TITLE
Privacy Auditing & Investigation of Shared EMR Systems

OBJECTIVES
To provide direction for the consistent review of a User access identified on pro-active audits for potential privacy breach investigations in the shared EMR system\(^1\) and privacy incident-based audits and investigations when applicable in accordance with the Information Sharing Framework\(^2\) (ISF).

APPLICABILITY
This protocol applies to individuals conducting proactive privacy audits and privacy breach investigation as the Information Manager\(^3\) (IM) for the services provided under the Information Management Agreement\(^4\).

PROTOCOL
1.0 General Process

Alberta Health Services Information & Privacy Office (AHS I&P), as the IM and service owner for privacy audits and privacy breach investigations, will implement an audit process, investigate,

---

\(^1\) EMR System means the software, hardware and communications facilities used by AHS and Participating Physicians for Patient care in an ambulatory or outpatient environment to electronically store EMRs, and to enable AHS and Participating Physicians to use and disclose EMR Information embedded in EMRs; and each EMR System shall be identified in the applicable IMA

\(^2\) Information Sharing Framework or “ISF” as reference in this document means the concept of governing the disclosure and use of EMR Information contained in an EMR System, utilizing binding agreements that are comprised of this MOU, the ISA and the IMA, and includes the rules for use and disclosure found in the EMR IEP

\(^3\) Information Manager means that person that has the responsibilities for an EMR System that are described in an Information Management Agreement

\(^4\) Information Manager Agreement as referenced in this document or “IMA” means that agreement between the Information Manager and Participating Physicians, entered into pursuant to section 66 of the HIA, that governs the terms under which the Information Manager, among other responsibilities prescribed by the HIA, receives, processes, stores and converts EMR Information, and maintains and secures the EMR System
take appropriate action, and advise the Information Stewardship Office\(^5\) (ISO) of any unauthorized access or disclosure in accordance with Section 4.1 (g)(h)(i) and Appendix C of the IMA and Section 5.7.1 of the Information Exchange Protocol\(^6\) (IEP) under the ISF.

AHS I&P as the Information Manager (IM) will work proactively with Governance Committee\(^7\) (GC) stakeholders as required to provide definition and standards for determining appropriate access and use of information contained in shared EMR system. AHS I&P will run same last name audits, on a monthly basis in the shared EMR system and forward the audits received to the Privacy Intake Line for tracking and assignment to the designated Privacy Investigator.

### 2.0 Audit Review by AHS I&P

The designated Privacy Investigator will review the audits, noting the dates of access to health information, and review the patient information in the shared EMR system to determine whether a patient/provider relationship exists between the user and the patient. If a clinical relationship is established, the audit of that user will be completed and identified as “appropriate access by the user – no breach”.

Patient/provider relationships will be validated based on the following information:

- Patient has visits, scheduled or attended, at the clinic where the user is employed.
- User has registered, checked in, cancelled, or discharged the patient.
- User has ordered tests, transcribed reports, treated, or provided consultation services for the patient as documented in the patient’s shared EMR.
- User is listed as a provider, treating physician, or family physician for the patient.
- Patient has a referral to the user, or to the clinic where the user is employed.

If an appropriate patient/provider relationship has been established, future audits that identify the same user and patient will be noted as appropriate without further investigation. The established patient/provider relationship will be reviewed and verified after six months to ensure it is still a valid, on-going relationship, if still identified on audits.

### 3.0 Responsible Custodian/Manager Review of EMR Affiliate Access Audits

Where no client/provider relationship can be established from the Privacy Investigators review of the audit report and the information available in the shared EMR system, the Privacy Investigator will initiate a further review by identifying the responsible custodian/manager for the EMR affiliate. The Privacy Investigator will forward a copy of the audit, with a summary requesting the responsible custodian/manager review the access for appropriateness.

---

\(^5\) Information Stewardship Office” or “ISO” means the office established by and reporting to the Governance Committee for the purposes described herein;

\(^6\) Information Exchange Protocol or “IEP” means the set of rules governing access by a Patient to his/her Health Information stored in an electronic health information system and the use and disclosure by authorized Custodians of Patients’ Health Information stored in that electronic health information system. The rules in an IEP are supplemental to the requirements of the HIA;

\(^7\) Governance Committee means that committee established under the MOU and having the responsibilities and duties described therein;
3.1 If the responsible custodian/manager determines that the access was appropriate and in accordance with the role of the EMR Affiliate, the responsible custodian/manager must provide the following information in writing to the Privacy Investigator accompanied by the custodian/manager’s attesting that the access was authorized:

- Explanation of the role of the user
- Identify that the patient was receiving treatment or care at the user’s clinic, or was scheduled for treatment at the clinic.
- Identify that the user was accessing information in accordance with their role at the time of access.

Following receipt and acceptance of this information by the IM, the audit will be withdrawn and if future audits are generated that identify this user and patient, they will be considered appropriate, subject to review after six months as outlined in section 2.

If the Privacy Investigator does not accept the information provided by the custodian/manager in the access audit review the Privacy Investigator may advance the access audit forward for investigation as described in section 3.2. If the custodian/manager refuses to cooperate or participate the matter will be escalated to the ISO and the GC Chairs for mediation and dispute resolution.

3.2 If the access shown on the audit cannot be determined as appropriate, as described in section 3.1, the Privacy Investigator will proceed to an investigation and notify the custodian/manager of this investigation. The investigation may include the responsible custodian/manager, and the custodian’s Human Resources, Medical Affairs and/or Privacy staff, as applicable. I&P will provide notification to the ISO indicating which audits are proceeding into an investigation. Additional or more extensive audits may be requested as determined appropriate by the custodian/manager and/or the Privacy Investigator. The ISF does not prohibit a custodian from conducting a separate or concurrent investigation at their discretion.

3.3 If the access is determined to be unauthorized and outside the role of the user and includes access to self, co-workers, family members, estranged family members, or community members, the Privacy Investigator will, in consultation with the custodian/manager, determine appropriate action to be taken which may include any of the following:

- Privacy/IT Security Training (offered by the custodian however if the custodian does not have specific training available they may utilize the Information Manager Privacy & IT Security Training made available on the AHS External website.)
- eLearning Module for Privacy & Security for eClinician
- Re-signing of the Custodian’s Confidentiality Agreement
- Follow-up audits
- Notification to affected individuals by the responsible custodian/manager
- Notification to the Office of the Information & Privacy Commissioner issued by the custodian in coordination with the ISO
- Recommendation of notification to the Health Professional Body by the GC
• Other recommendations such as a review of clinic/departmental processes that are agreed upon by the custodian/manager and the Privacy Investigator

The ISO will be advised of the inappropriate access and actions to be taken as soon as the actions to be taken have been determined, allowing for timely feedback from the ISO. If the user’s access is considered Potentially Serious, additional actions may be recommended by the Privacy Investigator, the custodian/manager, ISO or GC.

In addition, access considered Potentially Serious shall be reported to the ISO along with investigation findings and recommendations. The ISO will advise the GC in accordance with the ISO processes.

3.4 AHS Information & Privacy will provide GC, through the ISO, with a monthly report indicating the results of all the reviews of the EMR Affiliate Access Audits.

4 Participating Physician User Access Audits

If the initial review of the user’s access cannot be determined to be appropriate by the Privacy Investigator and the user is a participating physician, the Privacy Investigator will issue an introductory letter/email to the physician, advising them that an investigation is being initiated under Section 4.1(i) of the IMA and the ISO will be notified simultaneously. An investigation interview will be arranged between the physician and the Privacy Investigator. Any investigation that is unable to progress due to a physician’s refusal to cooperate or participate will be escalated to the ISO and the GC Chairs for mediation and dispute resolution.

4.1 If it is determined in the interview with the participating physician that the access was only to the physician’s own information, and does not include access to colleagues, family members, estranged family members, or community members, the Privacy Investigator will issue a letter to the physician, with a copy to the ISO, advising that the participating physician’s actions are unauthorized and not in accordance with the IEP. The participating physician will be advised that they are to take immediate actions to comply with the agreements. A written response agreeing with compliance will be requested from the participating physician. If the participating physician refuses to comply with the recommendations the matter will be escalated to GC through the ISO.

4.2 If it is determined in the interview with the participating physician that the access was to colleagues, family members, estranged family members, or community members, the Privacy Investigator will provide recommendations including

• Privacy/IT Security Training (offered by the Information Manager - Privacy & IT Security Training available on the AHS External website.)
• eLearning Module for Privacy & Security for eClinician
• Re-signing of the Physician Participation Agreement/Confidentiality Agreement additional education on the Health Information Act and the agreement to the physician.

The Privacy Investigator will issue a letter to the physician, with a copy to the ISO, advising that the participating physician’s actions are unauthorized and not in accordance with the IEP. The participating physician will be advised that they are to take immediate actions to comply with the agreements. A written response agreeing with
compliance will be requested from participating physician. If the participating physician refuses to comply with the recommendations the matter will be escalated to GC through the ISO.

4.3 If it is determined during the interview/investigation that the physician access is deemed Potentially Serious, the physician will be informed that the findings will be reported to GC through the ISO as unauthorized. A report outlining the investigation findings and recommended actions will be provided to GC through the ISO and a copy provided to the physician.

- Recommendations may include: Privacy/IT Security Training (offered by the Information Manager - Privacy & IT Security Training available on the AHS External website.)
- eLearning Module for Privacy & Security for eClinician
- Re-signing of the Physician Participation Agreement/Confidentiality Agreement
- Follow-up audits
- Notification to affected individuals, as coordinated by the GC
- Notification to the Office of the Information & Privacy Commissioner by the Privacy Investigator in consultation with the ISO as directed by GC
- Notification to the health professional body by the GC if appropriate
- Other recommendations such as a review of clinic/departmental processes that are agreed upon by the participating physician and the Privacy Investigator

Final decision regarding actions to be taken will be determined by GC and will come back to the Participating Physician through the ISO with a copy to Privacy Investigator. For physicians practicing in an AHS or Covenant Health facility, the Medical Affairs office will also be notified. A written response agreeing with compliance will be requested from the participating physician. If the participating physician refuses to comply with the recommendations the matter will be escalated to GC through the ISO.

5. Resolving Audit Review

5.1 The Privacy Investigator will maintain a record of all audits generated. A report of the outcome will be forwarded to the ISO for GC on a monthly basis.

5.2 The Privacy Investigator will maintain a summary explanation of the conclusions for all audits withdrawn from further investigation.

5.3 Where the user access is determined to be “appropriate” Privacy Investigator will finalize the summary report and indicate that no breach occurred.

5.4 When an investigation identifies unauthorized access, the Privacy Investigator may run additional audits in approximately four to six months to ensure continued compliance by the user. Additional audits would be addressed with the same process as routine proactive audits as outlined in the departmental protocol and reported to GC through the ISO as outlined in section 5.1.
DEFINITIONS

User means a person granted access to a shared EMR system subject to the ISF.

Appropriate means viewing results and information in the shared EMR system required to fulfill a user role and responsibility. Appropriate access may be determined by the custodian/manager responsible for the user by establishing a patient/provider relationship.

Unauthorized means viewing results and information in the shared EMR system not required to fulfill a user roles and responsibilities.

Potentially Serious means an access, viewing or alteration of any data in an EMR System (as that term is defined in the Information Sharing Framework) that results in substantial actual or potential harm to an individual or an individual's privacy, and includes any access, viewing or alteration of any data for personal or third party gain.

Custodian means a custodian under the Health Information Act that is permitted to access, use or disclose EMR information in accordance with an executed agreement under the Information Sharing Framework (ISF). The ISF enables a sharing of the custodial duties in a common manner with a shared ambulatory EMR environment. Defined services that have traditionally been completed exclusively within physician practices will now be managed through a common central service of which AHS is assigned the “Information Manager”.

REFERENCES

Alberta’s Health Information Act
Information Sharing Framework, EMR IEP 1.2.7(c), 8.1.7; IMA 4.1(g)(i)(v), ISA 11.3

REVISIONS

N/A