IT Developments in BC Health Care:

Confidentiality at the Crossroads

A BCPWA Background paper
August 1, 2006

Contents

Introduction - Agreement Reached

On March 11, 2006, it was announced that the BC Medical Association and the provincial Government had reached an Agreement for physician compensation and related matters for the period April 1, 2006 through March 31, 2012. Ratification of this Agreement by the BCMA's membership was announced on May 4, 2006.

The March 11 BCMA news release announcing the Agreement noted it "provides funding for the use of information technology in the delivery of care by physicians." The May 4 news release issued jointly by the BCMA and the provincial ministries of Finance and Health noted the ratified Agreement would provide "more resources to support full service family practice," and that "the BCMA elected to reinvest part of the incentive into information technology to enhance patient care."

Fairly innocuous stuff. The references cited are apparently the only public notice given of the provisions of the Agreement's "Schedule C", the provisions governing the new IT initiatives.

The Context – Development of "eHealth"

Warning: this section is fairly tough sledding; but, it really is necessary to an understanding of where Appendix C came from.

Because the IT developments provided in the Agreement's Appendix C are not new. Neither are they secret.

The concept was spelled out on pages 13 to 16 of the provincial Health Planning ministry's 2002 document *Information for Health; A Strategic Plan for Health Information Management in British Columbia, 2002/03 – 2006/07*. The first of six goals stated was to share people's health information electronically, and it held "Seamless care for individuals hinges on easy access to health records and care plans. Information needs to be shared across the full spectrum of health care from family physicians to hospital staff and community care providers. It needs to be available on the desktop, in a doctor's office, in outpatient clinics, at the bedside and on the move. Information also needs to be centred around the individual."

Intended to flesh out the first Campbell government's "New Era for Health Goals", the 2002 *Information for Health* document noted "The overarching strategy that underpins all future strategies for improving caregiver information is the Electronic Health Record (EHR) … a longitudinal collection of the personal health information of a single individual, entered or accepted by health care providers, and stored electronically. It can contain information about a person's health, what services they have received, where the service was provided and who provided the service."

(By November of 2005, this definition of the EHR had morphed into "a medical record or any other information relating to the past, present or future physical and mental health, or condition of a patient which resides in computers that capture, transmit, receive, store, retrieve, link, and manipulate multimedia data … EHR records includes patient demographics, progress notes, SOAP notes (subjective, objective assessment, and plan), problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports." – *eHealth Strategic Framework,* November 2005, p. 89 – see below.)

Although the second goal set out in *Information for Health* was "Public Access to Health Information", this did not mean individuals' access to their own EHR; rather, it meant general access to "Information that will help British Columbians improve wellness, learn about fitness, find and use appropriate health services effectively and become informed of the best options and treatment practices".

The first document to develop this Goal further was issued in January 2003. *Framework for an Electronic Health Record for British Columbians* proposed "… an information technology blueprint for the future – a future where health information is shared electronically to support health care decisions by caregivers." One of the 21 "building block projects of the EHR" envisaged by the document was "Citizen Access to their health information" – but it was one of only four such building block projects deemed to be not "critical to the development of a provincial EHR".

In January of 2005, the provincial Health ministry released the second iteration of its *Tactical Plan for Health Information Management in British Columbia: Key Projects 2004-05*. Pages 25 through 27 of that document detailed plans for an "Electronic Medical Summary" system intended "to deliver a standard subset of patient data suitable for communication amongst practitioners for the purpose of sharing the care of an individual patient. The system and standards will provide the integration and interoperability between disparate electronic medical record (EMR) systems and primary care physicians …". Continuing earlier documents' careless indifference to consumers, it lists the "stakeholders" in this project as: practicing physicians, nurses and other care providers, the BCMA, the College of Physicians and Surgeons, the College of Family Practice, the provincial Ministry of Health Services, the various Health Authorities – even "Electronic Medical Records Software Venders" … but not "consumers" or "patients" or "clients".

Finally, in April 2005 the "BC eHealth Steering Committee" (a "partnership between the Ministry of Health, the Health Authorities and the service provider community" that is "charged with accelerating the development and implementation of eHealth systems in British Columbia" in the words of Appendix C) published *BC eHealth Conceptual System Architecture*. It's sister (and much more substantial) document, *eHealth Strategic Framework*, was published in November 2005.

This latter document (*eHealth Strategic Framework*) starts with a "Vision for eHealth" that cites as it's very first element "A provincial EHR to facilitate the seamless, secure and timely sharing of accurate health information." It notes (at page 12) "Individual health care providers are essential to the design and adoption of eHealth".

Commendably, *eHealth Strategic Framework* contains a commitment to "Safeguard Privacy and Security" (pp 13-14); of the document's 92 pages, this commitment consumes three paragraphs covering a little more than half a page. In its entirety, this section states:

> *"Every eHealth project must place the utmost importance on the protection of personal health information as a key project priority, and must comply with provincial government requirements to protect personal information and secure technology systems. This is required by the legislation*

> *under which the health system operates, standard system operating procedures, and common principles of sound government management.*
> *"Adherence to all applicable Acts and Regulations protecting personal privacy is a mandatory part of any new procedural or systems development project. In addition, for system security and protection against unlawful access or malicious tampering, every effort must be made to ensure access is absolutely restricted to only those having a clear right and need to access personal health information or to access the systems within which such information resides. The transmission of information also has to be fully safeguarded from accidental or intentional interception and unauthorized users.*
> *"Trust in government processes and projects cannot be assumed, but must be earned through demonstrated actions and follow-through on commitments. Such trust can be seriously undermined, if individual privacy, confidentiality and system security are not strictly safeguarded. Public and provider trust is fundamental to realizing the eHealth vision of health information being accessible, when and where it is needed, to support personal health, health care decision making and health system sustainability."*

Unfortunately, nowhere is it spelled out how these comforting circumstances are to be effected. Indeed, the first attempt at any consultation with any healthcare consumer organization of which BCPWA is aware occurred in late July of 2006. Contact with the BC Freedom of Information and Privacy Association occurred, at that organization's request, a couple of months earlier.

Beyond, in essence, a commitment to "obey the law", it would seem little thought has gone into the implications of the eHealth initiative (and, especially, its EHR component) for such concerns as legitimate restrictions on access to patient information *within* the health care system, traditional doctor/patient confidentiality, and rights of patients to full control over the contents of their personal information when such is to be shared with persons in addition to the original recipient of that information.

Why is this important? As noted on page 23 of *eHealth Strategic Framework*, "Within 10 years of eHealth implementation, the majority of patient health information is expected to be maintained in a standardized, shareable electronic form. This will include medication histories, immunization records, laboratory test results, and other relevant patient information. The full patient record or a suitable subset will be easily transmitted to authorized care providers in other locations, and the results of specialist consultations will be electronically transmitted back to the primary care physician."

Further, through the implementation of the envisaged "Interoperable Electronic Health Record" (iHER), patients' hospital, home care, public health, laboratory, pharmacy and diagnostic imaging records will all be incorporated into one grand electronic record that can be viewed by any of the broad health care system's various operatives – all of it done over the internet, and all of it stored in facilities and by organizations completely independent of the individual patient's doctors' offices.

Finally, one small additional element of the whole eHealth project is a public health initiative that would, in unspecified ways, use the eHealth system (including the EHR) to develop "a client and population-centred information system to improve access, delivery and integration of health care services for managing communicable diseases." Among the benefits anticipated are

"Enhanced ability to recognize and manage potential communicable disease outbreaks" and "Faster response to public health issues".

With the exception of the document's section "Safeguard Privacy and Security" reproduced above, you will search through *eHealth Strategic Framework* in vain for a discussion of health care consumers' legitimate concerns for the maintenance of doctor/patient confidentiality in particular, and for the overall confidentiality of their health care records in general.

Appendix C

So. What the *Appendix C – Information Technology and Electronic Medical Record* addendum to the overall 2006 Agreement between the BCMA and the provincial Government does is provide the framework within which private practice physicians can be induced and assisted to participate in the emerging eHealth system. It runs to a little more than five pages of text. In quasi-legalese, it sets out how the EMR ("Electronic Medical Record", apparently the treating physician's customary record of a patient's medical history and treatment – and a crucial component of eHealth's larger EHR) system is to be effected at the level of doctors' offices.

At its core, Appendix C provides that, once the hardware/software is in place, "Custodianship of the EMR data shall normally reside with the physician", but "The EMR shall be hosted in an accredited, securely managed non Government third party service provider ("ASP") … Individual practices will have a secure and separate database for their data in this professionally managed environment."

Given this provision, Appendix C goes on to require physician participation "in the establishment and operation of core data set projects". These core data sets will include, for each identified individual patient:

- demographic information,
- current conditions,
- past medical and surgical history,
- allergies/alerts,
- current medications,
- immunizations,
- advance directives, and
- most recent and critical diagnostic data.

This is the same core data set that lies at the heart of the interoperable Electronic Health Record (iEHR) noted above. In other words, Appendix C is the means through which the key element of the entire eHealth strategy will be secured.

Importantly, Appendix C provides that "Physicians shall implement the EMR as their primary method of recording patient information on a voluntary basis." This is key – it seems to provide individual physicians with the option to decide on their own whether to participate or not.

Those who do decide to participate will be eligible to have the provincial Government pay for 70 percent of the cost of "the required hardware/software package", and "the administrative cost of EMR implementation … will be directly funded by the Government …" along with other inducements. This is an enormous incentive to participate. And it guarantees that those who do participate do so by securing the standardized hardware-and-software set in the standardized network specified by the provincial Government, thus minimizing future compatibility problems.

In the spirit of the *eHealth Strategic Framework*, Appendix C makes references to the development of "clearly defined rules" to ensure "compliance with freedom of information and privacy legislation" and with "all privacy laws and regulations and any other relevant legislation".

Unfortunately, what this necessarily boils down to is reliance by Appendix C for its protections of doctor/patient confidentiality and patient control over their own medical information on the provisions of the *BC Freedom of Information and Protection of Privacy Act* (FOIPPA). While the FOIPPA is admirable in many respects, it doesn't do the whole job here.

The Two Problems

1. According to BC's Information and Privacy Commissioner's website, the FOIPPA provides that any person may request access to records held by public bodies (including records of their own personal information) and may request the correction of their personal information, including their own personal information in records held by public bodies.

This at least ensures that individuals should be able to have access to their own EMRs and EHRs (although this has not been tested), and be able to secure corrections to incorrect information contained in them.

But it doesn't guarantee – indeed, it is has nothing to do with – physician-generated EMRs being "uploaded" to central servers, and with core data sets being extracted from those EMRs, for access and use by a host of players throughout the health care system. (This is because, as far as the FOIPPA is concerned, all of this information is collected legitimately for the purpose of giving the individual concerned timely access to appropriate health care. All of the envisaged uses are consistent with the reasons for which the information was collected originally. Indeed, substantial elements of the core data set are already "in the system", having been collected by BCMSP or FairPharmacare, among other players.)

This leaves individual health care consumers with one defence: withholding consent at the source. At any time you are free to decline to provide any information requested by your physician or to ask that any particular element of your record in your doctor's office be expunged.

But imagine for a moment the consequences of declining to give your doctor various aspects of your personal and personal health information. It could defeat the whole purpose of consulting a

physician. Indeed, this operational requirement for "full disclosure" is what lies at the heart of the time-honoured doctrine of doctor/patient confidentiality. It is widely recognized – including at law – that doctors secure information from their patients for vital medical and related purposes, and that such information ought not to be divulged to anyone else for any other purpose, ever. If such complete and dependable confidentiality were not dependable, it could have an intolerable "chilling" effect on the doctor/patient relationship, causing the withholding of occasionally crucial information and so reducing seriously the very effectiveness of that relationship. Further, access to sensitive but filtered-and-organized information by others in addition to the doctor who originally secured that information necessarily deprives those others of the *context* in which that information was supplied. That kind of knowledge and understanding can only come from a long-term relationship between patient and physician. As one physician deeply alarmed by and opposed to the current development of the EHR system in BC has put it, "*Having* all the information about a patient is not the same things as *knowing* all the information, and neither is the same thing as *knowing the patient*."

2. There is another problem that has run like a ghost through the entire evolution of the EHR paradigm. Throughout all of this planning and movement towards implementation, "patients" (aka "clients" and "consumers") are viewed simply as occasional seekers of generalized low- to mid-level health and medical information at best, and as passive suppliers of information with no other legitimate interest in the eHealth system's activities at worst. The concept that patients might have a legitimate – indeed, a vital – interest in the design and functions of the eHealth system seems never to have occurred to its proponents and architects.

No one would argue that the potential benefits of such a system as that envisaged in the overall eHealth package could be substantial. But – as AIDS activists will recognize better than most – the scope for error, abuse, and accidental or deliberate unauthorized disclosure of personal information is enormous. Given such alarming potential for harm, *it is absolutely imperative that individual and organized health care consumers be decisively involved in the development of the system and remain in control of their personal sets of information.*

The Solution - Empowerment

As with almost all instances where the interests of healthcare consumers and the interests of the healthcare delivery system have the potential to collide, the irreducible core of the solution lies with the doctrine of informed consent and with empowering individual health care consumers to be the masters of their own care.

In this instance that means a couple of things:

1. Individual doctors' EMRs maintained on their individual patients are strictly confidential and cannot be shared with any other person or information aggregation exceptin gonly those instances in which explicit informed consent is given to such sharing;

2. Except where explicit informed consent is obtained in each separate instance of discrete bits of health information, no person's health information contained in that person's doctor's EMR can be uploaded or in any other way shared with any other person or information aggregation; and

3. as is at very least implied in the FOIPPA, any person may at any time request and receive timely access to their entire EMR and EHR and may request such changes as they wish in the reasonable expectation that such requested changes will be effected with all due haste.

If these prior safeguards cannot be secured, then the implementation of EMRs as provided in Appendix C, and of the larger program of EHRs, must be prevented. It would simply be the case that the undoubted benefits would be outweighed by the certain costs.

What BCPWA Has Done So Far

In a June 7, 2006 letter to then BC Medical Association President Dr. Michael Golbey – sent immediately prior to the BCMA's annual convention – BCPWA Chair Paul Lewand wrote that the Society's Board of Directors was "… alarmed at what appears to be the requirement for physicians seeking IT funding to agree to such provisions as:

- hosting of their full patient charts (Electronic Medical Records – EMRs) on servers that are remote from the physician's office;
- the sending of a subset of "core data" – including patient identity and diagnoses – from those remote servers to other servers; and,
- the selection of available EMRs through a process in which the BCMA would be merely "consulted" – and individual patients would not be consulted at all (the potential implication being that the selection of EMRs will be via a Request for Proposal process rather than a process combining standards/functionality conformance and informed, that, in other words, the provincial Government would be deciding which EMRs physicians may use)."

He asked that the BCMA "…call an immediate halt to the implementation of the arrangements provided for in "Appendix C."

"More particularly," wrote Lewand, "we commend to your attention and to the attention of the delegates to the BCMA's AGM several of those motions which, we understand, are to be presented for consideration and disposition to the Association's membership, including:

- that the BCMA ensure that both patients and physicians are surveyed and consulted before any health IT initiative is undertaken that could undermine doctor-patient confidentiality, or patient trust in that confidentiality;
- that the BCMA ensure that explicit patient consent be required every time a physician uploads a patient's confidential clinical information to a computer that is accessible by a third party, and that the patient be able to control what is included in that information in real time; and,

- that the BCMA advocate for improvements in the confidentiality of patient information already stored on systems such as PharmaNet."

(In the event, the one substantial motion put to the floor of the BCMA convention regarding Appendix C was soundly defeated. No response to Lewand's June 7 letter had been received two months later.)

Lewand then sent a letter to BC Health Minister George Abbott on July 6 making essentially the same arguments and calling for implementation by the provincial Government of the same set of solutions.

Further, representatives of BCPWA have contacted several health care consumer organizations and the BC Freedom of Information and Privacy Association. Attempts are underway to build a broadly-based coalition in opposition to the current attempts to implement an EHR system in BC in the absence of appropriate safeguards.

What Individuals Can Do

There are two actions which BCPWA is currently suggesting concerned individuals can take.

First, notify your general practitioner and your various specialists that you are explicitly withholding your consent for the sharing by them of any of your confidential health information contained in the records they keep with any other person, excepting only such exchanges of information as they have previously undertaken in the normal course of their provision of health care services to you.

Second, write to the provincial Health Minister demanding a complete hault in the implementation of the EHR system until such time as a full and responsive public consultation with health care consumers has occurred and appropriate safeguards – including the requirement for explicit patient consent every time a physician uploads a patient's confidential clinical information to a computer that is accessible by a third party, and the requirement that the patient be able to control what is included in that information in real time.

Samples of both instruments (physician and specialist notification of withholding of consent, and letter to the BC Health Minister) are appended to this document.

A Note About Sources

All the documents cited in this background paper – with the exceptions of Appendix C to the Agreement between the BCMA and the provincial Health Ministry and the BCMA's news release quoted – can be viewed on-line at the provincial Health ministry's website:

www.healthservices.gov.bc.ca/. Copies of Appendix C can be obtained from BCPWA. Copies of the BCMA news releases can be obtained from their website (www.bcma.org).