Steps in Creating a Privacy and Security Policy Manual

The Health Information Protection Act of Saskatchewan (HIPA) was proclaimed in September 2003 and governs the collection, use, and disclosure of personal health information in the province. The Act defines and places obligations on “trustees”, which include government institutions, regional health authorities, and health professionals including physicians who are not employees of another trustee. HIPA applies to verbal and documented personal health information in any form.

Maintaining confidentiality is a professional responsibility of physicians, and is a central part of the doctor-patient relationship. The patient, with few exceptions, has a right of access to, and to request an amendment of, his or her personal health information, but the physician owns the medical record. Physicians designated as trustees are accountable for the personal health information they collect, use, and disclose.

HIPA expands on the principle of confidentiality by requiring that physicians be transparent in how they collect, use, and disclose personal health information and that they take reasonable measure to protect the personal health information while it is in their custody or control. HIPA does not require physicians to collect express consent for direct patient care but the Canadian Medical Association and best practice recommends that express consent be collect whenever practical.

Step One: Understanding the Privacy and Security Resource Materials

The Saskatchewan Medical Association in association with CPSS and its partners in the Saskatchewan EMR Program, the Ministry of Health and eHealth Saskatchewan, has developed privacy and security resource materials to assist physicians and their staff develop policies and procedures to meet the expectations of HIPA and the College of Physicians and Surgeons of Saskatchewan’s (CPSS) Bylaw 23.

The Privacy Resource Materials are comprised of:

- **Highlights**
- **Introduction and Acknowledgements**
- **Steps in Creating a Privacy and Security Policy Manual**
- **Two checklists** of the privacy and security requirements and policies for physicians in the EMR Program, which also include the expectations of the CPSS
- **Privacy and Security Reference Manual**: Requirements and Good Practices for Protecting Personal Health Information
- **Sample Policy and Procedure Manual for a Group Practice**
- **Sample Policy and Procedure Manual for a Sole Practitioner**
- **Templates: Forms and Letters**
- **Templates: Agreements**
- **Templates: Checklists**
- ***The Health Information Protection Act***

- **CPSS Bylaw 23**

The **Privacy and Security Reference Manual** is comprised of guidelines on many of the privacy and security topics physicians will have to address at some time in their practice. The guidelines do not focus solely on the needs of the EMR physician so the **Reference Manual** is suitable for use by any physician developing privacy and security policies and procedures.

The sample policy manuals provide examples of the policies and procedures that EMR physicians should have. Non-EMR physicians should use the **Sample Policy Manual for Non-EMR Physicians** available on the SMA website.

There are also templates for forms, letters and checklists to use in medical practices which focus on the requirements of EMR physicians but they can also be used for non-EMR physicians. The "Templates: Agreements" are specifically designed for physicians participating in the EMR program.

Structure of the Reference Manual and Sample Policy Manuals

The **Reference Manual** and the sample policy manuals are both structured in the same way and include the following Sections.

Accountability:
This includes the general responsibilities of physician under HIPA. This section discusses the roles and responsibilities of a privacy officer, the obligations of employees, and others who are subject to the policies and procedures, and other requirements of HIPA.

Patient Access, Amendment, and Authorized Representatives:
HIPA is very specific about patients' rights to have access to, or a copy of, their own personal health information, and to ask for amendments when there are errors and omissions. This section also includes information about who are authorized patient representatives.

Collection, Use, Disclosure and Consent:
This addresses patients' right to consent to certain collections, uses, and disclosures of their personal health information. There is an explanation of the different types of consent under HIPA and how to manage a patient's consent directive. It also addresses when expressed, implied or deemed consent can be used and what uses and disclosures of personal health information are authorized without consent under HIPA.

Safeguards:
This contains overviews of some of the tools that physicians can use to mitigate risks such as agreements, breach management strategies, and business continuity and disaster recovery plans. While these are not specifically required in HIPA, they will help physicians meet some of their general duties under the legislation to protect personal health information.

Guidelines on other safeguards:
This includes information on retention, storage, and destruction of records. This section provides advice applicable to both paper and electronic information.

Step Two: Understanding the Benefits of Written Policies and Procedures

Many physicians question the need for written policies and procedures. Beside the legal and professional requirements, good written policies can contribute to a well-managed practice.

- Policies and procedures provide consistent direction for employees and others on how personal health information should be managed to protect the privacy of patients.
- Policies and procedures allow physicians to guide the operation of a medical practice without constant management intervention, and staff to carry out their job and make decisions within defined boundaries.
- Clear procedures can support new and temporary staff with fulfilling their duties in a manner that is consistent with established practices.
- By following documented policies and procedures, a medical practice can reduce the risk of a privacy breach, can identify improvements in procedures, and ensure compliance with HIPA, professional standards of practice and Saskatchewan EMR Program policies.
- Policies and procedures need to be reviewed and updated on a regular basis. Physicians who are trustees should review them annually, when staff have frequent questions on how to do a particular activity, when activities are performed inconsistently or there is an increase in potential breaches or an actual breach occurs.
- It will be the physicians and staff who will use the policies and procedures daily; however they should be shared with third parties that have or may have access to personal health information. Patients can also be provided with a copy upon request.

The sample policy manuals; one for a sole practitioner and the other for group practices are examples of the policies and procedures that meet the requirements of HIPA and the CPSS Bylaw 23. They are designed to be used with the **Privacy and Security Reference Manual: Requirements and Good Practices for Protection Personal Health Information** when further information is needed.

Physicians must carefully review the appropriate sample policy manual and adapt it to their practice. The text in bold in the sample manuals is a requirement of HIPA.

There is no standard format for policies and procedures, however it is a good idea to include with each policy and procedure the title, the legislative and/or CPSS reference, and the date the policy came into effect with any revision date(s).

Policy Statement

- A policy statement is the permanent expectation of the behaviour of physicians, employee, other health professionals, and medical students and residents with regard to the policy.
- The policy statement should only change when there are changes to HIPA, the

CPSS Regulatory Bylaws, the scope of practice at the medical practice, the Saskatchewan EMR Program privacy policy, or contractual requirements.

- There should be enough detail in the statement to make the objective clear without it being cumbersome.

- Policies are written to reflect general behaviours; exceptions to the policy should be addressed in the procedures, including the conditions under which an exception is appropriate.

- When the word "must" is used in the sample policy manual it means it is a requirement under HIPA. "May" is used, as it is in HIPA, when a physician has discretion in how the HIPA requirement is met. "Should" and "recommended" generally refers to the expectations of the College of Physicians and Surgeons or a good practices.

Procedures

- The ultimate goal of every procedure is to provide a clear and easily understood plan of action required to be carried out or implemented to achieve the policy statement.

- Procedures should be written in a consistent style and format to encourage maximum usability.

- Procedures should evolve over time as the medical practice identifies improvements in how the policy can be met and to further minimizing risks.

- Depending on the policy, procedures may be quite detailed and include who is responsible to carry out specific tasks and what should be achieved by the task.

- Some of the procedures in the sample policy manuals are only used by the privacy officer or office manager, such as the details around providing access to personal health information. These can be incorporated into a separate procedures manual for these two people.

Forms

- If a policy requires a form or letter these should be included in the policy manual.

Step Three: Preparing the Sample Policy Manual

	Word 2003	Word 2007/ 2010
Download	Open the sample policy manual on the USB key or download from the SMA website	Open the sample policy manual on the USB key or download from the SMA website
Save	Click the "File" tab on the top left hand corner of the screen. Click "Save As" and select the folder the manual will be saved in and name the file.	Click the "File" tab on the top left hand corner of the screen. Click "Save As" and select the folder the manual will be saved in and name the file.
Remove the dates in the header	Click on the "View" tab and then on "Header and Footer". Block and delete the text in the Header. Type in the name of the clinic and the date you anticipate the policies will be approved.	Click on the "Insert" tab and then on "Header". Select "Edit Header" near the bottom of the drop-down box. Block and delete the text in the Header. You will have to block and delete both logos in the header separately. Type in the name of the clinic and the date you anticipate the policies will be approved.
Remove the Logos from the footer	If the Header is still open, move the cursor to the box that opened when you opened the header. The box has several small pictures. As you move your cursor over the small pictures there is an explanation of what is does. Click on the picture that says "Switch between Header and Footer". Double click on the logo until six or so small circle appear around the logo. Press the "delete" button.	Move to page 1 of the Manual and block and delete the current header "Privacy Resources Materials….." Click on the "Insert" tab and then on "Footer". Select "Remove Footer" near the bottom of the drop down box. Then block and delete logos.
Add Page Numbers	Click on the "Insert" tab, Select "Page numbers". Click on the "Format" box. Select "Start at". Be sure the number in the box is "1".	Click on the "Insert" tab and select "Page Number". Select "Format Page Numbering" and select "starting at". Be sure the number in the box is "1". Select the location you want for the page number from the drop down box. The page number will appear at the bottom centre of the page.
Change the name of the clinic throughout the document	Click on the "Edit" tab. Select "Replace". Type in "Forest Medical" or "Dr. Rahal" in the "Find" box and the name of your clinic in the "Replace" box. Select "Replace All" For the sole practitioner manual repeat the above step	Click on the "Home" tab. Select "Replace" Type in the top right-hand corner. Type in "Forest Medical" or "Dr. Rahal" in the "Find" box and the name of your clinic in the "Replace" box. Select "Replace All" For the sole practitioner manual repeat the above step

Read through the revised Policy Manual	Make changes to policy statements and procedures to reflect how the medical practice will meet the requirements of HIPA and the expectations of the CPSS.	Make changes to policy statements and procedures to reflect how the medical practice will meet the requirements of HIPA and the expectations of the CPSS.
Update the Table of Contents	Click anywhere in the table of contents. Right click and select "Update field". If no policies have been updated or deleted select "Update page number only". Otherwise select "Update entire table".	Click anywhere in the table of contents. Right click and select "Update field". If no policies have been updated or deleted select "Update page number only". Otherwise select "Update entire table".
Modify the Table of Contents	If some of the headings do not appear in the table of contents, you will need to change the format of the missing policy title. Highlight the title of one of the other policies. Click on the 'Format Painter' which is the picture of the paint brush in the toolbar. Go to the missing title and highlight it. The look of the title should change. Repeat the process for updating the table of contents. Modifying the title can also be done by highlighting the title; click on the "Format" tab, select styles and formats from the drop-down box. From the box select "Heading 1, Centre, 14pt, Bold".	If some of the headings do not appear in the table of contents, you will need to change the format of the missing policy title. Highlight the title of the policy. Click on the "Home" tab. Select "Heading 1". Repeat the process for updating the table of contents. Or highlight the title of one of the other policies. Click on the 'Format Painter' under the "Home" tab. Go to the missing title and highlight it.

Step Four: Using the Templates

There are three sections of templates, one for forms and letters, one for contracts, and the third includes some checklists to use in determining if best practices are being met. Each of these should be adapted to the requirements of the medical practice.

Step Five: Amendments and Questions

The information provided in these documents are to assist physicians in understanding their obligations and general duties under HIPA and the expectations of the CPSS Bylaw, it should not be construed as legal advice.

If you have questions or if you have some feedback about the **Privacy and Security Resource Materials for Saskatchewan EMR Physicians** please contact:

Saskatchewan EMR Program
Saskatchewan Medical Association
201 – 2174 Airport DriveEast
Saskatoon, SK S7L 6M6
(306)657-4557
EMR@sma.sk.ca