

ISO 27799:2008-07 (E)

Health informatics - Information security management in health using ISO/IEC 27002

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
1.1	General	1
1.2	Scope exclusions	1
2	Normative references	2
3	Terms and definitions	2
3.1	Health terms	2
3.2	Information security terms	3
4	Abbreviated terms	5
5	Health information security	5
5.1	Health information security goals	5
5.2	Information security within information governance	6
5.3	Information governance within corporate and clinical governance	7
5.4	Health information to be protected	7
5.5	Threats and vulnerabilities in health information security	8
6	Practical action plan for implementing ISO/IEC 27002	8
6.1	Taxonomy of the ISO/IEC 27002 and ISO/IEC 27001 standards	8
6.2	Management commitment to implementing ISO/IEC 27002	9
6.3	Establishing, operating, maintaining and improving the ISMS	10
6.4	Planning: establishing the ISMS	10
6.5	Doing: implementing and operating the ISMS	18
6.6	Checking: monitoring and reviewing the ISMS	19
6.7	Acting: maintaining and improving the ISMS	20
7	Healthcare implications of ISO/IEC 27002	20
7.1	General	20
7.2	Information security policy	21
7.3	Organizing information security	22
7.4	Asset management	25
7.5	Human resources security	26
7.6	Physical and environmental security	29
7.7	Communications and operations management	30
7.8	Access control	36
7.9	Information systems acquisition, development and maintenance	39
7.10	Information security incident management	41
7.11	Information security aspects of business continuity management	42
7.12	Compliance	42
Annex A (informative)	Threats to health information security	45
Annex B (informative)	Tasks and related documents of the Information Security Management System	50
Annex C (informative)	Potential benefits and required attributes of support tools	54
Bibliography		57