DIN EN ISO 27799:2008-10 (E)

Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)

Contents

Page

Foreword 3

Introduction 4

1 Scope 7
1.1 General 7
1.2 Scope exclusions 7

2 Normative references 8

3 Terms and definitions 8
3.1 Health terms 8
3.2 Information security terms 9

4 Abbreviated terms 11

5 Health information security 11
5.1 Health information security goals 11
5.2 Information security within information governance 12
5.3 Information governance within corporate and clinical governance 13
5.4 Health information to be protected 13
5.5 Threats and vulnerabilities in health information security 14

6 Practical action plan for implementing ISO/IEC 27002 14
6.1 Taxonomy of the ISO/IEC 27002 and ISO/IEC 27001 standards 14
6.2 Management commitment to implementing ISO/IEC 27002 15
6.3 Establishing, operating, maintaining and improving the ISMS 16
6.4 Planning: establishing the ISMS 16
6.5 Doing: implementing and operating the ISMS 24
6.6 Checking: monitoring and reviewing the ISMS 25
6.7 Acting: maintaining and improving the ISMS 26

7 Healthcare implications of ISO/IEC 27002 26
7.1 General 26
7.2 Information security policy 27
7.3 Organizing information security 28
7.4 Asset management 31
7.5 Human resources security 32
7.6 Physical and environmental security 35
7.7 Communications and operations management 36
7.8 Access control 42
7.9 Information systems acquisition, development and maintenance 45
7.10 Information security incident management 47
7.11 Information security aspects of business continuity management 48
7.12 Compliance 48

Annex A (informative) Threats to health information security 51

Annex B (informative) Tasks and related documents of the Information Security Management System 56

Annex C (informative) Potential benefits and required attributes of support tools 60

Bibliography 63