Saskatchewan EMR Program Privacy and Security Resource Material Highlights

In Saskatchewan, physicians who are trustees as described in *The Health Information Protection Act* are required to establish privacy programs for their staff and others who may have access to patients' personal health information. The privacy program should consist of

- Written privacy and security policies and procedures,
- Privacy and security education for staff,
- Confidentiality agreements signed by staff,
- Notices for patients to explain the information management practices of the trustee,
- Processes to provide patients with access to their own personal health information and to request amendments to errors and omissions in their records.
- Signed agreements with third parties and other trustees.

The Saskatchewan EMR Program has developed the Privacy and Security Resource Materials to help physicians enrolled in the EMR Program meet their obligations under *The Health Information Protection Act*. The materials also help EMR physicians meet the expectations of the College of Physicians and Surgeons of Saskatchewan's new Privacy Policy Bylaw, Bylaw 23.2 and the privacy and security requirements of the EMR Program. The Resource Materials are comprised of several different sections.

- **Introduction and Acknowledgements**
- **Steps in Creating a Privacy and Security Policy Manual**
- **Checklist of Privacy and Security Requirements and Expectations** – maps the requirements of HIPA, the CPSS and the EMR Program to the sample policies.
- **Reference Manual** - guidelines on many of the privacy and security topics physicians will have question about at some time.
- **Sample Policy Manual for a Group Practice** – sample policies and procedures for each item on the checklist
- **Sample Policy Manual for a Sole Practitioner** – sample policies and procedures for each item on the privacy and security checklist
- **Templates: Forms. And Letters** – sample letters and forms required or expected under *The Health Information Protection Act*.
- **Templates: Checklists –** helpful checklists
- **Templates: Agreements** – sample agreements expected under *The Health Information Protection Act* and the EMR Program.

Privacy and Security Policy and Procedure Highlights

- What should be included in privacy and security education for staff?
- What to do to improve the accuracy and integrity of health records?
- How much information to provide patients in a notice?
- What is a physician required to do about health records when ceasing to practice or leaving a practice?
- What are the specific rules under HIPA around providing patients access to their own personal health information?
- When a patient asks for an amendment to his/her personal health information, when must a physician make the amendment?
- When must express consent be given by the patient?
- When can personal health information be used or disclosed without consent?
- Can a physician discuss a patient's diagnosis and treatment with a family member?
- When should the masking functionality in the EMR be used?
- What agreements are required with third parties and what agreements are expected among physicians who practice at the same clinic?
- What to do when there is a breach of personal health information.
- What can a physician put in place to manage patients when the EMR goes down?
- How to determine the retention period for health records.
- How to audit who has accessed personal health information in the EMR.
- What to do with paper records once they have been scanned into the EMR?