PREPARING YOUR MEDICAL PRACTICE FOR HIPA AND PIPEDA

TOP 10 THINGS TO DO

Background

On September 1, 2003, *The Health Information Protection Act* ("HIPA") was proclaimed into force in Saskatchewan. On January 1, 2004, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") came into effect throughout Canada. Both HIPA and PIPEDA require Saskatchewan physicians to, at a minimum, take certain basic steps in their management of personal health information in their custody and control.

The following is a list of the top 10 things that physicians can do to increase their compliance with HIPA and PIPEDA, as recommended by lawyers from MacPherson Leslie & Tyerman LLP ("MLT"):

It is very important for physicians to note that HIPA and PIPEDA do not necessarily replace or change existing ethical requirements related to the practice of medicine. Practices that were, prior to HIPA and PIPEDA, unethical, but now appear to be permissible under HIPA or PIPEDA, continue to be unethical (For example, HIPA and PIPEDA make it **optional** for personal health information to be disclosed without consent in a number of situations. Physicians may not exercise that option if to do so would violate an underlying ethical obligation). Conversely, where previously permissible practices are now illegal under PIPEDA or HIPA, those practices must cease.

Important Notice: The purpose of this list is to highlight some of the key steps in HIPA and PIPEDA compliance that must be taken by physicians. It is not intended to be an exhaustive list, nor is it intended to provide a complete statement of the legal obligations of physicians. Reference should always be made to the official text of HIPA and/or PIPEDA for a complete statement of the law.

Top Ten To-Do's	✓
1. Designate one individual within your medical practice who will be responsible for implementing and overseeing privacy [and access] compliance. ➢ This is a mandatory requirement under PIPEDA and, although HIPA does not specifically require a Privacy Officer to be appointed, it will be very	

difficult for a medical practice to ensure HIPA compliance and consistent application of the principles and requirements contained in HIPA without ensuring that leadership regarding privacy compliance and access issues is clearly designated within the medical practice. ➢ It will be important to ensure that the individual is well trained and has adequate managerial support and resources for doing the job. Training may involve the achievement of certification or accreditation in administration of privacy and/or access legislation, as applicable. Additional individuals may be designated to assist the Privacy Officer as necessary.	
2. Ensure that appropriate agreements are in place with service providers, affiliates, etc. that have access to personal health information under the control of your medical practice. ➢ Agreements entered into between your medical practice and any service provider or affiliate should contain provisions respecting the protection of the confidentiality and security of personal health information, and audit procedures that may be used to audit the information management practices of the service provider or affiliate. ➢ Your medical practice remains responsible for personal health information it provides to services providers. ➢ It is also important to have appropriate agreements in place with employees of your medical practice who may have access to personal health information. Requiring employees to sign a short privacy pledge, a sample form which is attached, helps to ensure that employees are aware of and accept their responsibility to protect the privacy of the personal health information they may have access to by virtue of their employment duties. ➢ Where existing agreements are in place with service providers, affiliates, etc. they should be reviewed to ensure they contain proper confidentiality and audit clauses.	
3. Inventory your information holdings and identify the various purposes for which your medical practice collects, uses and discloses personal health information. ➢ It is important to distinguish between primary purposes and any secondary purposes for which the personal health information is being collected, used or disclosed by your medical practice. ➢ Your medical practice must ensure that each purpose for which it is	

collecting, using or disclosing personal health information is properly authorized on a Deemed, Implied, Express or without consent basis under HIPA and/or PIPEDA. *[Note: The Saskatchewan Information and Privacy Commissioner (the "Commissioner") recommends that Express Consent, or alternatively in appropriate circumstances Implied Consent, be used wherever possible.]*	
4. Develop an external communications plan that will provide patients with reasonable notice of the medical practice's privacy practices. ➢ Options to consider for inclusion in your communications plan include privacy brochures, electronic policies, or posters which outline the possible uses for patient information, the patient's right to access their records, and the patient's right to request amendments to those records. ➢ Sample privacy brochures and posters can be found at the following Industry Canada web site: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00230e.html	
5. Develop, document and implement privacy policies and practices for your medical practice. ➢ The development and implementation of such policy and procedure is specifically required by both PIPEDA (section 4.1.4 of Schedule 1) and HIPA (section 16). ➢ For example, policies should be implemented for updating and ensuring the accuracy of information in personal health records, and for obtaining appropriate patient consent to collection, use and disclosure of information. ➢ The Commissioner has recommended that the following four areas be treated as a priority from a policy development perspective (see the December 2003 issue of the Commissioner's "FOIP Folio" newsletter at www.oipc.sk.ca): ▪ **Security** ▪ **Individual access to personal health information** ▪ **Disclosure of personal health information outside of the "circle of care"** ▪ **Consent (when it is required, what it consists of, how it is recorded, etc.)**	

6. Implement privacy awareness training for your personnel. ➢ Privacy breaches are frequently the result of human error. ➢ Employees must receive thorough training and be regularly reminded of their obligations and responsibilities under HIPA and PIPEDA. ➢ Training should be initiated with a notice to your employees reminding them of their obligation and responsibilities under HIPA and PIPEDA. A sample form of notice is attached.	
7. Obtain express consent from patients where required or practical. ➢ HIPA and PIPEDA contemplate three types of consent: Express, Implied and Deemed. The type of consent that is required or should be sought from a patient will depend on the circumstances surrounding the particular collection, use or disclosure of personal health information of that patient. In addition, HIPA and PIPEDA include several circumstances where personal health information may be used or disclosed on a without consent basis. ➢ Express consent is not always required under HIPA and PIPEDA. For example, consent is deemed where the collection, use and disclosure of a patient's personal health information occurs for the purpose of arranging, assessing the need for, providing, continuing or supporting the provision of a service requested or required by that patient (see section 27(2) of HIPA). Consent may be implied when an informed individual takes action that may lead to an inference that he or she is consenting to the collection, use or disclosure (i.e. voluntarily providing personal health information to a physician). ➢ Despite the fact that different types of consent are acceptable under HIPA and PIPEDA, the Commissioner recommends as a best practice that where practical, Express Consent of the subject individual should be sought prior to collection, use or disclosure of personal health information. ➢ For general discussion on the issue of consent in the context of health care, please refer to the following Industry Canada web site: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00207e.html	
8. Review existing security safeguards to ensure that personal health information under the control of your medical practice is properly protected. ➢ Maintaining adequate and appropriate physical, technical and	

administrative safeguards within your organization is now required by law (section 4.7 of Schedule 1 to PIPEDA and section 16 of HIPA establish a duty to protect personal health information). ➢ Appropriate safeguards include the implementation of proper record retention and destruction policies. It is very important to remember that all documents and records in the custody and control of your medical practice must be retained for any minimum periods prescribed by law, and securely disposed of at the end of any such retention period. The risk of a privacy breach is high if care is not taken to ensure secure disposal.	
9. Develop policies and procedures for dealing with requests by individuals for access to their own personal health information. ➢ Both HIPA and PIPEDA establish a right of access for individuals to their own personal health information. ➢ Your medical practice must be prepared to respond to any request for access on a timely basis and in an open, accurate and complete manner (section 35 of HIPA sets out the duty of organizations to assist individuals with requests to access their own personal health information). **It is important that this duty to assist is taken seriously and that the request is dealt with in a transparent and expeditious manner.** ➢ HIPA (Part V) and PIPEDA (Principle 9 in Schedule 1) contain detailed rules and procedures governing how requests by individuals to access their own personal health information must be handled. ➢ Regulations prescribing appropriate fees for access are pending. In the interim, trustees are encouraged to charge minimal fees, and to consider waiving fees in appropriate circumstances.	
10. Develop policies and procedures for dealing with privacy-related complaints and privacy breaches. ➢ Despite the best efforts of your medical practice, privacy breaches can occur. In order to deal with a privacy breach in a timely and transparent manner should one arise, your medical practice must have privacy concern handling policies and procedures in place and accessible to all employees. ➢ All privacy concerns should be investigated and a response provided to the complainant. Key objectives of the process should be the completion of a comprehensive internal review and transparent and timely communication with the complainant. ➢ All complainants should be advised by your medical practice that they	

have the right to raise their privacy concerns with the Commissioner. The organization may want to consider contacting the office of the Commissioner as a proactive measure for more serious concerns. ➢ Staff and contractors of your medical practice should be reminded that discipline may result from privacy breaches. The discipline proceedings applicable will depend on the seriousness of the particular breach(es). Intentional breaches of privacy may be referred to police or relevant professional associations for investigation.	

Useful Links:

- Saskatchewan Medical Association (Privacy Toolkit):
  http://www.sma.sk.ca/privacy/
- College of Physicians and Surgeons of Saskatchewan (see Newsletters):
  http://www.quadrant.net/cpss/
- Office of the Saskatchewan Information and Privacy Commissioner:
  http://www.oipc.sk.ca

Prepared By: **MacPherson Leslie & Tyerman LLP**
1500 McCallum Hill Tower I
1874 Scarth Street
Regina SK S4P 4E9
(306) 347-8000

For Further Information: Contact Randy Brunet at RBrunet@mlt.com or Brad Vance at BVance@mlt.com.

SAMPLE EMPLOYEE PRIVACY PLEDGE

The confidentiality of the personal health information of its clients is a key concern of _____ [insert name of medical practice] (the "Practice") and accordingly the Practice has policies, procedures and practices in place to protect the confidentiality of the personal health information of its clients. In understand that in order to emphasize the importance of the protection of confidentiality, the Practice requires employees to sign a confidentiality pledge. Therefore, based on the above, I the undersigned agree as follows:

(a) That I will only collect, use or disclose personal health information on a need-to-know basis for the purpose of performing services on behalf of the Practice;

(b) That I will only use or disclose personal health information in the custody and control of the Practice with the consent of the subject individual, unless I am using or disclosing personal health information for a purpose that will benefit the subject individual, to support the provision of services required or requested by the subject individual, or for another purpose authorized by *The Health Information Act*.

(c) That I will keep all personal health information in my possession in the strictest of confidence and take appropriate steps to protect the integrity, accuracy and privacy of personal health information;

(d) That upon no longer requiring the personal health information for the purposes of providing services on behalf of the Practice, I will return or destroy all copies of the personal health information in my possession in accordance with policies and procedures of the Practice, or as otherwise instructed by the Practice;

(e) That I will comply with all policies, procedures and practices of the Practice applicable to the management, handling and security of personal health information;

(f) I acknowledge that I have read this Confidentiality Pledge and understand that a breach of it may be in contravention of the *Health Information Protection Act* or other applicable laws.

Name (Please Print): _____

Position: _____

Signature: _____ Date: _____

Witness: _____ Date: _____

SAMPLE STAFF REMINDER NOTICE

HIPA Reminder for All Staff

- Client-related issues are not to be discussed in areas where you may easily be overheard. _____ [insert name of medical practice] (the "Practice") recognizes that certain treatment areas within its facilities may not permit complete confidentiality of discussions that take place during the provision of patient care. However, staff are required to take all reasonable precautions to ensure that discussions about client-related issues do not take place in public areas, including waiting areas and public hallways.

- Client-related issues are not to be the subject of gossip or coffee conversation.

- You do not have a general "right" to collect, use or disclose personal health information in the custody and control of the Practice. You are only authorized to collect, use or disclose personal health information that you "need to know" for the purposes of fulfilling your duties and job responsibilities.

- Only share information with other health care workers if you believe it is required in order for them to provide care or a service to a client. In the event that you do share information with other health care workers, be sure to share only the minimum amount of information possible.

- Remember that family, friends, and Practice staff may also be clients of the Practice. You are expected to respect their privacy and to refrain from using or disclosing their personal health information unless you have a "need to know" for the purposes of fulfilling your job responsibilities. Their personal health information must be treated with the same level of protection that would be given to any other client of the Practice, and must not form the subject of gossip or conversations unrelated to client care that may occur between staff.

- Protect personal health information by ensuring that this information is not easily viewed by people or staff who do not have a need to know. Client Charts are to be closed, and where available, stored in a central location. At a minimum, Client Charts are not to be left "open" while unattended.

- Protect personal health information by locking doors, filing cabinets or rooms where client records are stored.

- Client records must be secured and protected until the moment of destruction. Remember that patient management, scheduling, and staff assignment lists often contain personal health information and should also be secured and protected until the moment of destruction.

- Where possible, shred any document containing personal health information. All documents containing personal health information, including personal working notes

made by staff, must be disposed of in the blue recycling bins located in the Practice's facilities and must not be disposed of in regular garbage.

- All requests for disclosure of or access to personal health information should be referred to the Practice's designated Privacy Officer.

Tips for Clinical Staff

- Be prepared to tell a client why you are collecting their personal health information and who it might be shared with.

- Only collect personal health information that is needed for the admission, assessment, examination, or treatment of a client.

- Under HIPA, clients have a right of access to the personal health information about them that the Practice holds. This means that a client has the right to request copies of all notes taken by you in the course of providing care and can require an interpretation of those notes. As a result, you should assume that anything you write down may be accessed by the client. Be factual, objective, and professional when making notes.