EMR. Custodians must consider and respond to a request for correction within 30 days.

If a custodian decides to make a requested correction, he/she must direct AHS to make the correction on his/her behalf. If the custodian decides not to make the correction, he/she must offer the patient the right to either attach a statement of disagreement to the record in the shared EMR or have the decision reviewed by the Information and Privacy Commissioner.
EMR Custodians with questions on the correction of health information are encouraged to contact the ISO for support and direction. (ISO@albertahealthservices.ca; Ph: 780-735-0662)

References:

EMR IEP 3.2 – Request to correct or amend health information by individual who is the subject of the EMR Information

Use

The ISF allows EMR Custodians to use health information in the shared EMR without patient consent for primary and secondary purposes.

In keeping with the principles of the Health Information Act, a custodian should use the least amount of health information necessary for the purpose and should only access health information in the shared EMR where there is a “need to know” the information.

The EMR IEP also recognizes that non-identifying information can be used by an EMR Custodian for any purpose. In general, all information that can be accessed directly through the shared EMRs is identifiable; this provision will only come into play when a custodian has requested access to a report that can be de-identified by a systems analyst.

Primary Use

Participating physicians may use health information contained in the shared EMR when they are providing health services and access to the information is necessary for the provision of the health service or for making a determination for a related health service.

A physician’s affiliate may also use health information for the purpose of providing health services, provided such access is in accordance with their duties for the physician.
References:

EMR IEP 4.1.1 An EMR custodian may access and use EMR information for the provision of health services.

EMR IEP 4.1.2 Use of EMR information shall adhere to the principles of:
- using the least amount of EMR information necessary for the purpose, and
- using EMR information only on a “need to know” basis.

EMR IEP 4.1.3 EMR custodians may access and use EMR information when:
- they are providing health services to the individual, and
- their access to the EMR information is necessary for the provision of health services or for making a determination for a related health service.

EMR IEP 4.1.4 Subject to the professional standards of practice of the CPSA and other professional bodies, non-identifying EMR information may be used by an EMR custodian for any purpose.

EMR IEP 1.2.14 An affiliate of a custodian (i.e. physician office staff under physician as custodian) must not use health information in any manner that is not in accordance with the affiliate’s duties to the custodian. Any use or disclosure of EMR information by an affiliate is considered use or disclosure by the custodian.

Secondary or Health System Use

EMR Custodians may also use health information in the shared EMR for secondary or “health system” purposes. The same overarching principles which guide use for primary care purposes guide the use of health information for secondary purposes, including using the least amount of information necessary and accessing information only when there is an established need to know.

The following are authorized secondary uses of health information in the shared EMR:

- Self-audit to determine if the physician’s own standards and procedures are being effectively and efficiently executed
- Performance or periodic review under the AHS and/or Covenant Health Medical Staff Bylaws
- To determine if CPSA Standards of Practice are being complied with
• To determine if the requirement of another other governance or oversight body are being maintained
• To determine if a participating physician’s claim submissions are accurate and compliant with applicable requirements
• To investigate breaches of privacy obligations
• For health services provider education
• For quality assurance/quality improvement activities
• To audit/monitor access to and use of the shared EMR
• For internal management purposes
• To bill for the provision of health services

Alberta Health Services has unique permissions under the Health Information Act given its role as a provincial regional health authority. These authorities are reflected in the EMR IEP and, as a consequence, AHS may also use health information in the shared EMR for the following purposes:

• Planning and resource allocation
• Health system management
• Public health surveillance
• Health policy development

⚠️ While AHS has broad authorities to use health information in the shared EMR for the four purposes laid out above, the EMR IEP also clearly restricts AHS from using health information in its possession solely in its role as Information Manager for these purposes. As a consequence, AHS is only able to use health information it directly contributes to the shared EMR for these broad “health system management” purposes.

References:

EMR IEP Section 5
Disclosure

EMR Custodians may disclose health information from the shared EMR to any person where the individual who is the subject of the information has provided written, informed consent. This is a discretionary disclosure provision; custodians are not obligated to make such a disclosure should it be requested.

The EMR IEP also allows a participating custodian to disclose health information without consent where such disclosure is authorized or required by sections 35 – 37 of the Health Information Act or another Act of Alberta or Canada. These are detailed legislative provisions, which include the authority to disclose health information:

- To another custodian for the purpose of providing health services or determining eligibility to receive a health service
- To any person for the purpose of providing continuing care and treatment
- To family members or others with a close personal relationship provided such disclosure is in general terms and is not contrary to the expressed wishes of the individual
- Where an individual is deceased, to family members or others with a close personal relationship if the information relates to circumstances surrounding the death of the individual or health services recently received by the individual
- For the purpose of a court or quasi-judicial proceeding to which the custodian is a party
- To comply with a warrant, subpoena or order of a court
- To any person if the custodian believes that disclosure will avert or minimize an imminent danger to the health or safety of any person

Custodians contemplating such disclosure are reminded that EMR information can only be disclosed where it is necessary to comply with the requirement or demand and that the general HIA duties continue to apply. For example, a custodian contemplating disclosure in response to a subpoena would not be able to disclose the entire EMR record if the subpoena specifically requested access to only the health records generated by one particular provider or clinic.

⚠️ A participating physician with questions on whether or not a particular disclosure is authorized by the HIA and EMR IEP should contact the ISO for guidance. (ISO@albertahealthservices.ca; Ph: 780-735-0662)
References:

**EMR IEP 6.1.1** An EMR custodian may disclose EMR information for any purpose where the individual who is the subject of the EMR information has provided consent for that disclosure.

**EMR IEP 6.2.1** An EMR custodian may disclose specific EMR information in the EMR System where expressly authorized or required by sections 35 – 37 of the Health Information Act or other legislative enactments of Alberta or Canada an only that EMR Information that is necessary to comply with the requirement or demand.
Research

FOUNDING PRINCIPLE

EMR information may be eligible for use and disclosure for research only where the research proposal has been approved by a Research Ethics Board (REB) and has met the requirements of the EMR IEP. *EMR IEP 5.4.1 and 6.3.1*

The ISF supports the use and disclosure of health information in a shared EMR for research purposes.

Information is considered to be used for research purposes when the principle investigator is an EMR Custodian (i.e. has signed the PPA) and he/she is looking to use information for research that he/she or his/her affiliates have directly contributed to the shared EMR. Information is considered to be disclosed for research purposes when the principle investigator is not an EMR Custodian and is seeking access to health information contributed to the shared EMR by others.

Under the HIA and EMR IEP, custodians have broad responsibilities when they use and disclose health information for research purposes, including ensuring the researcher has obtained research ethics approval, imposing REB requirement and conditions, evaluating the research proposal and imposing any other requirements on the researcher they believe necessary to protect the privacy of health information. Custodians must also enter into a research agreement if they wish to disclose health information to a researcher.

These responsibilities are discharged by the ISO on behalf of EMR Custodians in the shared EMR.

A participating physician who wishes to use health information in the shared EMR for research purposes should:

- Obtain REB approval for the proposed research project, clearly identifying in that proposal what health information is to be accessed through the shared EMR, the steps that will be taken to protect the health information if it is extracted from the shared EMR, and the members of the research team that will be accessing the shared EMR to obtain the information
• Submit a request to the ISO to use health information in the shared EMR for research purposes, including a copy of the research proposal and the REB’s approval

• Execute the formal research agreement with the ISO on behalf of all participating custodians.

The steps to be followed by external researchers are very similar – they will be required to obtain REB approval and apply to the ISO for access to information for research purposes. The ISO will evaluate the proposal and information provided, impose any additional conditions it believes necessary to protect the privacy of health information to be disclosed to the researcher and enter into the required research agreement.

References:

**EMR IEP 5.4.2** A research applicant who is an EMR custodian may be eligible to access EMR information for research purposes where:

- The research proposal has been approved by the REB
- The request has been accepted for review by the ISO
- The request has been presented through a research protocol summary in a form acceptable by the ISO
- The Researcher has entered a formal agreement with the ISO (on behalf of the EMR custodians)

**EMR IEP 5.4.3** An EMR affiliate may be eligible to access EMR information for research purposes as outlined above (same as custodian). The affiliate must be identified by the Researcher as part of the research team in the proposals sent to the REB and ISO.

**EMR IEP 5.1.1** Secondary use (research) of EMR information must adhere to the principles of:

- Using the least amount of EMR information necessary for the intended purpose.
- Using the highest degree of anonymity that is reasonable in the circumstances.
- Using the EMR information based on a “need to know” basis.

**EMR IEP 5.4.4** EMR information provided to the Researcher is for the exclusive use of the Researcher and where applicable, members of the research team, for purposes of conducting specified research and only for the duration of the research period.

**EMR IEP 5.4.7 and 5.4.9** The Researcher can only access and use EMR information described in the research agreement signed by the ISO. Masked information will not be made available except where the individual, who is the subject of the information, has provided consent.
Appropriate Use - Self/Family

The issue of appropriate use of the shared EMRs has received considerable attention by the ISF GC, specifically as it relates to the use of a shared EMR by an authorized user to review his/her own health information or the health information of a family member.

System access is a privilege and is granted based on a user’s role and responsibility related to the provision of health services. This privilege to access information extends to the information about individuals with whom a physician has an established and active care relationship.

Privacy, security and confidentiality of health information are essential, particularly in a shared EMR environment. In considering this issue of self and family access, the ISF GC noted that all individuals must have the right to access their health information through appropriate and secure means. They can seek access to the information through the custodian that contributed the information to the shared EMR or through Alberta Health Services as the shared EMR Information Manager. These mechanisms of access are the same that would be available to any patient. The ISF GC does not believe that health services providers should be able to obtain access to health information for their personal use on a preferential basis due to their employment within the health sector.

⚠️ EMR users generally do not have the right to access information of a family member or themselves through the shared EMR. The exception to this general rule occurs when a health services provider is directly involved in the provision of a health service to a family member, for example in an emergency. Physicians should be aware of CPSA practice guidelines in this regard and should note that such access is likely to trigger an audit event within the shared EMR and is subject to investigation under the ISF.
Privacy Features

FOUNDING PRINCIPLE
A custodian has the duty to protect the confidentiality of health information and the privacy of individuals who are the subjects of that information HIA Section 60(1)(a). A custodian is obligated to consider the expressed wishes of the patient when deciding how much health information to disclose HIA Section 58(2).

Each of the shared EMR systems possesses functionality that provides physicians with options through which they can limit or restrict the disclosure of health information in the shared EMR. These include:

- Masking a patient record
- Creating a sensitive note
- Charting through a confidential clinic

As the options available to a physician vary based on the shared EMR platform, the following sections of this guide are system specific.

Masking of Patient Records - eCLINICIAN

Patients may request their information be masked within eCLINICIAN. By means of Global Person-Level Masking (GPLM), all of the patient’s information within eCLINICIAN can be restricted from disclosure, with the exception of demographic information such as name, date of birth and address. When a patient requests their record by masked, please follow the directions below:

1. A physician approached by a patient with a request for masking or privacy concerns should discuss privacy concerns with the patient, using the patient counseling script located on the eCLINICIAN home page under Clinical eTools.

2. If physicians agree that the health information should be masked, they must complete the Application for Global Person-Level Masking form found on the eCLINICIAN home page under Clinical eTools.
3. Masking is completed by attaching a confidential flag to the patient record in the AHS Client Registry. Most requests for a record to be masked can be completed within 48 hours.

⚠️ Participating physicians may decline a request for masking if they reasonably believe that masking the record could pose a threat to public health and safety.

⚠️ Physicians should note that applying a mask in eCLINICIAN will also result in the patient’s record being masked in Alberta Netcare. The reverse is also true with rescinding of the mask. This is due to the fact that eCLINICIAN and Alberta Netcare share a common enterprise patient identification record.

**Unmasking of Patient Records - eCLINICIAN**

If a record has been masked in eCLINICIAN, any user attempting to access the record will see basic patient demographic information and a notice that the information being accessed is masked. Some users, based on role, have been given permission to unmask records for limited and specific purposes. This is colloquially referred to as “breaking the glass” on a masked record.

*Breaking the glass* is a temporary unmasking of information. A reason for doing so i.e. patient care must be clearly identified prior to the information being released.

1. Provide reason for *breaking the glass*.
   - Direct patient care
   - HIM Operations (i.e. coding/abstracting)
   - Medical emergency
   - Patient consented
   - Public Health follow up
   - Release of Patient Information
   - Required by Law or Licensing Authority

2. Enter additional details

3. Enter eCLINICIAN password
A user will not be required to break the glass when they have broken the glass in the last 7 days, has an encounter with the patient in the next 15 days, or had an encounter with the patient in the last 15 days.

⚠️ All break the glass incidents are audited by the Information Manager to ensure this function is being used properly.

**Rescinding a Mask - eCLINICIAN**

Patients may request that their masking status be rescinded (removed completely) by contacting a participating physician. For eCLINICIAN users, the process and form are located on the eCLINICIAN home page under Clinical eTools.

Providers may also request that masking be rescinded if they are aware of a change in circumstances of the patient's eligibility for masking. It is the responsibility of the custodian to notify the patient of this prior to removal of the mask.

**Sensitive Notes - eCLINICIAN**

Physicians and some other users have the ability to create a progress note within eCLINICIAN and mark that note as sensitive. When progress notes are marked as sensitive, the ability to view these notes is limited.

![NoteWriter](image)

Depending on the setup of the provider's clinic, sensitive notes can either be:

- viewed by only the provider that has signed the progress note,
- viewed by all providers within that clinic, or
- viewed by all providers within a specialty

Decisions on how sensitive notes will be shared (i.e. limited to provider or shared with the clinic/specialty) are made during deployment planning.
It is important that information valuable to the patient’s ongoing care and treatment not be contained within a sensitive note. Sensitive notes viewable only by the provider cannot be accessed if care is needed in your absence.

**Confidential Departments - eCLINICIAN**

For clinics whose information is deemed ‘sensitive in nature’, the clinic’s records and appointments may be protected and viewable by clinic staff only.

Requesting a status of a ‘confidential department’ is done through an application to the Information Stewardship Office.

All providers within a confidential clinic will have the ability to view the clinic’s patient records. Users outside the clinic will not be able to access this information.

⚠️ The break the glass functionality does not expose appointment or encounter information from a confidential department.

**Example:** Discussions regarding sexual orientation, abuse, information from the patient on a family member (i.e. health history), or third party issues with insurance or lawyer can be documented as sensitive.
Security

FOUNDING PRINCIPLE
A custodian must take reasonable steps to protect the confidentiality of health information in their custody and the privacy of the individuals who are subjects of the information. HIA 60(1)(a) A custodian must take reasonable steps to protect against anticipated threats to security, integrity, loss or unauthorized use, disclosure, modification or access to EMR information. EMR IEP 7.1.2

- Participating physicians have the ability to authorize their affiliates to access the EMR system as it relates to their job duties. Physicians are responsible and accountable for the actions of their affiliates within the system and are advised to take steps to ensure their affiliates understand appropriate use.

- Users must be assigned access based on their role and the ‘need to know’ principle. User roles are identified by their Supervisor or the Custodian based on the responsibilities they are expected to perform.

- Users are to access the EMR system using their own username and password. Users are expected to keep their login credentials secure and up to date. The use of another person’s login credentials is strictly prohibited.

- Users are expected to log off or secure their session prior to leaving their workstation. If no activity is done after a predefined period of time, the session will automatically be secured.

Securing your session will enable you to log back into the session and be at the exact same location within the patient’s chart.

- Regular auditing will be completed to identify misuse of system privileges.
Auditing

FOUNDING PRINCIPLE
EMR information will be managed with due diligence and attention, recognizing the potential harm that can arise from misuse.

The EMR system tracks each access to a patient’s record. These records are subject to audit, which will be completed on random, routine and by request basis. Auditing reports can be run on a specific patient or user.

Regular auditing will be completed by the Information Manager (IM). Incidents where the IM is unable to establish a clinical relationship between the provider and patient will be subject to further investigation by the IM under the direction of the ISO and ISF GC.

Participating physicians can obtain more information on the audit and investigation process by contacting the ISO. (ISO@albertahealthservices.ca; Ph: 780-735-0662)

⚠️ System access is a privilege. Misuse can result in restriction or suspension of access rights, which may impact employment or ability to deliver patient care.
Training

There are two types of privacy training that are relevant for shared EMR use:

- General privacy training
- Application or system specific training

All EMR Custodians are required to take reasonable steps to advise their affiliates of their privacy expectations. As per Health Information Regulation Section 8(6), custodians must ensure that their affiliates are aware of and adhere to all the custodian’s administrative, technical and physical safeguards in respect of health information. A custodian can discharge this responsibility, in part, through development of a privacy training program. For shared EMR users who have not yet developed such a program or who require additional support, AHS has extended its privacy training program to shared EMR users.

All EMR system users are required to complete application specific training before they are granted access to the system. This training includes mandatory “Privacy, Security and Confidentiality” training. Currently this training is classroom based; eCLINICIAN users may register by sending a training request to: ISeCLINICIANTrainingRequests@albertahealthservices.ca.

Online eCLINICIAN training, including the required Privacy, Security and Confidentiality module will be available to users in November 2013.
Questions & Answers

What shared EMR systems fall under the Information Sharing Framework?

Currently, eCLINICIAN (outpatient data in Edmonton area) is active under the ISF agreement. Work is being done to extend this framework to Allscripts Ambulatory (formerly known as SCM) in the Calgary Zone.

Can other users easily view my patient’s information if they are not the provider?

Access within a shared EMR system will be distributed according to the role/position of the requestor. Those in positions of providing health services, i.e. physicians, will receive broader access than those in administrative roles. All users are educated on the appropriate use of the shared EMR system and should access only what is pertaining to their current role and responsibilities.

Access within eCLINICIAN can be further limited by means of:

1. **Masking:** Patients concerned with their data being shared in an electronic environment may request that their information be masked. Requests for masking must be made to an EMR custodian (i.e. physician).

   ![Masking](image)
   Masking will enable an additional layer of security to the record. All those requiring information within a masked record must **break the glass** to do so. All **break the glass** incidents are audited for misuse.

2. **Sensitive Notes:** If a provider feels it is necessary or is expressly requested by the patient not to share certain clinical information, the provider can create a progress note and mark it a 'sensitive' to limit access to only the provider, providers within the clinic, or providers in the same specialty.

   ![Sensitive Notes](image)
   It is important that information valuable to the patient’s ongoing care and treatment **not** be contained within a sensitive note. Sensitive notes viewable only by the provider cannot be accessed if care is needed in your absence.
3. **Confidential Departments:** Clinics that desire a higher level of confidentiality due to the sensitive nature of their information may request the status of ‘confidential department’. Only those with appropriate security, i.e. clinic staff, will be able to view appointments and encounter information by that clinic. A clinic desiring this status must meet certain criteria and make an official request to the ISO.

**Does breaking the glass enable a user see all protected patient information?**

*Breaking the glass* will permit the user to view ‘masked’ patient information. *Breaking the glass* does not allow access to sensitive notes or appointment/encounter information from a confidential department.

All *break the glass* incidents are tracked and the Information Manager audits for misuse of this feature.

**When is a user entitled to break the glass?**

The criteria for *breaking the glass* include:

- Direct patient care
- HIM Operations (i.e. coding/abstracting)
- Medical emergency
- Patient consented
- Public Health follow up
- Release of Patient Information
- Required by Law or Licensing Authority

**Example:** If a user accesses ‘masked’ information outside of the required criteria, this would be considered a misuse of the EMR information and can result in sanction.
If I require information for research purposes that is masked, what is the process?

The individual whose information is masked would need to provide consent for the temporary unmasking of their information. You would access the information by *breaking the glass* and selecting “patient consented”.

⚠️ A copy of the patient consent must be provided to the ISO and IM prior to accessing the information. Approval from the ISO is required prior to accessing any masked information for research purposes. A copy of the consent must be uploaded and saved on in the shared EMR system.

How do you ensure that EMR information is being used appropriately?

All custodians wishing to use or disclose EMR information are required to sign the ISF agreements, certifying that they have read and agree to abide by the terms of the agreements. In addition, regular auditing is completed by the Information Manager to identify inappropriate access and disclosure of EMR information. Auditing will be done on a random, routine and by request basis.

Can I access the EMR system to obtain my own health information?

*Personal access to and use of information in an EMR system is strictly prohibited.* You must not access your own health information or that of your family, friends, co-workers or any other person for any purpose unrelated to your job duties.

- Access must be requested through the same request process as all other applicants - *HIA Section 8 (1); EMR IEP 3.1.2 and 3.1.7*

If I am in a patient’s chart within eCLINICIAN, will another provider be able to access that same chart?

Yes. The chart is accessible to multiple providers at one time. If a provider is documenting on the chart or ordering medications, this may lock the chart for other users depending on what they are trying to access. When a chart is locked, it is still accessible as a read only for other users.
**What is the retention of shared EMR documents?**

The minimum retention of shared EMR documents includes:

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Description</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient care records</td>
<td>Assessment, diagnostic, treatment records.</td>
<td>10 years after the date of discharge.</td>
</tr>
<tr>
<td>Adults</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient care records</td>
<td>Assessment, diagnostic, treatment records.</td>
<td>TBD</td>
</tr>
<tr>
<td>Minors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clinical Trials</td>
<td>Documentation surrounding investigation of medical care, equipment, or medication on human subjects. Includes assessment, diagnostic and treatment records.</td>
<td>25 years after the trial has ended.</td>
</tr>
</tbody>
</table>

The Information Manager manages retention on behalf of all participating custodians of the shared EMR.

**How are records that have met their retention disposed of?**

The Information Manager manages the disposal of records. As per the *HIA 60(2)(b)*, records must be disposed of in a manner to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal. Any destruction of records will be permanent.
For Additional Information:

Information Stewardship Office
ISO@albertahealthservices.ca
Ph: 780-735-0662
Fx: 780-735-0646