

MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF SOUTHERN ALBERTA PRIVACY AND SECURITY POLICY

1 Purpose

The collection, **use** and **disclosure** of **health information** by physicians who are members of MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF SOUTHERN ALBERTA CORPORATION, (hereinafter referred to as the MDERA) are governed by the provisions of the *Health Information Act* (HIA) and this policy. The following principles and the procedures appended to this policy are intended to enable patient care and effective service delivery, while protecting the privacy of patients of the member physicians.

2 Scope

This policy applies to:

- Health service providers and staff, including contractors providing services for individual physicians;
- **records** in any form created or received in the course of carrying out the medical services of the member physicians;
- all facilities and equipment required to collect, manipulate, transport, transmit or keep health information.

3 Principles

- 3.1** Physician members will comply with this policy and associated procedures with respect to health services provided to their patients. All records related to these health services shall be deemed to be under the control of the physician who provides the services.
- 3.2** Notwithstanding section 3.1 of this policy, physician members and Calgary Health Region have an interest in and require access to records created in facilities owned and operated by the health region and these records and/or information contained in these records shall be made available to Calgary Health Region in accordance with the data sharing agreement between MDERA and Calgary Health Region.
- 3.3** Physicians and their affiliates shall protect the confidentiality of health information and personal information in their custody or control, and the privacy of the individuals who are the subjects of that information. This includes protection against unauthorized use, disclosure, modification, or access to the information.
- 3.4** Individuals have a right of access to any information about themselves that is in the custody or control of the physician members, subject to the limited and specific exceptions set out in HIA. Individuals who believe there is an error or omission in their health information have a right to make a request to correct or amend the information. [See Privacy and Security Procedure 1]

- 3.5 When collecting **health information** or personal information directly from an individual, and when that information is being retained by one of the physician members and proper notice is not already given by the health region, the individual will be informed by the physician of the purpose for which the information is collected and the legal authority for the collection. This should be done through a poster or other visible medium but can be done orally if appropriate.
- 3.6 Health information shall only be used and disclosed for the purpose for which it was collected, unless alternate use or disclosure is authorized or required by law, or with the knowledge and **consent** of the subject individual.
- 3.7 **Affiliates** of physicians will collect and use identifying **health information** and personal information only to perform their duties for the physician.
- 3.8 Individuals have the right to request the Information and Privacy Commissioner to review access, privacy and correction decisions made by physician members.
- 3.9 Physician members will ensure that they use the forms appended to this policy or similar forms that comply with the HIA.

4 Sanctions

Failure to comply with this policy and its procedures will place an individual at risk of prosecution under the **HIA**. An **affiliate's** failure to comply will result in disciplinary action, up to and including termination of employment or contract.

5 Privacy Officer Responsibilities

The *Health Information Act* (HIA) requires custodians to identify a contact person who is responsible for ensuring compliance with the Act.

- 5.1 MDERA shall elect one of its members to be Privacy Officer and he or she will act on behalf of member physicians. Each physician member is responsible for ensuring implementation of this policy and for ensuring cooperation with the privacy officer as required for his or her practice. The Privacy Officer may delegate any responsibilities to an Executive Assistant who will be responsible for day to day privacy issues.
- 5.2 The responsibilities of the Privacy Officer include:
- Identifying privacy compliance issues and making recommendations for improvements both to MDERA and member physicians;
 - Ensuring that privacy and security policies and procedures are developed and maintained as necessary;
 - Ensuring that affiliates and contractors of MDERA are aware of their responsibilities and duties under HIA;
 - Responding as directed by member physicians to requests for access to or correction of health information,
 - Assisting member physicians with the implementation and monitoring of the MDERA privacy policy and procedures,
 - Ensuring the overall security and protection of health information in the custody of MDERA and member physicians, and
 - Dealing with regional health authorities, third parties and the Office of the Information and Privacy Commissioner respecting privacy and security issues.
 - Manage the Data Sharing Agreement with the Calgary Health Region

Terms or phrases that are **bold** and *italicized* are defined in Appendix 1

APPENDIX I: DEFINITIONS

This section provides definitions of terms used in applicable privacy legislation, and Clinic policies and procedures.

Affiliates: includes all employees, volunteers, students, residents, fellows and persons contracted to provide services for custodians.

Authorized Representative means any person who can exercise the rights or powers conferred on an individual under applicable privacy legislation. This includes the right of access to an individual's health information and the power to provide consent for disclosure of such information.

- If the individual is under 18 years of age, and does not understand the nature of the right or power or the consequences of exercising the right or power, by the guardian of the individual
- If the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the estate
- A guardian or trustee appointed under the *Dependent Adults Act* if the right or power related to the powers or duties of the guardian or trustee
- An agent under the *Personal Directives Act* if the directive so authorizes
- A person who has power of attorney granted by the individual if the exercise of the right or power relates to the powers or duties conferred by the power of attorney
- If the individual is a formal patient as defined in the *Mental Health Act*, by the individual's nearest relative as defined in the *Act* if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that *Act*.
- Any person with written authorization from the individual to act on the individual's behalf.

Consent: Agreement by an individual to the disclosure of their own health information to a third party. The consent must include:

- An authorization for the custodian to disclose the information specified in the consent
- The purpose for which the information may be disclosed
- The identity of the person to whom the information may be disclosed
- An acknowledgement that the individual providing the consent has been made aware of the reasons why the information is needed and the risks and benefits to the individual of consenting or refusing to consent
- The date the consent is effective and the date, if any, on which the consent expires
- A statement that the consent may be revoked at any time by the individual providing it.

A consent or revocation of consent can be provided in writing or electronically.

Electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting the consent or revoking the consent.

In the case of a minor who has consented for diagnosis or health services, consent for the release of information must be obtained from the minor (not the parent or guardian).

Custodian includes the following:

- Regulated health professionals paid through the Alberta Health Care Insurance Plan, including physicians, chiropractors, dental surgeons, dental mechanics, opticians, optometrists, podiatrists and osteopaths
- Licensed pharmacists and pharmacies
- Regional Health Authorities (RHAs), Alberta Mental Health Board and Alberta Cancer Board
- Other nursing homes and hospitals not owned by the above
- Community Health Councils and subsidiary health corporations of RHAs, Boards
- Minister and the Department of Health and Wellness
- Boards, committees, panels, councils or agencies established by any of the above

Disclosure: Means releasing information to individuals or agencies external to a physician member (i.e. to non-affiliates). This includes sharing information between member physicians or their affiliates.

Health Information: Recorded information about individuals. There are three types of health information: (1) diagnostic, treatment and care information, (2) registration information (including billing information), and (3) health provider information (personal information about the individual who provides health services). The collection, use and disclosure of all three types are regulated by the *Health Information Act*.

Record: Information in any form, including notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner. Does not include software or any mechanism that produces records.

Research: Means academic, applied or scientific health-related research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

Use: Means the internal use of information (i.e. between affiliates of a physician member).

APPENDIX 2: FORMS

NOTIFICATION OF COLLECTION OF PERSONAL HEALTH INFORMATION (POSTER FOR CLINIC OFFICE OR EXAMINING ROOM)

When you receive health services of any kind from *<named physician>* we collect individually identifying health information from you and share this within the clinic and with other health service providers that need the information to provide you with health services or to manage the provision of health services to you.

The health information that you provide to us is collected, used and disclosed in accordance with the provisions of the *Health Information Act (HIA)*, and is primarily used to provide diagnostic, treatment and care services to you, and to bill the Alberta Health Care Insurance Plan for services provided. It may also be used to enable a researcher to contact you if you have consented to being contacted to determine willingness to participate in research projects. The privacy provisions of the legislation require that we protect your health information from unauthorized access, use, disclosure or destruction.

For more information, please talk to your treating physician or call *<physician office phone #>*

NOTIFICATION FOR FAX COVER SHEET

This facsimile contains confidential information intended only for the person to whom it is addressed. Any other distribution, copying, or **disclosure** is strictly prohibited by law. If you have received this facsimile in error, please inform the sender immediately by phone and then return the original to us at our expense without making a copy. Thank you.

**MDERA
Confidentiality agreement**

MDERA recognizes and supports a patient's right to privacy in relation to his/her health information. Member physicians, their staff and residents are expected to treat patient information as confidential.

It is imperative that patient information contained on the EMR is accessed and/or used only by those users who are trained and authorized.

Access codes and passwords are used to protect the confidentiality of computerized patient information and to prevent access by unauthorized users.

I, the undersigned, acknowledge receipt of my EMR sign on code (s) and understand that:

- 1) My EMR sign-on code is the equivalent to my signature.
- 2) I will not disclose this code to anyone.
- 3) I will not tape the passwords to or around the computer but rather keep confidential.
- 4) I will not attempt to learn another person's EMR sign-on code.
- 5) I will not attempt to access any unauthorized information via the EMR; nor will I make any unauthorized use of the information in the EMR.
- 6) I will not attempt to access information in the EMR by using an EMR password other than my own.
- 7) I will protect the patient's right to the confidentiality of his/her medical record.
- 8) I will not change the EMR password unless discussed with EMR Coordinator.
- 9) I acknowledge that the Windows password will be changed every three months.
- 10) I will not change the time outs on the screen savers.
- 11) I will minimize or close screens where necessary if computer is unattended.
- 12) I will lock the computer screen prior to leaving an exam room.
- 13) I will keep records confidential when viewing on home computer.
- 14) I will have up to date virus software and firewalls on my home computer.

User name: _____ User signature _____

Role: _____

CONSENT FOR DISCLOSURE OF IDENTIFYING HEALTH INFORMATION

I, _____, give consent for

< *Physician Name* >

to disclose:

(Identify nature of health information)

to _____
(Identify individual/organization to whom information is released)

for the purpose of _____
(Indicate how information will be used/disclosed)

I acknowledge that I have been made aware of the reasons for the disclosure of the above information, and the risks and benefits associated with consenting to its release.

I understand that I may revoke my consent at any time, by providing a signed, written statement to that effect.

Date: _____
Valid Until: _____

Signature: _____
Print Name: _____

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA
CONFIDENTIALITY OATH**

- 1) I, _____ agree that I will faithfully discharge my duties as an employee / contracted service provider for <physician names> and will observe and comply with all policies and procedures of the MDERA with respect to privacy, confidentiality, and security of health information.
- 2) Unless legally authorized to do so, I will not use or disclose health information that comes to my knowledge or possession by reason of my affiliation with the above mentioned physicians, including after I cease to be employed by them.
- 3) I understand that a breach of this agreement may be just cause for termination of my employment or affiliation with the physicians.
- 4) I am aware that MDERA has policies and procedures regarding the privacy, confidentiality, and security of health information that apply to its member physicians and I understand that it is my responsibility to be familiar with the requirements outlined in these policies and procedures.
- 5) I understand that I can refer to MDERA's Privacy Officer for the details of these policies and any other information required for me to understand my obligations.

Signature

Printed Name

Date

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA
Privacy and Security Procedure 1**

RIGHT OF ACCESS TO IDENTIFYING HEALTH INFORMATION

1 Purpose

Subject to limited and specific exceptions in the *Health Information Act* (HIA), individuals have a right of access to information about themselves that is in the custody or control of a physician member, and the right to request corrections or amendments to this information. This procedure is intended to define a process for facilitating requests for access to and correction of an individual's own health information. Further information about processing requests, including model letters and guidance on applying exceptions can be found in "*Health Information Act Guidelines and Practices*".

2 General Procedures

- 2.1 During the provision of health services, physicians and their affiliates will share information verbally with the patient or authorized representative and allow access to or provide copies of their health information records when practical.
- 2.2 In the case of a request by the parent or guardian of a minor, physicians will determine whether the minor understands the consequences of disclosing or not disclosing the health information before making a decision to share information with the parent or guardian.
- 2.3 When an individual or authorized representative asks for a correction of factual information and can substantiate that the information is incorrect, an authorized affiliate will make the correction to the medical record. (Examples include name, address, telephone number and other demographic information). This correction will also be provided to Calgary Health Region so that the Enterprise Master Patient Index (EMPI) can be corrected.

3 Procedure to Request Access to Information

- 3.1 When access cannot be provided under section 2.1 of this procedure, patients may make a request for access to information in writing. An individual may request access to another person's information only if they are an ***authorized representative***.
- 3.2 All requests for access to information should be directed to the physician member. If the request includes information from the EMR, it will be forwarded to the MDERA Privacy Officer. Requests must be accompanied by \$25.00, or the basic fee set out in the Health Information Regulation, which will ensure provision of up to 20 pages of records.

- 3.3** The Privacy Officer shall consult with the Calgary Health Region Information, Access and Privacy Office in accordance with the data sharing agreement and, if applicable, transfer the request to the health region.
- 3.4** After receiving the request, the Privacy Officer will ensure the retrieval of the requested **records** and, in accordance with the fee schedules set out in the Health Information Regulation, prepare a fee estimate and provide that estimate to the applicant. The applicant has up to 20 days to indicate if the fee estimate is accepted or to modify the request to change the amount of fees assessed.
- 3.5** Processing a request ceases once a notice of estimate has been forwarded to an applicant and begins again immediately on the receipt of an agreement to pay the fee, and on the receipt of at least 50% of any estimated fee.
- 3.6** Physician members may agree to waive fees, including the basic fee, for reasons of financial hardship or fairness and will inform the privacy officer of any fee waiver decision.
- 3.7** Once the estimate has been agreed to, the privacy officer will review the records subject to the access request for possible exceptions to disclosure and ensure that copies are prepared for disclosure. All records relating to the request will be reviewed on a line-by-line basis. (See Section 5 of this Procedure)
- 3.8** The Privacy Officer will provide recommendations to the physician member with regard to any exceptions to disclosure that might be applied and the physician member will make the final decision on release.
- 3.9** Response to the applicant must be made within 30 days of receipt of the request unless the time limit has been extended in accordance with HIA.
- 3.10** As part of the member's response, the applicant shall be told:
- Whether access to the record or partial record is granted or refused;
 - If access is granted, where, when and how access will be given, and
 - If access is refused, the reasons for refusal and basis of refusal; the name, title, business address and phone number of the Privacy Officer or physician member; and that the applicant has a right to request a review of the decision by the Alberta Information and Privacy Commissioner.
- 3.11** An affiliate or the physician member shall be present if the applicant views the original record to answer questions and maintain the integrity of the record. If information is severed from the record before disclosure of the information, the applicant no longer has the option of viewing the original record.

4 Authentication of Recipient

- 4.1 When an authorized representative requests an individual's health information, an affiliate may request documentation of the representative's authority to act and verify that the powers and duties of the representative allow for requesting health information on behalf of the individual. If the authorized representative is not known to the physician member, a copy of such documents as a guardianship order, power of attorney, personal directive or letters of administration for an estate must be shown.
- 4.2 Affiliates shall take reasonable steps to verify the identity of the individual or authorized representative before disclosing health information. This may involve looking at a driver's license or health card.

5 Making the Disclosure

- 5.1 Physician members **must refuse** to disclose health information to an applicant:
- If it is about an individual other than the applicant unless it was originally provided by the applicant in the context of a health service being provided to that applicant;
 - If it sets out procedures or contains results of an investigation, discipline proceeding, practice review or inspection relating to a health services provider; or
 - If disclosure is prohibited by provincial legislation (e.g. information protected under the *Protection for Persons in Care Act*, information about organ or tissue donations).
- 5.2 Physician members have the **discretion to refuse** disclosure of health information to an individual:
- If it could reasonably be expected to result in immediate and grave harm to the applicant's mental or physical health or safety;
 - If it could reasonably be expected to threaten the mental or physical health or safety of another individual or pose a threat to public safety;
 - If it could reasonably be expected to lead to the identification of a person who provided health information in confidence and the physician considers it to be appropriate that the name of the person be kept confidential;
 - If it could prejudice the use or results of audits, diagnostic tests or assessments.

6 Procedure to Request Correction of Health Information

- 6.1** When information cannot be corrected under section 2.3 of this procedure, an individual may make a request for correction or amendment in writing. An individual may request a correction to another person's information only if they have written authorization of the individual the information is about or are an authorized representative.
- 6.2** The physician member will review the request to determine whether the request is to be granted or refused. Corrections will only be made to factual information. Corrections cannot be made to professional opinions or observations. The correction process must be completed within 30 days of receipt of the request for correction, unless the time has been extended under HIA.
- 6.3** When a physician member determines that a correction or amendment is to be made, the physician member shall notify the Privacy Officer and ensure that the correction is made on all records containing the corrected information, and inform the applicant in writing of the corrections made.
- 6.4** When a physician member refuses to correct or amend the information, the member will advise the Privacy Officer who shall inform the individual that they may
- Ask for a review of this decision by the Information and Privacy Commissioner, or;
 - Submit a statement of disagreement setting out in 500 words or less the requested correction or amendment and the applicant's reasons for disagreeing with the custodian's decision.
- 6.5** When the applicant submits a statement of disagreement, the privacy officer will ensure that the statement is incorporated into the electronic medical record next to the information that was not corrected, or append the statement in any paper records in the same manner.
- 6.6** The privacy officer will advise any person to whom the information was disclosed in the preceding year that a statement of disagreement has been filed. Physician members are responsible for advising persons to whom the information was disclosed in the preceding year if a correction is made to the record.

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA
Privacy and Security Procedure 2**

**COLLECTION, USE AND DISCLOSURE OF IDENTIFYING HEALTH
INFORMATION**

1 Purpose

The *Health Information Act* (HIA) provides rules for the collection, use and disclosure of individually identifying health information. Physician members are bound by these rules and this procedure provides guidance for their application.

2 General Rules

- 2.1 Physician members will not collect, use or disclose individually identifying health information if aggregate or other non-identifying health information is adequate for the intended purpose.
- 2.2 When collecting, using or disclosing health information, physician members will only collect, use or disclose the amount of health information that is essential to enable the physician, or the recipient of the information, to carry out the intended purpose.
- 2.3 Before using or disclosing health information physicians and their affiliates will make a reasonable effort to ensure that the information is accurate and complete.
- 2.4 Physician members will not use identifying health information to market any service for a commercial purpose or to solicit money without the express consent of the individual who is the subject of that information.

3 Collection and Use of Identifying Health Information

- 3.1 Health information will be collected directly from the individual it is about or an authorized representative unless indirect collection is authorized by HIA. Examples of indirect collection are:
 - When the individual authorizes collection from a third party (this authorization can be verbal).
 - When direct collection would compromise the interests of the individual, the purpose of collection, the accuracy of the information or the safety of another person (e.g. patient is not being completely truthful or cannot remember information).
 - When direct collection is not reasonably practicable (e.g. language barrier, or cognitive impairment).
 - When information is collected from another custodian during referral or consultative processes.

3.2 When collecting health information directly from an individual, the individual will be informed of the purpose for which the information is collected, the legal authority for the collection and the title and business contact information of a staff member who can answer questions. Notification will be done by means of posters in the reception area and/or examination rooms, and verbally when appropriate.

3.3 Individually identifying health information shall only be used to:

- Provide health services
- Determine or verify the eligibility of the individual to receive a health service
- Education of health service providers in the Clinic
- Carry out purposes authorized by federal or provincial legislation (e.g. *Public Health Act*)
- Obtain or process payment for health services
- Internal management purposes, including quality improvement and monitoring processes,

or for other purposes set out in section 27 of HIA.

3.4 Affiliates shall only use health information as required to perform their assigned duties.

4 Disclosure with Consent

4.1 Physician members will normally require written consent from the individual to disclose identifying health information to anyone other than the individual (or authorized representative) or to another custodian.

4.2 Consent will be provided on the prescribed form or be in a format acceptable to the physician member.

4.3 MDERA members may seek consent from patients at the time of referral, or during a subsequent consultation, to disclose registration information to researchers. This will enable a researcher to contact individuals to determine if they are interested in participating in a research project.

4.4 If the written consent is not in the prescribed form, physician members may consult with the individual to ensure that he or she understands the reasons for the disclosure and the content of the information that is being disclosed (e.g. to insurers or lawyers).

5 Disclosure without Consent

Physician members may, but are under no obligation to, disclose identifying health information without consent in the following circumstances. In all cases, physicians must consider the expressed wishes of the individual with regard to his or her health information and disclose the least amount of identifying health information at the highest level of anonymity that they consider necessary to fulfill the request.

- 5.1** To another custodian, or affiliate of a custodian, for the legally authorized uses identified in section 27 of HIA.
- 5.2** To a person who is responsible for providing continuing treatment and care to the individual.
- 5.3** To family members or persons with whom the individual has a close personal relationship providing the individual has not asked that such disclosure not be made, and providing that the information is given in general terms and concerns the condition, diagnosis and prognosis of the individual on the day on which the information is disclosed, or if the individual is deceased relates to the circumstances surrounding the individual's death or to health services recently received by the individual.
- 5.4** To any person in order to contact a family member or person with whom the individual has a close personal relationship when the individual is ill, injured or deceased, unless the individual has asked that such contact not be made.
- 5.5** For the purpose of a court proceeding, or a proceeding before a quasi-judicial body to which the physician member is a party.
- 5.6** To comply with a subpoena, warrant or order for the information providing the provider of the subpoena, warrant or order has jurisdiction in Alberta to compel the production of records.
- 5.7** For the purpose of obtaining or processing payment for health services provided to the individual by a person that is required under a contract to pay for those services for that individual.
- 5.8** To another custodian if there is a reasonable expectation that the disclosure will detect or prevent fraud, limit abuse in the use of health services or prevent the commission of a criminal offence.
- 5.9** To any person to avert or minimize an imminent danger to the health or safety of any person.
- 5.10** If the disclosure is authorized or required under federal or provincial legislation (e.g. *Workers' Compensation Act, Child, Youth & Family Enhancement Act, Public Health Act*).
- 5.11** To the successor custodian of the physician member.

- 5.12** To a police officer or the Minister of Justice and Attorney General in accordance with sections 37.1, 37.2 and 37.2 of the Act.
- 5.13** To a health professional body for the purpose of an investigation, discipline proceeding, practice review or inspection.
- 5.14** To a researcher who has signed a written agreement with the physician member in accordance with HIA (see Procedure 3).
- 5.15** In other circumstances provided for in sections 35 – 40 and 46 – 47 of HIA.

6 Notation and Notification

- 6.1** When a record containing individually identifying diagnostic, treatment and care information is disclosed under section 5.1 – 5.14 above, or in accordance with section 35 of HIA, the physician or authorized affiliate will make note of the following information and place it on the patient’s electronic medical record:
- The name of the person to whom the information is disclosed;
 - The date and purpose of the disclosure, and;
 - A description of the information disclosed.
- 6.2** When disclosure is from one physician member to another physician member (or between affiliates thereof), or to the Calgary Health Region, the audit trail on the EMR is deemed to be sufficient record of the disclosure and will be retained for a period of 10 years.
- 6.3** When individually identifying diagnostic, treatment and care information is disclosed to anyone other than another custodian, a police officer or the Minister of Justice & Attorney General without consent, the physician member will inform the recipient in writing of the purpose of the disclosure and the authority under which the disclosure is made. This will be done in the covering letter or fax cover sheet accompanying the information or by means of the form appended to this procedure.

**SECTION 42 (HIA) NOTICE TO RECIPIENT TO ACCOMPANY THE
DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC,
TREATMENT AND CARE INFORMATION**

The identifying health information of _____ accompanying this form has been disclosed to _____ either with the consent of the individual (also enclosed) or is authorized under the following provision of the *Health Information Act*. By receiving this information, the receiving party accepts responsibility under applicable privacy legislation for protection from unauthorized use or further disclosure of this information, and becomes the custodian, holding the physician and his staff indemnified against any further claim, and free from responsibility, however caused. Once the purpose for which this information release has been accomplished, the receiving party is responsible for its secure protection and confidential destruction.

To provide continuing treatment and care to the above named individual (s. 35(1) (b))

To provide information to family or friends (s. 35(1) (c))

To advise family members that the individual has been injured, is ill or has died (s. 35(1) (d))

To provide health services to the above named individual who is being detained in a penal or custodial institution (s. 35(1) (e))

To conduct an audit of the information (s.35 (1) (f))

To carry out quality assurance activities within the meaning of the Alberta Evidence Act (s.35 (1) (g))

To provide information for a court proceeding or a proceeding before a quasi-judicial body (s. 35(1) (h))

To comply with a subpoena, warrant or court order (s. 35(1) (1) (i))

To enable an Officer of the Legislature to carry out his duties (s.35 (1) (l))

To detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada (s.35 (1) (k))

To avert or minimize an imminent danger to the health or safety of a person (s.35 (1) (m))

To act in the best interests of the above named individual who lacks the mental capacity to provide consent (s.35 (1) (n))

To provide necessary health services to a descendant of the above named individual (s.35 (1) (o))

To comply with another Act or regulation of Alberta or Canada that requires or authorizes disclosure (s.35 (1) (p))

To enable a health professional body to conduct an investigation, practice review, discipline proceeding or inspection (s. 35(4)).

To enable the Minister of Health and Wellness to carry out his or her duties (s.40)

Date _____

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA
Privacy and Security Procedure 3**

RESEARCH

1. Purpose

The Health Information Act (HIA) sets out rules for the disclosure of individually identifying diagnostic, treatment and care information and/or individually identifying registration information for research purposes. These rules are in sections 48 – 56 of the Act. This procedure also sets out guidelines for the collection and use of health information by physician members for research purposes.

2. Ethics Committees

The following committees and boards are designated as ethics committees for the purposes of this procedure:

- Alberta Cancer Board – Research Ethics Committee;
- College of Physicians and Surgeons – Research Ethics Review Committee;
- Alberta Heritage Foundation for Medical Research – Community Health Ethics Research Review Committee;
- University of Alberta – Health Research Ethics Board;
- University of Calgary – Conjoint Health Research Ethics Board;
- University of Lethbridge – Human subject Research Committee.

3. Collection of Health Information

Before collecting health information from other custodians for research purposes, physician members shall obtain approval from the University of Calgary Conjoint Health Research Ethics Board and forward to the other custodians a written application for disclosure of the health information to be used in the research, the title of the research proposal and a copy of the Ethics Board's response to the research proposal. If the other custodian(s) agree to disclose the requested health information, the physician member shall sign a researcher agreement that complies with section 54 of HIA. (See section 5 of this procedure)

4. Use of Health Information

Before using health information from his or her health records for research purposes, physician members must determine whether the research purposes can be achieved without using identifying health information. If so, the physician member must strip, encode or otherwise transform the individually identifying health information to create non-identifying health information.

If it is not possible to achieve the research purposes with non-identifying health information, the physician member must submit a research proposal to the University of Calgary Conjoint Health Research Ethics Board and include with that proposal the consent form that will be used to obtain individual consent to this use of the individual's

health information or the rationale for not requiring such consent. The physician member must receive the committee's approval letter prior to commencing research. If the research is being carried out by an affiliate (e.g. student, research nurse or research fellow) the physician member may require the affiliate to sign a research agreement that complies with section 54 of HIA.

5. Disclosure of Health Information

If an individual has consented in the prescribed manner to having his/her registration information disclosed for the purpose of determining participation in a research project, the member physician may disclose that information to a researcher when the member believes that participation in the research project is in the patient's interests.

All requests for access to any other identifying health information for research purposes must be in writing and accompanied by the response of the ethics board to the researcher's proposal and an application for the disclosure of the health information to be used in the research.

Upon receipt of a request for disclosure, physician members may, but are not required to, disclose the health information applied for. If the physician member decides to disclose the health information, he or she may impose any conditions on the researcher that he or she feels necessary in addition to any conditions imposed by the ethics committee.

If consents are required from the individuals whose health information is being disclosed, physician members must verify that consent has been obtained either by seeing the consent forms from a random sample or from the full study population.

Physician members may assign costs associated with preparing the records for disclosure, copying health information and obtaining consent. Such costs must not exceed the actual cost of the work.

A research agreement must be entered into between the physician member and the researcher in which the researcher agrees to:

- comply with the Health Information Act and regulations;
- comply with any conditions imposed by the physician member relating to the use, protection, disclosure, return or disposal of the health information;
- comply with any requirement imposed by the physician member to provide safeguards against the identification, direct or indirect, of an individual who is the subject of the health information;
- use the health information only for the purpose of conducting the proposed research;
- not to publish the health information in a form that could reasonably enable the identity of individuals to be readily ascertained;
- only contact individuals to obtain additional health information if the individuals consent to being contacted;
- allow the physician member to access or inspect the researcher's premises to ensure that researcher is complying with the terms of the agreement, and
- to pay any costs related to preparing the records for disclosure, copying the health information or obtaining consents for further contact of individuals.

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA**
**Sample Research Agreement for use when accessing electronic medical
records.**

This Agreement is between <name of lead researcher> (hereafter referred to as “the researcher”) and <name(s) of member physicians of MDERA> as represented by the MDERA governing board (hereafter referred to as “the members”), and is to enable the researcher to access the electronic medical records in the control of the members for the purpose of conducting <Name of the Research Study>.

The researcher has applied to the members as represented by the MDERA governing board for disclosure of health information as listed in Schedule A <Letter of Application> and has provided a summary of the research proposal <Schedule B>. The University of Calgary Conjoint Health Research Ethics Board met on <date of approval> and is satisfied that the researcher has met the requirements of section 50 of the *Health Information Act*.

The members have agreed to disclose the requested health information by providing access by the researcher to the electronic medical records that contain that information and subject to any other conditions imposed by the Ethics Board or the members.

This Agreement is in force from <date of commencement> to <date of end of project> and may be extended only with the consent of the members.

Responsibilities of Researcher

The researcher agrees to comply with:

- ***The Health Information Act*** and all regulations under that Act.
- The following conditions imposed by the members <list any conditions imposed pursuant to section 53(2)>

The researcher agrees that if the researcher or any member of the research team knowingly breaches the terms and conditions of this agreement, the researcher is guilty of an offence and liable to a fine of up to \$50,000.

Responsibilities of Custodians

The members agree to disclose the research information outlined in Schedule C <specifics of data elements> by making it available from the MDERA electronic medical record system.

If the researcher wishes to contact individuals to obtain additional data, the members agree to obtain consent from the subject individuals for such contact subject to payment of any costs incurred by the members in obtaining such consent.

Restrictions on Use and Disclosure of Health Information

The researcher agrees to only access the electronic medical record system to obtain the research information identified in Schedule C and to use it only for the purposes identified in Schedule A.

The research agrees not to use or disclose the information for any subsequent or other purposes not identified in Schedule A without the prior written approval of the members <and the consent of the individuals who are the subject of the information (if this is required)>. The members may arbitrarily withhold such approval.

The researcher agrees to disclose information only to individuals working with the research on the research project, as listed in Schedule D <List of Research Affiliates> and to ensure that all these individuals comply with the Privacy Policy and Procedures of MDERA and the *Health Information Act* and regulations under that Act.

Publication of Results

The researcher agrees that no identifying information or information that could be manipulated to identify any individual will be published.

The researcher agrees to provide the members with the proposed report of the results of the research for the members' review and the members agree to acknowledge its receipt. The report must include a statement that some of the information used in this study was provided by the members and that the members express no opinion on the interpretation and conclusions in the report.

Requirements to Safeguard Data

The researcher agrees to adequately safeguard the confidentiality and security of the information obtained from the electronic medical record and to safeguard the privacy of the individuals who are the subject of that information by ensuring that they cannot be identified directly or indirectly.

The researcher agrees to immediately report to the MDERA Privacy Officer any breaches of confidentiality and/or security respecting the information and to take steps to both remedy the breach and prevent a similar occurrence in the future.

The researcher agrees to allow the MDERA Privacy Officer to access or inspect the researcher's premises to confirm that the researcher is complying with this Agreement.

The researcher agrees to dispose of the information after the research has been completed <set out time period for disposal> by destroying it <indicate methods of destruction for both paper and electronic information and electronic storage devices> or by returning it to the MDERA Privacy Officer for destruction.

Financial Arrangements

<Provide details of any payments required for providing access to the EMR or obtaining consents>

Termination

In the event the Agreement is breached and/or health information is disclosed or used in contravention of the terms and conditions of the Agreement or the Act or the regulations, the Agreement may be immediately cancelled by the members, the research privileges of the researcher may be withdrawn, all research information will need to be returned to the members and the researcher may be found guilty of an offence under section 107 of the Act.

The Agreement may be terminated by either party on provision of 7 days written notice <or whatever terms MDERA wishes to impose. This may include conditions regarding retention, disposition or return of the information and any notification to be given by the researcher if the researcher is terminating the agreement prior to completion of the research>.

Indemnity

The researcher agrees to hold the custodian harmless from any third party claims, demands or actions for which the researcher is legally responsible, including those arising out of negligence, willful harm or crimes by the researcher, its employees and agents.

The researcher agrees to indemnify the members for any and all costs and expenses incurred by the members as a result of any breach of any term or condition of this Agreement or contravention of the Act or a regulation under the Act, or arising out of any unauthorized disclosure by the researcher of the health information that is subject to this Agreement. Such indemnification will survive the termination of the Agreement.

The members are not responsible for any bodily or personal injury or property damage or business losses that may be suffered or sustained by the researcher, its employees or agents in the performance of the Agreement.

The researcher has no recourse against the members for any loss or damage arising from the researcher's interpretation or analysis of the information received from the members or from the conclusions reached by the researcher. The researcher has no recourse against the members for any loss or damage arising from any advice provided by the members about the research information.

Transfer of the Agreement

The researcher may not transfer this Agreement to another person without the written consent of the members. Consent may be arbitrarily withheld. Successors are bound by the terms and conditions of the Agreement.

Notices

Any required notices under the Agreement shall be given to:

The Researcher <provide contact information>

The Members <provide contact information for Privacy Officer>

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA
Privacy and Security Procedure 4**

INFORMATION HANDLING AND SECURITY

1 Purpose

The information security provisions of the *Health Information Act* (HIA) require custodians to protect individually identifying health information in their custody or control by making reasonable security arrangements to protect against unauthorized access, collection, use, disclosure or destruction. The Act also requires custodians to take appropriate safeguards for the security and confidentiality of records, including addressing the risks associated with electronic health records. This procedure outlines administrative, technical and physical safeguards to protect confidential information and electronic health records.

This procedure sets out the minimum standards for participation in the University of Calgary, Department of Medicine Electronic Medical Record System.

2 Administrative Safeguards

- 2.1** Physician members shall adopt these procedures with respect to that physician's practice, so far as they are applicable.
- 2.2** The need for confidentiality and security of information shall be addressed as part of the conditions of employment for all affiliates, beginning with the recruitment stage, and included as part of any job descriptions and contracts. The performance of individuals shall be monitored to reduce the risk of error, fraud, or misuse of information. Affiliates must be aware of, and appropriately trained with regard to, MDERA policies and procedures for safeguarding information. Affiliates will sign the "Confidentiality Oath" appended to the Medical Doctors Electronic Record Application privacy policy if they have not signed a similar oath for the Calgary Health Region.
- 2.3** Patients and visitors shall be accompanied by a physician or affiliate to the examining room, the physician office or other non-public areas of the clinic.
- 2.4** The reception area of clinics shall be staffed when clinics are open and no-one shall be allowed behind the reception desk or in the administrative area without permission.
- 2.5** The least amount of information necessary for the intended purpose will be used or disclosed, and only to affiliates or recipients with a need to know. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information shall be made anonymous.

- 2.6 Reasonable steps shall be taken in the clinic areas to reduce the potential for overhearing identifying health information. [Examples include use of glass partitions; use of private offices for making telephone calls or for consultations; use of radio, television, music or white noise to mask conversations and use of first names only when talking to patients.]
- 2.7 Before implementing new administrative practices or information systems related to the collection, use and disclosure of health information, physician members or MDERA shall complete a privacy impact assessment (PIA) for submission to the Office of the Information and Privacy Commissioner. The PIA will describe how the new initiative will affect privacy, and what measures the custodian will put in place to mitigate risks to privacy.
- 2.8 Affiliates shall report any violations or breaches of information security as soon as possible to the privacy officer and physician member in order that corrective action can be taken to resolve the immediate problem and minimize the risk of future occurrence. Physician members must report a violation or breach to the Privacy Officer within 24 hours. The nature of the response will be determined according to the level of gravity of the breach / violation and may include dismissal. Any breach involving the EMRS must be reported by the Privacy Officer to the Alberta Medical Association (POSP Office) immediately. Any breach involving Alberta netCARE must be reported by the Privacy Officer to Calgary Health Region's Information Access and Privacy Office.
- 2.9 MDERA will enter into Information Manager Agreements on behalf of physician members with the University of Calgary and the Calgary Health Region.

3 Technical Safeguards

- 3.1 Each systems user must have a unique User ID/password pair for access to the computer operating system. Physician members may determine that a single User ID for the operating system may be deployed when a terminal is used by a number of personnel and use of unique User ID/password pairs would impair the efficiency of the clinic.
- 3.2 Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes.
- 3.3 Users shall enter a separate and unique password to access the EMR. This password must be at least 8 characters in length and consist of a mix of numbers and letters that cannot be easily identified. The password for the EMR shall be changed at least every 90 days as prompted by the system.
- 3.4 Access to the EMR from other than Calgary Health Region sites will require two factor authentication (password and fob) through the myCHR portal.
- 3.5 Access to regional or provincial electronic health records systems will be governed by protocols established by those systems. Physician members shall not transfer their passwords to affiliates but, if necessary, obtain distinct access rights for those with a need to access these systems.

- 3.6** Computer monitors must default to a screensaver or be locked after a maximum of 20 minutes of inactivity (for physicians) or such lesser period of time as does not affect the efficiency of the clinic operations, and require password entry to reactivate. Administrative workstations must be locked or on a screensaver when users leave the work station for a period of more than 5 minutes. All computers must be shut down at the end of the business day.
- 3.7** Confidential business or identifiable health information will not be sent via e-mail over public or external networks without the use of appropriate security measures such as encryption, password protection, virtual private network or by the use of a two factor authentication terminal services connection.
- 3.8** Downloading and transportation of identifying health information to portable computing devices is prohibited except for scheduling information of physician members.
- 3.9** Billing data will be transmitted by secure 128 bit encryption FTP transfer to Microquest, the University of Calgary Medical Group's billing agent.
- 3.10** If a physician member is not using Microquest as billing agent, the physician member must ensure that billing data is transmitted with the same level of security as outlined in 3.9 or in a sealed envelope if in paper format. Physician members are responsible for ensuring that their billing agent has adequate security and protection measures in place to protect their billing records.
- 3.11** To detect unauthorized access and prevent modification or misuse of user data in applications, systems will be monitored randomly by Calgary Health Region to ensure conformity to access policies and standards. Audit trails will be accessible in the case of a suspected privacy or security breach.
- 3.12** User rights and accounts will be assigned by the physician member. Maintenance of accounts for the EMR may be delegated to the Calgary Health Region's IT contact.
- 3.13** Physician members must ensure that there is high speed internet access from all access points.
- 3.14** All computers with access to the EMR must be protected by hardware firewalls, an antivirus program and a malware protection program. The antivirus and malware protection programs must be installed so as to update automatically and alert the physician member or designated affiliate of any potential infection.
- 3.15** All computers must have power bars and surge protectors to filter out power spikes.

4 Physical Safeguards

- 4.1** All records, both on and off site, will be held and stored in an organized, safe and secure manner. Any paper records will be housed in a locked room or in locked cabinets inaccessible to the public.
- 4.2** Clinical areas and physician offices that are not in CHR sites must have fire protection and suppression systems in place. At a minimum this includes smoke detectors and a fire extinguisher.
- 4.3** Physician members must ensure that there are controls in place over who has keys to areas where health information and computers are housed. Keys should only be assigned to those who need them and be returned to the physician or security personnel on termination of employment or contract. Locks must be changed if keys are not returned or it is suspected that copies have been made.
- 4.4** All exterior doors that allow public access to clinical areas and physician offices must be kept locked when the areas are not open to the public. When possible doors should be steel or solid wood and have deadbolts.
- 4.5** Buildings or areas that contain health information or computer equipment must be either alarmed or protected by 24/7 security. Physicians and affiliates should have unique alarm codes that are deactivated on termination of employment.
- 4.6** Identifying health information will not be displayed or left unattended in public areas. Computer monitors in reception areas or other areas where the public could view them will be positioned so that on-screen information cannot be viewed by the public unless the physician desires the public to be able to view that information.
- 4.7** Identifying health information that is transported between physician members and other custodians or third parties will be sealed, marked as confidential, and directed to the attention of the authorized recipient. Transportation of identifying health information within Calgary Health Region facilities or within the University of Calgary Health Sciences Centre will follow procedures specified by the health region or university as appropriate.
- 4.8** Affiliates will verify the credentials and identity of courier services used to transport health information.
- 4.9** All fax transmissions will be sent with a cover sheet that indicates the information being sent is confidential and giving a telephone number to call if received in error. Fax transmissions may be sent directly from the EMR application and all numbers will be verified before being entered into a fax directory. Reasonable steps will be made to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine and that fax numbers are confirmed before information is transmitted.
- 4.10** All computer equipment will be physically secured to standards set by Calgary Health Region. Portable computers shall be locked up when not in the physical possession of a user.

- 4.11** Information that is not confidential or sensitive in nature will be disposed of by placing it in recycling bins. Identifying health information will be destroyed by shredding following Calgary Health Region or University of Calgary waste management procedures. Destruction of records at the end of their scheduled life will be documented by listing the records / files destroyed, recording the date of destruction, and having an affiliate sign off that the destruction occurred.
- 4.12** Information that is scanned into the EMR will be retained for one week to ensure proper verification of entry into the EMR and backup of the data. It will then be shredded.
- 4.13** Physician members must ensure that any removal of computer equipment is properly logged and recorded in accordance with Calgary Health Region standards.
- 4.14** Prior to disposal of electronic storage devices (e.g. computers, hard drives, diskettes, tapes, CDs), the media will be destroyed or overwritten to Calgary Health Region standards so as to be unusable.
- 4.15** Patient health information, in any format (hard copy or electronic), is retained for a minimum of 10 years following the last documented contact with the patient or, in the case of a minor patient, when the patient reaches the age of 20 if that is longer than 10 years following the last contact.

5 Information Security in Contracting

Contractors performing a service for physician members are subject to these privacy policies and procedures. For greater surety, the following procedures will apply.

- 5.1** An agreement or contract shall be completed and signed between MDERA and all third parties who require access to the information systems and assets of physician members. This agreement will include specific information security provisions for the contractor, or will bind the contractor to the MDERA's information security policies and procedures.
- 5.2** Any related third party information security and privacy policies should be made available to the Privacy Officer upon request, including any updates or revisions that occur after execution of the contract.
- 5.3** All contractors and their employees who have exposure to and use MDERA information assets and systems shall sign a confidentiality (non-disclosure) agreement. Third party service providers should remind their employees on termination of their continued responsibility to maintain the confidentiality of physician members' information. Any privacy breach must be reported to the Privacy Officer or physician member within 24 hours.
- 5.4** Agreements or contracts will include provisions for destroying or returning all information assets, including hardware, system documentation and data, upon termination of agreements and in accordance with contract provisions reflecting records retention and data management policy
- 5.5** Contractors will be provided with a copy of the MDERA's privacy policies and procedures and will be asked to sign a declaration that they have received these documents

**MEDICAL DOCTORS ELECTRONIC RECORD ASSOCIATION OF
SOUTHERN ALBERTA
Privacy and Security Procedure 5**

ELECTRONIC MEDICAL RECORD SECURITY

The facility that houses the EMR server(s) will meet the following requirements.

1. Card access locks, with card access strictly limited to those employees whose functions require them to enter the data centre.
2. 24 hour operator supervision
3. On-site security staff
4. Security cameras
5. Intrusion detection system
6. Sign-in/sign-out log book for systematic identification / supervision of authorized guests
7. Uninterruptible power supply (UPS), which instantly provides a temporary supply of electrical to all computers in the centre in the event of power failure, allowing for a seamless switch to emergency generator power. UPS also “conditions” the power supply to the computers, eliminating power surges and depressions.
8. Halon fire suppression system
9. Raised flooring, allowing for isolation of electrical and data wiring, sufficient air circulation and temperature control, flood protection, and protection from dust which might accumulate on the sub-floor.

The network on which the EMR resides must have security procedures in place that meet or exceed the standards of ISO 17799 / BS 7799. The network host will have internal policies and standards, such as an Internet Firewall Policy, a Virus Protection and Prevention Policy, and a System Management Security Policy. These and other IT Security policies will meet or exceed those outlined in the MDERA Information Handling and Security Procedure.