



- BRENDAN SEATON, SENIOR EDITOR -

# 17799: Winning Numbers in the Security Lottery

Brendan Seaton is the President of PRIVA-C, a division of CareLink Incorporated, a consulting firm headquartered in Fredericton, NB that provides a wide range of services focusing on security, privacy and confidentiality issues.

At the best of times security is a gamble. It is just like insurance. You invest some money up front to provide protection in the event of a disaster. The challenge for health care organizations is how to improve the odds. How do you bet as little cash as possible while ensuring that you are protected from security threats that can have serious consequences for your organizations, staff and patients?

ISO/IEC 17799 was recently published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), to provide an international framework for information security. Titled *Code of Practice for Information Security Management*, it represents the most comprehensive guide for health CIO's and security officers available.

ISO/IEC 17799 began life as BS7799, or British Standard 7799, originally published by the British Standards Institute in 1995. It quickly became recognized around the world as a comprehensive reference for security management. Many international organizations and consulting firms promoted its use in all sectors of the economy dependent upon information technology. BS7799 underwent a major revision in 1999 and was launched with formal certification and accreditation schemes.

In 2000 the ISO/IEC Joint Technical Committee (ISO/IEC JTC1), in collaboration with the British Standards Institute, adopted the British Standard through a special "fast track" procedure, in parallel with the normal approval process by national member bodies. BS7799 was reborn as ISO/IEC 17799 and published as an international standard.

ISO/IEC 17799 can provide a comprehensive framework for health organizations. It addresses the following areas:

**Security Policy** - a guide to the form and content of information security policies to provide management direction and support for information security.

**Organizational Security** - recommendations for the security organization required to manage the security function, including the responsibilities of management, outsourced operations and the use of specialist information security advice.

**Asset Classification and Control** - provides the foundation for determining the value and sensitivity of information and information system assets including inventories and classification guidelines.

**Personnel Security** - methods for managing people issues with respect to security to reduce the risk of human error, theft, fraud or

misuse of facilities.

**Physical and Environmental Security** - guidelines to prevent unauthorized access, damage and interference to business premises and information, and recommendations to prevent loss, damage or compromise of physical facilities or equipment.

**Communications and Operations Management** - a comprehensive section dealing with operational procedures and responsibilities, system planning and acceptance, protection against malicious software, housekeeping activities such as information backup and logging, network management, media handling and security, and the exchange of information and software between organizations.

**Access Control** - guidelines for access control policies, privilege management, user responsibilities, network/ operating system/ application access control, system monitoring and event logging, mobile computing and telecommuting.

**Systems Development and Maintenance** - specifications to ensure that security is built into information systems, this section outlines the definition of security business requirements, use of cryptographic controls, and security in development and support processes.

**Business Continuity and Management** - guidelines to counteract interruptions to business activities and to protect critical business processes from the effect of major failures or disasters.

**Compliance** - guidelines to avoid breaches of any criminal or civil law, whether they are statutory, regulatory or contractual and to ensure compliance with organizational security policies and standards, including system audit.

ISO/IEC 17799 is recommended by the COACH Guidelines for the Protection of Health Information, published last year, as a suitable foundation for the security programs developed and implemented by Canadian health care organizations. 17799 is not a competing document to the COACH Guidelines. They should be considered as companion documents. The COACH Guidelines can be used to "Canadianize" the ISO standard, and to complement security considerations with the broader issues of information privacy.

Adopting ISO/IEC 17799 is not simply a matter of paying a few dollars to ISO and downloading a copy of the code. It is a high level code of practice that provides a framework for the development of more in-depth security policies. Each section of the code effectively lays out the table of contents for each of your detailed organizational security policies, identifies the principle issues you need to consider, and provides useful suggestions and direction.

Why should health organizations in Canada adopt ISO/IEC 17799? As an international standard, it defines the meaning of “due diligence” with respect to information security. No Chief Executive, CIO, or security officer will ever get fired for following 17799. All major firms providing security or security audit are able to map your organization’s security practices to the international standard. If they can’t, don’t hire them. If you have already hired them, fire them. There are well-established certification programs and lots of educational programs available.

ISO/IEC 17799 can be used as a reference for outsourcing or systems development contracts. ISO standards are often used in this fashion. They provide criteria by which vendors and their products and services can be evaluated for compliance with security requirements.

This information security standard will be an important tool as we globalize health care delivery. While we rarely think about cross-border health care, there is a surprising amount of health care traffic between provinces and between Canada and the United States. The growing use of telehealth, bringing state of the art diagnostic and therapeutic technology to communities that cannot afford their own facilities, drives the need for a common approach to information security management. A recent EU ruling directs European countries with backlogs in waiting lists to allow citizens to obtain treatment from other member countries that have excess capacity for health care delivery. We can anticipate that Canadians will demand access to global resources for health care. An

international standard for information security provides a solid foundation for information sharing agreements between health care organizations in different jurisdictions.

While a security standard or code of practice could be intimidating to approach, ISO/IEC 17799 is surprisingly readable and contains common sense principles that are accessible to anyone with a basic understanding of information systems. I wouldn’t distribute them to end users, but each security officer, privacy officer, and any manager responsible for the custody or management of health information should have a copy.

I personally have started to apply ISO/IEC 17799 in several of my projects. I have met some resistance, especially from organizations that have adopted a competing approach to information security management. With a little mapping, it can be shown that the ISO standard complements and extends the organization’s security practices. There is a lot of comfort and peace of mind to be derived from applying an international standard.

As I said, no one will ever get fired for implementing ISO/IEC 17799.



# 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:  
1-800-842-6077  
info@carelink.ca  
[www.ehealthprivacy.com](http://www.ehealthprivacy.com)

**PRIVA-C**  
A Division of CareLink