# Update on Privacy and eHealth

***British Columbia Medical Association***

***July 2008***

# Contents

# Key points on EMR and eHealth privacy

- The data stored in an EMR (including the application service provider (ASP)-hosted PITO EMRs) remains completely within the custodianship of the physician within his/her private practice with no access by government or third parties[1]. Neither the PITO contracts nor the recently passed Bill 24 (the eHealth Personal Health Information Access and Protection of Privacy Act) changed that fact.

- The part of the EMR that will be shared outside the practice in the future as a stipulation of PITO funding is a medical summary called the Core Data Set that will be "pushed out" by the physician from the EMR. The use of the Core Data Set information was defined in the Physician Master Agreement (PMA) to include the use of data to support direct patient care in its nominal (identifiable) form and health system planning in its anonymous (de-identified) aggregate form.

- Initial PITO EMR implementations do not enable sharing of a Core Data Set. In the future when sharing of the Core Data Set becomes possible, it will be required only as permitted by legislation.

- The Personal Information Protection Act (PIPA) legislation dictates that physicians in private practice can only disclose confidential data with patient consent. This is unchanged by Bill 24 and PITO. The requirement under PITO to share the Core Data Set medical summary would therefore only apply where there is patient consent. *As such, PITO cannot and does not in any way require physicians to disclose confidential patient data contrary to the consent requirements of the PIPA legislation.*

- In the future when Core Data Set sharing becomes possible, physicians will have the opportunity to review the Core Data Set that the EMR automatically generates, modify it as appropriate, and approve it before making it available to other care providers outside of their practices.

- As the default, access to the shared Core Data Set will be restricted to care providers based on their professional scopes of practice and only for direct patient care needs. This access approach is known as "roles-based access".

- In addition to the default limitations defined through the roles-based access model based on scopes of practice and direct patient care needs, patients will have the right to assign disclosure directives further limiting access to their own information.

- While the clinical value is significant, physician use of eHealth systems (e.g., Pharmanet, CDM Toolkit) and EMRs is voluntary. Physicians have the right to terminate their PITO agreement at any time and retain the funds they have received with no ongoing financial commitments or commitment to share data. For example, if at any time all of the above protections ever fail to satisfy physicians' concerns for patient privacy, they always have the option to withdraw.

- The BCMA will notify physicians before any sharing of the Core Data Set becomes possible. Information on the privacy protections that have been established for data sharing and any concerns the BCMA believes exist will be provided.

[1] Except as already permitted equally with paper records (e.g. College, court orders, communicable diseases)

- The College of Physicians and Surgeons of BC has indicated they expect that physicians should be mindful of their ethical, professional, and fiduciary obligations to maintain patient privacy as they adopt EMRs. Additionally, the PMA makes provisions for the College to introduce additional requirements on the sharing of the Core Data Set should it find that necessary.

## THE BCMA's early work on privacy

The BCMA has been involved in assessing the risks and opportunities of moving to an electronic health information world for many years. In 2004, the BCMA "Getting IT Right" policy document addressed several key concepts regarding privacy of confidential medical records (Appendix A). Since then a number of important steps have been completed toward establishing the right foundations that will allow physicians to meet clinical needs and at the same time protect patient confidentiality.

In 2005, the BCMA created a "Privacy Toolkit" and later participated in the creation of the College of Physicians and Surgeons of British Columbia (CPSBC)'s 2007 Data Stewardship document. Through representation at a number of Ministry of Health (MOH) groups -- the MOH eHealth Privacy & Security Steering Committee (ePSSC), the MOH eHealth Privacy & Security Stakeholder Advisory Group (ePSSAG), and the MOH eHealth Privacy & Security Stakeholder Working Group (ePSSWG) -- the BCMA was instrumental in advocating for robust eHealth-wide policies, including disclosure directives, audit, and breach provisions.

The BCMA continues to work closely with all of the primary organizations involved in medical practice regulation and eHealth to ensure that new eHealth systems are introduced according to sound privacy principles. We have been working in collaboration with the College and the MOH, and in consultation with the Canadian Medical Protective Association (CMPA) and the Office of the Information Privacy Commissioner of BC (OIPC).

# Recent provincial legislation

The provincial government recently passed Bill 24, the eHealth Personal Health Information Access and Protection of Privacy Act (http://www.leg.bc.ca/38th4th/3rd_read/gov24-3.htm). Bill 24 introduced important new requirements to support privacy of health information stored by government entities, including legislating the right of patients to introduce disclosure directives to define how their information can be collected, used and disclosed, significant fines for contravention of portions of the Act, whistle-blower protection, and the creation of a Data Stewardship Committee (with representation from the College and BCMA) to oversee access, use, and disclosure of data used for secondary purposes such as research and health system planning.

Bill 24 provides the legislative authority that previously did not exist to set up the mechanisms that are recognized internationally as central to an eHealth privacy framework. It is important to note that Bill 24 in no way removes the privacy requirements affecting physician offices under the existing PIPA legislation, including the requirement for patient consent to disclose confidential patient data. Bill 24 sets an important minimum bar for eHealth privacy in general, but it does not preclude the addition of new standards in situations where they are necessary.

Bill 24 makes possible the definition of certain government eHealth databases as "Health Information Banks" to enable data sharing and secondary uses. The scope of Health Information Banks under Bill 24 is limited to databases held by "Health Care Bodies" as defined in Bill 24 and the Freedom of Information and Protection of Privacy Act (FOIPPA) and does not include physician offices (or EMRs) because health care bodies are strictly limited to the following:

(a) the ministry of the minister,
(b) a health care body as defined in the Freedom of Information and Protection of Privacy Act (FOIPPA),
(c) the Provincial Health Services Authority, and
(d) a society that reports to the Provincial Health Services Authority

Further to item (b), FOIPPA defines Health Care Bodies as:

(a) a hospital as defined in section 1 of the Hospital Act,
(b) a Provincial auxiliary hospital established under the Hospital (Auxiliary) Act,
(c) a regional hospital district and a regional hospital district board under the Hospital District Act,
(d) a local board of health as defined in the Health Act,
(e) a metropolitan board of health established under the Health Act,
(f) a Provincial mental health facility as defined in the Mental Health Act, or
(g) a regional health board designated under section 4 (1) of the Health Authorities Act

*(Excerpt from the Freedom of Information and Protection of Privacy Act available at http://www.qp.gov.bc.ca/statreg/stat/F/96165_07.htm#Schedule)*

Accordingly, physicians' electronic and paper medical records in their own private practices cannot be defined as Health Information Banks. However, the following medical records *are* affected by Bill 24:

- Data housed in health authority systems used by physicians (e.g. hospital information systems).
- Data provided to the government and housed in government systems (e.g. billing data).
- Data stored by any of the health care bodies as defined above.

Section 6(2) of Bill 24 states that prescribed persons can be required to provide data to a government Health Information Bank, but it is important to be aware that Section 6(2) is introduced with the phrase "Subject to any other enactment that prohibits disclosure." As such, physicians could only be required to disclose data to a Health Information Bank within the limitations of PIPA, which governs privacy in physician private practices and dictates that the personal information cannot be shared without patient consent nor against patient directives**.**

# Privacy and the Physician Information Technology Office (PITO)

The BCMA has been working with the Ministry of Health since the ratification of the 2006 Agreement to establish the Physician Information Technology Office (PITO). PITO implementation is well ahead of the other eHealth projects and, as such, is identifying and addressing many of these important privacy questions.

The primary purpose of the PITO program is to accelerate adoption of electronic medical records (EMR) by physician practices. The BCMA believes that PITO is an essential initiative and that it should not be compromised or delayed while the longer-term eHealth data sharing protocols are finalized.

There are six principles vital to ensuring privacy of EMRs and shared data (Core Data Set):

1. The data stored in a physician's own records (paper or EMR) must remain strictly confidential with the physician as the custodian.
2. Access to identifiable patient data must be limited to care providers based on professional scopes of practice and only accessed for direct patient care needs.
3. Patients must have the right to further limit who has access to their own identifiable data shared outside the physician's office (disclosure directives).
4. Patients must have the right to grant and revoke consent to the sharing of their identifiable data.
5. Data used for health system analysis must be aggregated and de-identified before disclosure.
6. Physicians must have the right to opt out (cease participation) in any data sharing program with no penalties, financial or otherwise.

Following is a description of each principle and how it is being addressed:

### *1. The data stored in a physician's own records (paper or EMR) must remain strictly confidential with the physician as the custodian.*

The PITO program is based on an application service provider (ASP) model of EMR delivery with hosting of the EMR provided by a third-party non-government ASP. In this model, the EMR vendor stores and manages the EMR computer server for the physician in their secure and professionally managed data centre (strictly within Canada). It is important to understand that under the PITO Program, neither the government nor any other party has access to the data in the vendor-hosted EMR (except as already permitted with paper records, such as for College audits or according to court orders). The physician's contract with the EMR vendor will stipulate that point explicitly.

This fact is unaffected by Bill 24 because a physician's private medical practice is not within scope of Bill 24 (i.e., the EMR cannot be designated a "Health Information Bank"). The fact that a physician will access their EMR over the government-provided Private Physician Network (PPN) rather than the Internet does not change this fact because the PPN is only a network and does not store data.

The remotely hosted ASP model of off-site servers stored in professionally managed data centres is increasingly becoming the standard across the country for EMRs -- not surprising as it is already the standard in every other industry and most other parts of health care. Many physicians have been using remotely hosted EMRs in BC and across Canada for years. Many of BC's most remote hospitals ,such as Terrace, Kitimat, Smithers, Invermere, and Nelson already use remotely hosted systems for their critical hospital data.

The remote-hosting server model has been extensively reviewed by the BCMA and has been scrutinized by privacy commissioners, provincial and national medical associations, and colleges across the country prior to its now widespread adoption. While it may seem relatively novel to some physicians in community practice within BC, remote hosting is not new in health care or even medical practice.

### *2. Access to identifiable patient data must be limited to care providers based on professional scopes of practice and only accessed for direct patient care needs.*

The larger questions of privacy regarding EMRs come when we consider sharing patient data outside the practice and EMR, namely sharing of the medical summary called the Core Data Set as stipulated in the Physician Master Agreement (PMA). The role and scope of the Core Data Set was stated in the PMA as:

- Sharing of a patient-identifiable subset of patient data that supports continuity of patient care, and
- Aggregation of a de-identified subset (Core Data Set) of key patient data that can support health system planning.

The notion of sharing a nominal (identifiable) Core Data Set is built on the Electronic Medical Summary (eMS) pilot projects on Vancouver Island and in the Okanagan and recommendation 13 in the 2004 BCMA "Getting IT Right" policy document that states ". . . following a successful pilot project evaluation, the Electronic Medical Summary (eMS) be introduced as a necessary feature of any Electronic Medical Record."

The PITO Core Data Set Privacy Policies incorporated into the PMA stipulate that the Core Data Set will only be accessible through a "roles-based" access model which is access based on professional scopes of practice combined with the notion of direct patient care needs only. Roles-based access makes it possible to differentiate what can be accessed by each type of practitioner based on scope of practice and other related factors. For example, what a patient's GP can see will be different from what either a walk-in clinic physician, a specialist, or an emergency department physician can access. Direct patient care needs establishes that the individual in that role has a legitimate need to access the information based on a "circle of care" relationship with the patient. This means that just being an emergency physician does not justify viewing a patient's file if that physician has not treated or is not currently treating that patient. The combination of the "roles-based access model" and "direct patient care needs" is used extensively within hospital information systems to define appropriate access. It is also used within some physicians' EMRs to differentiate what a physician can access compared to what their MOA, billing clerk, or office manager can see and modify.

### *3. Patients must have the right to further limit who has access to their identifiable data shared outside the physician's office (disclosure directives).*

In addition to the default limitations of the roles-based access model, the PITO Core Data Set Privacy Policies further stipulate that any Core Data Set medical summary that is shared (as in the eMS pilot project with the emergency departments in Oliver) will incorporate disclosure directives that allow each patient to mask (hide) data at their individual discretion so that other care providers cannot access that data. The masking through disclosure directives usually includes the use of a keyword release so that a patient can prevent access in general, but allow individual physicians access to their data on a case-by-case basis at his/her own discretion by providing the keyword. Bill 24 does not change the inclusion of disclosure directives in the PITO Core Data Set Privacy Policies, rather it reinforces it in legislation.

### *4. Patients must have the right to grant and revoke consent to the sharing of their identifiable data.*

The Physician Master Agreement (Appendix B) stipulates that EMR products will "automatically generate the Core Data Set as a normal business practice." The Ministry and the BCMA recently confirmed their existing mutual understanding that the phrase "automatically generate" was meant to connote ease of use for the physician by allowing the EMR software to pre-populate (automatically generate) on the screen a Core Data Set template, much like a referral template or the eMS template, providing the physician the ability to review, add/remove data, and approve before sharing. The term "automatically generated" has been misinterpreted by some to mean that the Core Data Set would be automatically uploaded without any physician involvement. This was not the intent of that phrase and would be contrary to the principles of privacy and good patient care.

It is important that the terms of the PMA and PITO Agreements be read in context of the Personal Information Protection Act (PIPA), which governs privacy in private physician practices. PIPA requires consent for sharing of information and prevents sharing without patient consent or where consent is declined (except in certain unique legislated circumstances such as communicable disease reporting).

As such, a physician could not disclose the Core Data Set contrary to a patient's wishes. The requirements and process for obtaining patient consent to share their information (whether explicit or implied, frequency, etc.) need to be determined. The BCMA and College intend to collaborate to harmonize their recommendations to physicians on how best to meet the requirements of legislation and ethical practice standards for consent. The PITO Core Data Set Privacy Policies explicitly state that the Core Data Set can only be shared in alignment with the policies of the College, so any such guidelines would directly define sharing of the Core Data Set through PITO.

### *5. Data used for health system analysis must be aggregated and de-identified before use.*

The PITO Core Data Set Privacy Policies stipulate that any Core Data Set that is to be used for health system analysis must be aggregated and de-identified (anonymized) before it is made accessible. To ensure that this process of de-identification is designed and managed appropriately, the PITO Core Data Set Privacy Policies further stipulate that the de-identification process and requests for access to the de-identified data will be overseen by a Data Stewardship Committee that will include representatives of both the BCMA and College. The recent Bill 24 legislation provides additional provisions regarding secondary use of data ,including significant fines and whistle-blower protection.

### *6. Physicians must have the right to opt out (cease participation) in any data sharing program with no penalties, financial or otherwise.*

It is expected that the provisions already put in place, combined with those that will be added over time, will create an environment for data sharing with which most physicians will feel comfortable.

Above all, however, physician autonomy, including the right to decline participation if situations change, is the ultimate protection physicians have to ensure the interests of their patients and themselves are upheld.

The PITO program is entirely voluntary (as defined by the PMA). Physicians participating in the program can terminate their PITO Registration Agreement at any time and for any reason at their sole discretion and retain all funding received to that point. This clause is contained in the PITO Registration Agreement that is signed by both the physician and government when the physician enters the program. Upon terminating the PITO Registration Agreement, physicians also have the right to immediately terminate their EMR and PPN contracts with no financial penalty. They can choose to continue their contract with their EMR vendor outside the PITO program and without any data sharing if they wish, as their contract is directly with their vendor, not through government.

Currently, as the initial EMRs are being implemented through PITO, there is no sharing of the Core Data Set. In fact, the best estimate is that any such sharing is probably two years away as eHealth builds up the infrastructure to allow physicians to exchange that information in a fashion similar to the eMS pilot project. The BCMA will continue to work with the College and the Ministry to ensure that when the Core Data Set does become shareable, such sharing will support clinical care while preserving patient privacy.

Before such data sharing becomes possible, the BCMA will provide an in-depth update for physicians so that each physician can individually confirm his/her comfort with the privacy provisions that are established. If they are not comfortable with the provisions put in place, they are free to cease participation in PITO without having shared the Core Data Set and without any commitment to share the Core Data Set.

# Going forward

The BCMA will continue to work closely with the College, Ministry of Health, and other parties over the coming months on these privacy-related topics. In particular, we intend to focus effort on the following:

- The role-based access model that will define regular (default) access to the identifiable Core Data Set based on scopes of practice and only for direct patient care needs.
- The mechanisms for enabling disclosure directives.
- The guidelines in accordance with PIPA and College policies for patient consent for sharing of the identifiable (nominal) Core Data Set.
- The functionality to be created within EMRs to automatically generate and present a template containing the Core Data Set for review and approval by the physician prior to sharing.
- The roles and responsibilities for creation and maintenance of the Core Data Set.
- The governance (data stewardship) model for oversight of the identifiable (nominal) Core Data Set shared for the purposes of direct patient care.
- Plans for evaluation of the clinical benefit of sharing the various elements of the Core Data Set.

The BCMA believes that when the Core Data Set is introduced, it should be on a limited pilot project basis, focused on specific clinical situations, to assess what data should be shared in which circumstances in order to maximize clinical value and minimize privacy and other risks. These pilot projects should build on the existing experience of the Electronic Medical Summary (eMS) pilot project.

While this longer-term work on privacy related to future data sharing progresses, PITO will be working closely with individual physician practices to help physicians prepare their offices for privacy standards appropriate for EMR adoption, including physical security, confidentiality agreements, office privacy policies and responsibilities, and other important items. It is important that we ensure that our own medical offices are consistently as secure as the eHealth systems.

Neither physician offices nor the EMRs used in those offices should be independent islands of information. However, sharing of confidential patient data must not jeopardize the fundamental principle of patient privacy or risk the sanctity of the physician-patient relationship.

The BCMA will provide further updates on privacy as PITO and the government's eHealth program proceed. Prior to any sharing of the Core Data Set through PITO, the BCMA will provide an in-depth update and description of the privacy protections in place so that physicians with PITO EMRs can make an informed decision as to whether they are comfortable proceeding to data-sharing with the privacy provisions in place at that time. For now, physicians can proceed with EMR implementations, knowing that such data-sharing is not currently possible and that they can opt out if they wish at any time.

# Appendix A

# Privacy-related excerpts from the BCMA policy document "Getting IT Right," 2004

4. That a "Privacy Toolkit" be developed jointly by the BCMA, the BC College of Physicians and Surgeons, and the BC Office of the Privacy Commissioner, outlining a strategy to protect patient information within physician offices that meets legislative requirements.

5. That the joint Health Information Technology (HIT) Committee develop electronic transfer guidelines that preserve doctor-patient confidentiality.

7. That an effective strategy be developed, which addresses the issue of patient consent for the collection, use, and disclosure of health information. This strategy should use implied consent for direct patient care and billings, while information for research purposes should require express consent.

8. That the role of physician, as primary custodian and with responsibility for stewardship of patient data, be maintained with the shift to electronic patient information.

10. That the security and privacy of electronic prescription information be protected through appropriate safeguards such as auditing systems and patient keywords.

12. That health IT systems be developed which integrate primary care providers, hospitals, and long-term care facilities through an Electronic Medical Record (EMR), such as pharmaceutical and laboratory information systems

13. That following a successful pilot project evaluation, the Electronic Medical Summary (e-MS) be introduced as a necessary feature of any Electronic Medical Record.

14. That incentives be developed to support virtual practice groups through the use of information systems that share relevant patient information.

16. That, in conjunction with the creation of a program to computerize physician offices, the Health Information Technology (HIT) Committee establish minimum requirements for health IT vendors operating in BC.

# Appendix B

# PITO Core Data Set Privacy Policies (per the Physician Master Agreement)

**Policy—Access to EMR Information**

**Pursuant to Article 3.4 of Appendix H of the Physician Master Agreement**

The Government and the British Columbia Medical Association (BCMA) have agreed to work collaboratively to co-ordinate, facilitate and support information technology planning and implementation for physicians within the e-Health Strategic Framework, including the development and implementation in British Columbia of standardized systems of Electronic Medical Records. Appendix H – Physician Information Technology Office (PITO) of the Physician Master Agreement among the Government, the BCMA and the Medical Services Commission dated November 1, 2007, provides for the establishment and support of PITO. Section 3.4 – Access to EMR Information, of Appendix H states:

> *The Government, through the Ministry, and the BCMA shall jointly develop and maintain a policy and clearly defined rules regarding the use, disclosure and access to EMR data and information in compliance with all applicable freedom of information and privacy legislation and any other relevant legislation. It is the intention of the parties that the policy and rules developed and maintained pursuant to this section will contemplate the availability of and allow to be used certain EMR data and information on an aggregate basis for health system planning by the Government, with appropriate protections for the privacy of individuals.*

Pursuant to Section 3.4 of Appendix H, the following policy will guide the use, disclosure and access of the Core Data Set through the Electronic Medical Record:

- Patients will be able to restrict access to their identifiable Core Data Set information through disclosure directives. In case of patient refusal to disclose their identifiable Core Data Set information, access to health care services will not be refused.
- Access to identifiable Core Data Set is permitted only for the purpose of direct patient care using a role-based access model that grants permissions to the appropriate provider roles according to the provincial eHealth privacy policy, which meets legislation, professions' scopes of practice and the policies of the College of Physicians and Surgeons of BC (CPSBC).
- Access to the identifiable Core Data Set, for purposes other than for direct patient care will be managed by the Data Stewardship Committee (the DSC) in accordance with provincial eHealth privacy policy, which meets legislation, professions' scopes of practice and the policies of the College of Physicians and Surgeons of BC (CPSBC).
- It is the Ministry's intention to establish the DSC consisting of representation from the CPSBC, Ministry of Health, Health Authorities, research community and general public. The Ministry will include a representative of the British Columbia Medical Association on the DSC.
- Access by the Ministry of Health to a de-identified aggregated Core Data Set will be permitted for the purpose of health system planning only, in accordance with the provincial privacy legislation. Policies and procedures to govern the access to the de-identified Core Data Set information will be developed based on this legislation and the policies of the CPSBC. The DSC will determine the process for linkage of data and subsequent de-identification to enable useful analysis while protecting patient confidentiality.
- Compliance with these parameters will be assured at every level of the eHealth as it exists in Health Authorities and Ministry of Health operations where the identifiable and de-identifiable Core Data Set information is used.

# Appendix C

# Glossary of Terms

| | |
|---|---|
| ASP | Application Service Provider - a secure and professionally managed data centre outside of physicians' offices where the EMR vendor can store and manage the EMR computer server for the physician |
| Bill 24 | eHealth Personal Health Information Access and Protection of Privacy Act, passed May 29, 2008 |
| Core Data Set | A medical summary shared amongst care providers to support continuity of care, and aggregated in de-identified form to support health system planning |
| eHealth | A broad term describing any electronic technology used to support the delivery of health care |
| EMR | Electronic Medical Record |
| eMS | Electronic Medical Summary pilot project |
| FOIPPA | The BC Freedom of Information and Protection of Privacy Act which governs privacy within publicly owned organisations |
| Health Information Bank | A government eHealth database that is designated by Ministerial order as a Health Information Bank in order that the privacy provisions of Bill 24 may apply (http://www.leg.bc.ca/38th4th/3rd_read/gov24-3.htm) |
| OIPC | Office of the Information and Privacy Commissioner |
| PIPA | The BC Personal Information Protection Act which governs privacy within non-governmentally owned organisations, which includes physician's offices |
| PITO | Physician Information Technology Office – the office created to implement the physician office EMR implementation agreed to in the PMA |
| PMA | Physician Master Agreement |
| PPN | Private Physician Network – secure, high speed, private network and secure email for BC physician offices provided by the government to support the implementation of PITO |