HealthManagement
Promoting Management and Leadership

Volume 2 / Issue 2 2007 - Management

ISO/IEC 27799

What's In This Standard for Healthcare IT Managers ?

Even as European healthcare IT professionals brace themselves to understand the shifting contours of the emerging e-Health wave and cope with its implications, regulatory developments in yet another sphere are appearing on the horizon.

The ISO (International Standards Organisation)/ IEC ((International Electrotechnical Committee) 27799 standard concerns Security Management in Health. It is based on applying the more catch-all ISO 17799 information security standard to the specific (and sometimes 'special'/'unique') security management needs of healthcare.

INTERNATIONAL STANDARDISATION:

Three bodies are responsible for the planning, development and adoption of all International Standards:

ISO (International Organization for Standardization) is responsible for all sectors except Electrotechnical, which comes under **IEC** (International Electrotechnical Committee) and Telecommunications under **ITU** (International Telecommunication Union).

ISO is a legal association. Its members are the National Standards Bodies (NSBs) of some 140 countries (organisations representing social and economic interests at the international level), supported by a Central Secretariat based in Geneva, Switzerland.

An Emerging Standard

Officially, the ISO/IEC 27799 standard is known as "Health informatics – Information security management in health using ISO/IEC 17799". At the time of HITM going to press, it is officially classified as being "under development".

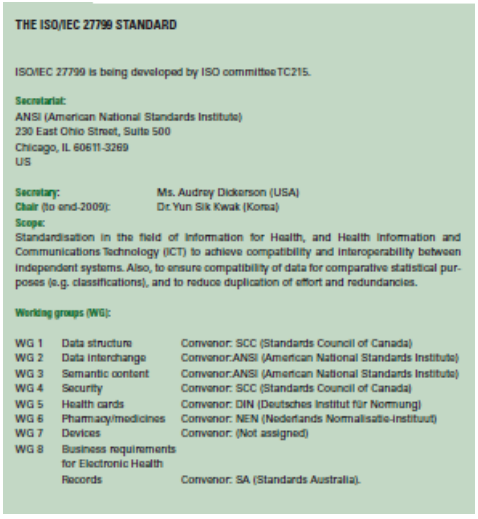
The ISO 27000 series – of which 27799 will form another new facet – is already used as a 'common language' for best practices in IT security management, and lays the frameworks for emerging European and international information security laws. It has moved to the top of the executive agenda after the growth in global compliance requirements, above all in the shape of the 2002 US Sarbanes-Oxley Act, which followed the gush of corporate and accounting scandals at Enron, Tyco International and WorldCom earlier in the decade.

Healthcare Faects Driven by Wider Business Concerns, Scandals

This, in turn, led to a rapid rise in the profile of previous healthcare sector-specific initiatives such as HIPAA (the Health Insurance Portability and Accountability Act), which was enacted in 1996. Although, HIPAA was aimed at providing job security in the US health sector, the Act's Title II (known as Administrative Simplification provisions) covers standards for electronic health care transactions, alongside national identifiers for providers, health insurance plans and employers. Crucially, the Administrative Simplification provisions also address the security and privacy of health data.

Personal Certifications: Proactive or Defensive

Such an environment evidently gives healthcare IT professionals a strong motive to pursue certifications like CISSP (Certified Information Systems Security Professional), which is itself based on another ISO standard (17024). They have also provided senior managers at healthcare institutions the incentive to move information security to the top of their agendas. In theory, ISO/IEC 27799 is designed to furnish a "minimum set of requirements" to provide adequate information security in healthcare, in terms of its integrity and availability. However, it is also directed at protecting personal health information –which is a relatively 'soft' but nonetheless crucial objective within the panoply of emerging e-Health rules.



THE ISO/IEC 27799 STANDARD

ISO/IEC 27799 is being developed by ISO committee TC215.

Secretariat:
ANSI (American National Standards Institute)
230 East Ohio Street, Suite 500
Chicago, IL 60611-3269
US

Secretary: Ms. Audrey Dickerson (USA)
Chair (to end-2009): Dr. Yun Sik Kwak (Korea)

Scope:
Standardisation in the field of information for Health, and Health information and Communications Technology (ICT) to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g. classifications), and to reduce duplication of effort and redundancies.

Working groups (WG):

WG 1	Data structure	Convenor: SCC (Standards Council of Canada)
WG 2	Data interchange	Convenor:ANSI (American National Standards Institute)
WG 3	Semantic content	Convenor:ANSI (American National Standards Institute)
WG 4	Security	Convenor: SCC (Standards Council of Canada)
WG 5	Health cards	Convenor: DIN (Deutsches Institut für Normung)
WG 6	Pharmacy/medicines	Convenor: NEN (Nederlands Normalisatie-Instituut)
WG 7	Devices	Convenor: (Not assigned)
WG 8	Business requirements for Electronic Health Records	Convenor: SA (Standards Australia).

ISO/IEC 27799: Who and What

ISO/IEC 27799 is being developed by ISO committee TC215 (see box), which is separate from the SC27 committee mandated with the development of other ISO 27000 standards. This has allegedly led to inefficiencies (such as duplication, lack of fit and clarity) as well as personal frictions. The Secretariat is US-led, which also controls two of eight working groups. Of the remainder, one still lacks a convenor, while the others are split as follows: Canada (two), Australia (one), Netherlands and Germany (one each).

Given below is a structural overview of ISO/IEC 27799:

1. Information security within information governance.

2. Information governance within corporate and clinical governance.

3. Health information requiring protection:

a. Personal health information

b. Pseudonymised data derived from above

c. Statistical/research data, including anonymised data.

d. Clinical data not related to specific patients (for example, on adverse drug reactions)

e. Data on health professionals and staff

f. Data concerning public health surveillance

g. Audit trail data generated by HIS containing personal health information or data about user actions in regard to such information

h. System security/configuration data – access control, and other security-related data for HIS.

4. Threats and vulnerabilities in health information security.

a. Description of over 20 threats to health information security. (TS)

Published on : Mon, 31 Dec 2007