Health information privacy and patient safety: A delicate balance

By Barry Burk and Christine Callahan

By 2010, half of all Canadians will have an electronic health record (EHR), and by 2015, that number is expected to be 100 per cent. That means paper medical records, lab tests, diagnostic imaging results and medication history currently residing at doctors' offices and hospitals will be available electronically to caregivers. EHRs bring important, positive changes to health care, but also lead to privacy concerns for both patients and care providers.

The benefits are many: fewer medical errors; less chance of adverse drug interactions; less duplication of medical tests; more accurate diagnoses; improved chronic care and; billions of dollars in cost savings to the health-care industry.

And because doctors, nurses and other care providers will have immediate access to important medical information, they can provide better care.

If a patient is traveling out of province and is admitted into the ER but cannot communicate, the care team can look for drug allergies and other potential health issues with the click of a mouse.

But even with the benefits, digitizing personal health information (PHI) raises important issues: If PHI is "out there" in cyberspace rather than in a folder in the doctor's office, who can access it, and who controls access to it? And what would be the impact on patient safety if PHI is blocked for privacy reasons?

According to some provincial privacy laws, once a patient has gone to a care provider for treatment, that patient has, essentially, given consent for his or her PHI – electronic or otherwise – to be used and shared with other health-care professionals. But this may not be completely in keeping with the patient's wishes. Although some patients want all doctors and nurses to have access to their entire medical record, others have sensitive PHI that they

would like to keep private.

It's a little-known fact patients can actually control the privacy of their health information. In several regions in Canada, health privacy law – or hospital privacy policy – permits patients to limit access to sensitive health information. And for good reason, as few types of information are more personal than PHI.

The reasons for restricting access to PHI may be as personal as the PHI itself. Does a radiologist need to know his patient is taking antidepressants? Does a dermatologist need to know her patient had an abortion 15 years ago? Or, if a hospital nurse is admitted to her workplace for treatment, should curious coworkers have access to her PHI?

Health-care providers are required by law to meet certain privacy requirements. But for medical staff, the privacy issue also raises safety concerns. If a patient can limit access to PHI, will the care team be able to get the information they need to properly treat the patient?

And if not, will the patient's health be at risk?

The key is to balance patient information privacy with caregivers' need to access PHI in critical situations. This is now achievable with technology. HIPAAT, an Ontario-based health-privacy software company, has teamed with IBM to address the issue locally, regionally and nationally.

HIPAAT's consent software, Privacy eSuite, enables patients to restrict access to sensitive health information. IBM's SOA Foundation software provides additional identity and access management capabilities to ensure when PHI is accessed – in any health-care setting, such as a hospital, clinic or health information network – it is done securely.

To decrease the patient safety risk, the software is able to quickly provide caregivers with "break the glass" access to restricted PHI in emergency situations, when permitted by law and by the patient.

HIPAAT and IBM technologies let patients decide:

- *who* can access their PHI (e.g. do not allow Dr. Jon Smith to access my PHI)
- *what* PHI can be accessed (e.g. do not allow anyone

to access my HIV-related medical files), and
- when (e.g. do not allow anyone to access PHI related to my visits from October 15 – 21, 2007).

Privacy eSuite and the SOA Foundation work together "in the background" on computer networks to help doctors, nurses and other health-care providers meet patient and legal privacy requirements. And patients are kept in the loop. All access to PHI is recorded in an audit trail so when required, patients can be advised who looked at – or tried to look at – their information.

Health information privacy and patient safety do not need to be mutually exclusive. With a Pan-Canadian EHR on the horizon, it's a delicate but important balance.

To find out about health information privacy rights, http://www.privcom.gc.ca

For information on HIPAAT, visit www.hipaat.com. For information on IBM, visit www.ibm.com.

Barry Burk is Vice-President, Healthcare Industry at IBM and Christine Callahan is Manager, Corporate Relations at HIPAAT.