

- BRENDAN SEATON, SENIOR EDITOR -

THE COMING CHAOS IN HEALTH INFORMATION PRIVACY

Brendan Seaton is the President of CareLink

Incorporated, a consulting firm headquartered in
Fredericton, NB that provides a wide range of services
focusing on security, privacy and confidentiality issues.

www.ehealthprivacy.com

Health enterprise CEOs and CIOs who have been complacent about the privacy issue should mark April 14, 2003 and January 1, 2004 on their calendars. These are the dates that the privacy provisions of the US Health Insurance Portability and Accountability Act (HIPAA) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA - formerly Bill C6) come into full force. By 2004 health care organizations and professionals in Canada will face a bewildering array of privacy legislation and other influences that will create chaos in the management of health information. The impact will be on a scale that will exceed Y2K.

Three major, and sometimes conflicting, forces are converging to complicate the lives of every consumer and provider of health care: a shifting legislative landscape, changing consumer attitudes, and international reaction to terrorist threats as a result of the tragedies in New York City and Washington DC.

The legislative landscape for health information privacy has always been confusing. A patchwork of provincial and federal legislation has resulted in inconsistent application of privacy rules across the country. With the exception of Quebec, Canadian laws have only applied to public sector organizations. Even public sector legislation is inconsistent in its application to health care. New Brunswick's new privacy law, the Protection of Personal Information Act, applies to hospitals, but Ontario's Freedom of Information and Protection of Privacy Act does not. Alberta, Saskatchewan and Manitoba have specific Acts dealing with health information. The rest of the country does not.

The current legislative landscape misses most independent health practitioners and private sector organizations in this country. The Federal government has partially addressed this imbalance with PIPEDA. Several provinces are rushing to introduce and pass similar legislation. However, given the timing we can now expect a somewhat confused and potentially conflicting environment in health care once PIPEDA takes effect.

PIPEDA is a piece of legislation implemented in response to the European Directive on Data Protection, passed in 1995 by the European Parliament. The Directive prohibited trade in personal information between the European Union and countries that did not have comparable privacy protection in place. As a result, PIPEDA applies to all commercial transactions, including any health care transaction where an exchange of money takes place (such as a claim for payment).

PIPEDA comes into effect 1n January 2002 for health care organizations that trade health information across provincial or international boundaries. In January 2004 it comes into effect for all organizations and commercial transactions, except in those provinces where substantially similar legislation has been passed by the provincial legislatures. As most health care activity takes place within provincial boundaries, the majority of health care organizations will have until 2004 to comply.

The implementation of PIPEDA will profoundly impact the legislative landscape in Canada. While the implementation of privacy protection is a laudable goal, a measure of chaos is expected in the Canadian health sector. Some of the implications include:

Inconsistent Application - Because of its inter-relationship with provincial privacy legislation, PIPEDA will be implemented inconsistently across the country. For example, New Brunswick and other Atlantic provinces have no intention of passing similar legislation, so PIPEDA will apply to much of the health sector. PIPEDA may not apply in Alberta, Saskatchewan and Manitoba, because health privacy legislation is in place at the provincial level.

Canada will continue to have a patchwork of privacy legislation across the country, resulting in different rights and privileges for Canadians living in different parts of the country.

Gaps in Privacy Protection - Even with PIPEDA, some parts of the health sector may fall through the cracks. For example, PIPEDA would not cover the non-profit sector that may hold large repositories of personal health information. Unless comprehensive privacy legislation is in place at the provincial level, significant amounts of personal health information will be without protection.

Competing Jurisdictions - In a number of provinces, both the federal and provincial governments will have jurisdiction over some elements of health information privacy. Many health care transactions will span jurisdictions. For example, an exchange of health information between a doctor and hospital in New Brunswick would be subject to both the federal and provincial Acts. Which one takes precedence? To confuse matters, the same transaction in Alberta would be subject to the provincial Act only. In Ontario it would be an exclusive federal matter, unless the province passes similar legislation before 2004.

Oversight - The federal government and some provincial governments have appointed privacy commissioners to oversee the application of the legislation. Which jurisdiction has oversight is a big question. There is the potential for confusion as the federal privacy commissioner rules on matters affecting physicians in New Brunswick and Ontario, but not in Alberta or Saskatchewan. Which privacy commissioner would have jurisdiction on a matter spanning both federal and provincial Acts is unclear.

Confusion - In most provinces, health care consumers and providers will be facing confusion concerning privacy protection. Who will they complain to - the federal or provincial privacy commissioner? Whose rulings must health care providers follow? Which jurisdiction will have the right to investigate and prosecute complaints in transactions spanning jurisdictions?

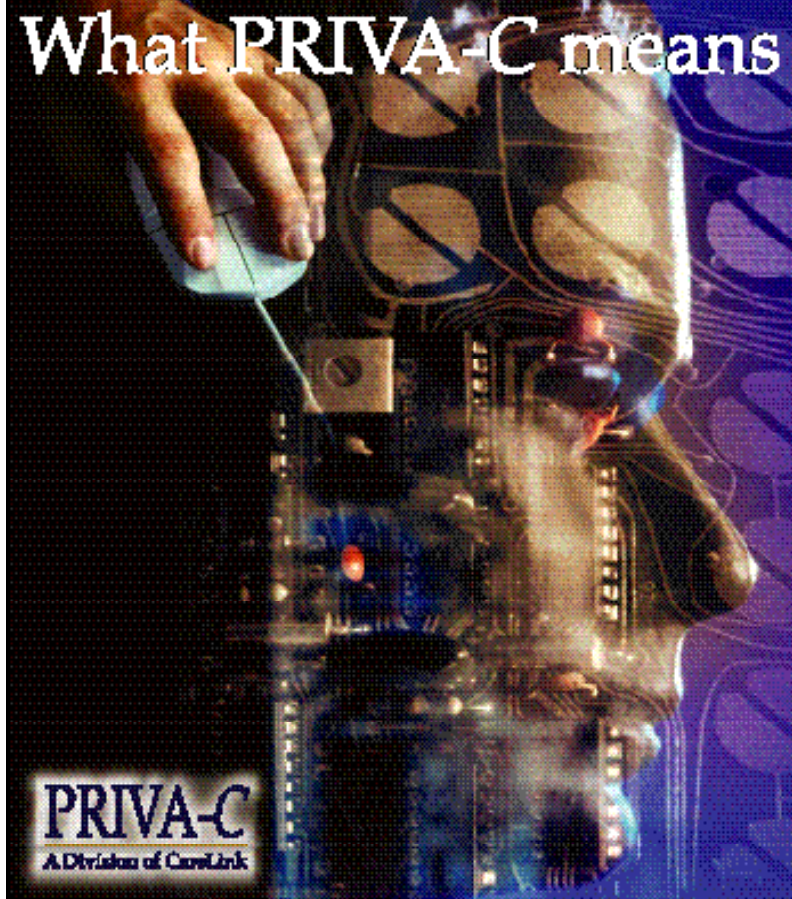
To add an international flavor to the issue, health care CEOs and CIOs must also look south of the border to what is happening in the United States with respect to HIPAA. Many privacy issues will be addressed in the design of our health information systems. Every HIS developer and vendor in the United States and Canada are now rushing to make their systems "HIPAA compliant". This means that those systems will be built to HIPAA specifications. While at the 100,000-foot level, both Canada and the United States have built their privacy frameworks on internationally accepted fair information practices, there are important and subtle differences between countries. It is not clear that solutions built to US specifications will satisfy Canadian legislative requirements.

Two years is a long time in our frenetic world. While we can anticipate the full implementation of PIPEDA in 2004, and prepare ourselves as best we can, changes on the national and world stage will profoundly affect how we end up addressing the privacy question. The commercialization of the Internet, and its increased use for health care purposes will raise, and in some cases resolve privacy issues in cyberspace. Early signs of concern about genomics and potential use, and abuse of genetic information are emerging. The current economic downturn has resulted in many consumers putting the privacy question on the back burner. However, as the economy rebounds, and business turns more and more to technology, consumer concern and alarm about privacy protection will resurface.

The latest wild card in the privacy game comes from the tragic events in New York City and Washington DC. In response to the threat of terrorism, governments and societies will challenge some of our current assumptions concerning privacy. Already, cries for more surveillance can be heard from many sectors of society. What effect might DNA testing to identify the 5000 victims of the tragedy have on the technology and its use? It is far too early to even speculate on the outcome of this development, but we can reliably predict that it will influence how we deal with the privacy question in the future.



What PRIVA-C means for you... and your clients.



New Legislation. New Concerns.
The result? Increased Accountability and Responsibility.

When it comes to privacy protection, we have the know-how and the tools — a total solution. And, we have the track record you can depend on. PRIVA-C's experienced consultants have helped health organizations deal with privacy issues for over a decade.

Let us help you navigate the pitfalls of privacy compliance. Build trust with your clients. Avoid risk.

A sound investment. Just ask our clients.

Offices located in Toronto and the Maritimes
Contact us at:
1-800-842-6071
info@csalink.ca
www.healthprivacy.com

PRIVA-C
A Division of CSALink