

New ISO standard provides information security guidelines for health sector

by Janet Maillard,
Acting Communication Officer,
ISO Central Secretariat

The highly sensitive area of personal health information and how best to protect its confidentiality and integrity while assuring its availability for healthcare delivery is the issue addressed by the newly published ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002*.

ISO 27799:2008 applies to health information in all its aspects – whatever form the information takes, whatever means are used to store it and whatever means are used to transmit it. The standard specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines.

By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their size and circumstances.

Health informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. At the same time, the data they contain is confidential and its integrity must be preserved. Because of these critical requirements, and regardless of their size, location and model of service delivery, all healthcare organizations need to have stringent controls in place to protect the health information entrusted to them.

Further, the increasing use of wireless and Internet technologies in healthcare delivery, and the consequent growth of electronic exchange of personal health information between health professionals, not only makes the need for effective IT security management in healthcare all the more urgent, but also implies a clear benefit to adopting a common reference for information security management in healthcare.

As indicated by its title, ISO 27799:2008 is a companion to ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*. Professionals from the health sector have contributed their expertise to defining guidelines to specifically support the interpretation and implementation of ISO/IEC 27002 in health informatics.



Adaptability

An important consideration was the adaptability of the guidelines, bearing in mind that many health professionals work as solo health providers or in small clinics that lack dedicated IT resources to manage information security.

Although all of the security control objectives described in ISO/IEC 27002 are relevant to health informatics, some controls require additional explanations with regard to how they can be used to best protect the confidentiality, integrity and availability of health information. Also, there are some additional requirements that are specific to the health sector.

This International Standard therefore provides additional guidance in a format that persons responsible for health information security can readily understand and adopt.

ISO 27799 contains a practical action plan for implementing ISO/IEC 27002 in

a health environment. Taken together, these two standards define what is required in terms of information security in healthcare.

Three informative annexes are included in the new standard, covering respectively, the general threats to health information; tasks and related documents of the information security management system; and the advantages of support tools as an aid to implementation.

ISO 27799:2008, *Health informatics – Information security management in health using ISO/IEC 27002*, was developed by ISO/TC 215, *Health informatics*. It costs 154 Swiss francs and is available from ISO national member institutes (listed with contact details on the ISO Web site www.iso.org) and from ISO Central Secretariat (sales@iso.org).