

# E DIN EN ISO 27799:2014-10 (E)

Health informatics - Information management in health using ISO/IEC 27002 (ISO/DIS 27799:2014); English version prEN ISO 27799:2014

---

## Contents

Page

|              |                                                                     |           |
|--------------|---------------------------------------------------------------------|-----------|
| <b>1</b>     | <b>Scope .....</b>                                                  | <b>1</b>  |
| <b>1.1</b>   | <b>General .....</b>                                                | <b>1</b>  |
| <b>1.2</b>   | <b>Scope exclusions .....</b>                                       | <b>1</b>  |
| <b>2</b>     | <b>Normative references .....</b>                                   | <b>2</b>  |
| <b>3</b>     | <b>Terms and definitions .....</b>                                  | <b>2</b>  |
| <b>4</b>     | <b>Structure of this standard .....</b>                             | <b>4</b>  |
| <b>5</b>     | <b>Information security policies .....</b>                          | <b>5</b>  |
| <b>5.1</b>   | <b>Management direction for information security .....</b>          | <b>5</b>  |
| <b>5.1.1</b> | <b>Policies for information security .....</b>                      | <b>5</b>  |
| <b>5.1.2</b> | <b>Review of the policies for information security .....</b>        | <b>7</b>  |
| <b>6</b>     | <b>Organization of information security .....</b>                   | <b>8</b>  |
| <b>6.1</b>   | <b>Internal organization .....</b>                                  | <b>8</b>  |
| <b>6.1.1</b> | <b>Information security roles and responsibilities .....</b>        | <b>8</b>  |
| <b>6.1.2</b> | <b>Segregation of duties .....</b>                                  | <b>10</b> |
| <b>6.1.3</b> | <b>Contact with authorities .....</b>                               | <b>10</b> |
| <b>6.1.4</b> | <b>Contact with special interest groups .....</b>                   | <b>10</b> |
| <b>6.1.5</b> | <b>Information security in project management .....</b>             | <b>11</b> |
| <b>6.2</b>   | <b>Mobile devices and teleworking .....</b>                         | <b>11</b> |
| <b>6.2.1</b> | <b>Mobile device policy .....</b>                                   | <b>11</b> |
| <b>6.2.2</b> | <b>Teleworking .....</b>                                            | <b>13</b> |
| <b>7</b>     | <b>Human resource security .....</b>                                | <b>14</b> |
| <b>7.1</b>   | <b>Prior to employment .....</b>                                    | <b>14</b> |
| <b>7.1.1</b> | <b>Screening .....</b>                                              | <b>14</b> |
| <b>7.1.2</b> | <b>Terms and conditions of employment .....</b>                     | <b>15</b> |
| <b>7.2</b>   | <b>During employment .....</b>                                      | <b>16</b> |
| <b>7.2.1</b> | <b>Management responsibilities .....</b>                            | <b>16</b> |
| <b>7.2.2</b> | <b>Information security awareness, education and training .....</b> | <b>17</b> |
| <b>7.2.3</b> | <b>Disciplinary process .....</b>                                   | <b>18</b> |
| <b>7.3</b>   | <b>Termination and change of employment .....</b>                   | <b>19</b> |
| <b>7.3.1</b> | <b>Termination or change of employment responsibilities .....</b>   | <b>19</b> |
| <b>8</b>     | <b>Asset management .....</b>                                       | <b>19</b> |
| <b>8.1</b>   | <b>Responsibility for assets .....</b>                              | <b>19</b> |
| <b>8.1.1</b> | <b>Inventory of assets .....</b>                                    | <b>19</b> |
| <b>8.1.2</b> | <b>Ownership of assets .....</b>                                    | <b>20</b> |
| <b>8.1.3</b> | <b>Acceptable use of assets .....</b>                               | <b>21</b> |
| <b>8.1.4</b> | <b>Return of assets .....</b>                                       | <b>21</b> |
| <b>8.2</b>   | <b>Information classification .....</b>                             | <b>21</b> |
| <b>8.2.1</b> | <b>Classification of information .....</b>                          | <b>21</b> |
| <b>8.2.2</b> | <b>Labelling of information .....</b>                               | <b>23</b> |
| <b>8.2.3</b> | <b>Handling of assets .....</b>                                     | <b>23</b> |
| <b>8.3</b>   | <b>Media handling .....</b>                                         | <b>24</b> |
| <b>8.3.1</b> | <b>Management of removable media .....</b>                          | <b>24</b> |
| <b>8.3.2</b> | <b>Disposal of media .....</b>                                      | <b>25</b> |
| <b>8.3.3</b> | <b>Physical media transfer .....</b>                                | <b>25</b> |

|        |                                                                                                              |    |
|--------|--------------------------------------------------------------------------------------------------------------|----|
| 9      | Access control .....                                                                                         | 26 |
| 9.1    | Business requirements of access control .....                                                                | 26 |
| 9.1.1  | Access control policy .....                                                                                  | 26 |
| 9.1.2  | Access to networks and network services .....                                                                | 28 |
| 9.2    | User access management .....                                                                                 | 28 |
| 9.2.1  | User registration and de-registration .....                                                                  | 28 |
| E      | DIN EN ISO 27799:2014-10 <sup>2</sup> (QWZXUI <sup>2</sup> ISO/WD 27799 9.2.2 User access provisioning ..... | 29 |
| 9.2.3  | Management of privileged access rights .....                                                                 | 30 |
| 9.2.4  | Management of secret authentication information of users .....                                               | 31 |
| 9.2.5  | Review of user access rights .....                                                                           | 32 |
| 9.2.6  | Removal or adjustment of access rights .....                                                                 | 32 |
| 9.3    | User responsibilities .....                                                                                  | 33 |
| 9.3.1  | Use of secret authentication information .....                                                               | 33 |
| 9.4    | System and application access control .....                                                                  | 34 |
| 9.4.1  | Information access restriction .....                                                                         | 34 |
| 9.4.2  | Secure log-on procedures .....                                                                               | 35 |
| 9.4.3  | Password management system .....                                                                             | 35 |
| 9.4.4  | Use of privileged utility programs .....                                                                     | 36 |
| 9.4.5  | Access control to program source code .....                                                                  | 37 |
| 10     | Cryptography .....                                                                                           | 37 |
| 10.1   | Cryptographic controls .....                                                                                 | 37 |
| 10.1.1 | Policy on the use of cryptographic controls .....                                                            | 37 |
| 10.1.2 | Key management .....                                                                                         | 38 |
| 11     | Physical and environmental security .....                                                                    | 39 |
| 11.1   | Secure areas .....                                                                                           | 39 |
| 11.1.1 | Physical security perimeter .....                                                                            | 40 |
| 11.1.2 | Physical entry controls .....                                                                                | 41 |
| 11.1.3 | Securing offices, rooms and facilities .....                                                                 | 41 |
| 11.1.4 | Protecting against external and environmental threats .....                                                  | 42 |
| 11.1.5 | Working in secure areas .....                                                                                | 42 |
| 11.1.6 | Delivery and loading areas .....                                                                             | 42 |
| 11.2   | Equipment .....                                                                                              | 43 |
| 11.2.1 | Equipment siting and protection .....                                                                        | 43 |
| 11.2.2 | Supporting utilities .....                                                                                   | 44 |
| 11.2.3 | Cabling security .....                                                                                       | 44 |
| 11.2.4 | Equipment maintenance .....                                                                                  | 45 |
| 11.2.5 | Removal of assets .....                                                                                      | 45 |
| 11.2.6 | Security of equipment and assets off-premises .....                                                          | 46 |
| 11.2.7 | Secure disposal or re-use of equipment .....                                                                 | 46 |
| 11.2.8 | Unattended user equipment .....                                                                              | 47 |
| 11.2.9 | Clear desk and clear screen policy .....                                                                     | 47 |
| 12     | Operations security .....                                                                                    | 48 |
| 12.1   | Operational procedures and responsibilities .....                                                            | 48 |
| 12.1.1 | Documented operating procedures .....                                                                        | 48 |
| 12.1.2 | Change management .....                                                                                      | 49 |
| 12.1.3 | Capacity management .....                                                                                    | 49 |
| 12.1.4 | Separation of development, testing and operational environments .....                                        | 50 |
| 12.2   | Protection from malware .....                                                                                | 51 |
| 12.2.1 | Controls against malware .....                                                                               | 51 |
| 12.3   | Backup .....                                                                                                 | 52 |
| 12.3.1 | Information backup .....                                                                                     | 52 |
| 12.4   | Logging and monitoring .....                                                                                 | 53 |
| 12.4.1 | Event logging .....                                                                                          | 53 |
| 12.4.2 | Protection of log information .....                                                                          | 54 |
| 12.4.3 | Administrator and operator logs .....                                                                        | 56 |
| 12.4.4 | Clock synchronisation .....                                                                                  | 56 |

|        |                                                                                                                |    |
|--------|----------------------------------------------------------------------------------------------------------------|----|
| 12.5   | Control of operational software .....                                                                          | 57 |
| 12.5.1 | Installation of software on operational systems .....                                                          | 57 |
| 12.6   | Technical vulnerability management .....                                                                       | 58 |
| 12.6.1 | Management of technical vulnerabilities .....                                                                  | 58 |
| 12.6.2 | Restrictions on software installation .....                                                                    | 59 |
| 12.7   | Information systems audit considerations .....                                                                 | 59 |
| 12.7.1 | Information systems audit controls .....                                                                       | 59 |
| 13     | Communications security .....                                                                                  | 60 |
| E      | DIN EN ISO 27799:2014-10 <sup>2</sup> (QWZXUI <sup>2</sup> ISO/WD 27799 13.1 Network security management ..... | 60 |
| 13.1.1 | Network controls .....                                                                                         | 60 |
| 13.1.2 | Security of network services .....                                                                             | 60 |
| 13.1.3 | Segregation in networks .....                                                                                  | 61 |
| 13.2   | Information transfer .....                                                                                     | 61 |
| 13.2.1 | Information transfer policies and procedures .....                                                             | 61 |
| 13.2.2 | Agreements on information transfer .....                                                                       | 63 |
| 13.2.3 | Electronic messaging .....                                                                                     | 63 |
| 13.2.4 | Confidentiality or non-disclosure agreements .....                                                             | 64 |
| 14     | System acquisition, development and maintenance .....                                                          | 65 |
| 14.1   | Security requirements of information systems .....                                                             | 65 |
| 14.1.1 | Information security requirements analysis and specification .....                                             | 65 |
| 14.1.2 | Securing application services on public networks .....                                                         | 67 |
| 14.1.3 | Protecting application services transactions .....                                                             | 68 |
| 14.2   | Security in development and support processes .....                                                            | 69 |
| 14.2.1 | Secure development policy .....                                                                                | 69 |
| 14.2.2 | System change control procedures .....                                                                         | 69 |
| 14.2.3 | Technical review of applications after operating platform changes .....                                        | 70 |
| 14.2.4 | Restrictions on changes to software packages .....                                                             | 71 |
| 14.2.5 | Secure system engineering principles .....                                                                     | 71 |
| 14.2.6 | Secure development environment .....                                                                           | 72 |
| 14.2.7 | Outsourced development .....                                                                                   | 72 |
| 14.2.8 | System security testing .....                                                                                  | 73 |
| 14.2.9 | System acceptance testing .....                                                                                | 73 |
| 14.3   | Test data .....                                                                                                | 74 |
| 14.3.1 | Protection of test data .....                                                                                  | 74 |
| 15     | Supplier relationships .....                                                                                   | 74 |
| 15.1   | Information security in supplier relationships .....                                                           | 74 |
| 15.2   | Test data .....                                                                                                | 74 |
| 15.2.1 | Information security policy for supplier relationships .....                                                   | 74 |
| 15.2.2 | Addressing security within supplier agreements .....                                                           | 76 |
| 15.2.3 | Information and communication technology supply chain .....                                                    | 77 |
| 15.3   | Supplier service delivery management .....                                                                     | 78 |
| 15.3.1 | Monitoring and review of supplier services .....                                                               | 78 |
| 15.3.2 | Managing changes to supplier services .....                                                                    | 78 |
| 16     | Information security incident management .....                                                                 | 79 |
| 16.1   | Management of information security incidents and improvements .....                                            | 79 |
| 16.1.1 | Responsibilities and procedures .....                                                                          | 79 |
| 16.1.2 | Reporting information security events .....                                                                    | 80 |
| 16.1.3 | Reporting information security weaknesses .....                                                                | 81 |
| 16.1.4 | Assessment of and decision on information security events .....                                                | 82 |
| 16.1.5 | Response to information security incidents .....                                                               | 82 |
| 16.1.6 | Learning from information security incidents .....                                                             | 83 |
| 16.1.7 | Collection of evidence .....                                                                                   | 83 |
| 17     | Information security aspects of business continuity management .....                                           | 84 |
| 17.1   | Information security continuity .....                                                                          | 84 |

|                                                                                                |                                                                                                                           |     |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-----|
| 17.1.1                                                                                         | Planning information security continuity .....                                                                            | 84  |
| 17.1.2                                                                                         | Implementing information security continuity .....                                                                        | 85  |
| 17.1.3                                                                                         | Verify, review and evaluate information security continuity .....                                                         | 85  |
| 17.2                                                                                           | Redundancies .....                                                                                                        | 86  |
| 17.2.1                                                                                         | Availability of information processing facilities .....                                                                   | 86  |
| 18                                                                                             | Compliance .....                                                                                                          | 86  |
| 18.1                                                                                           | Compliance with legal and contractual requirements .....                                                                  | 86  |
| 18.1.1                                                                                         | Identification of applicable legislation and contractual requirements .....                                               | 86  |
| 18.1.2                                                                                         | Intellectual property rights .....                                                                                        | 87  |
| 18.1.3                                                                                         | Protection of records .....                                                                                               | 88  |
| 18.1.4                                                                                         | Privacy and protection of personally identifiable information .....                                                       | 88  |
| E                                                                                              | DIN EN ISO 27799:2014-10 <sup>2</sup> (QWZXUI <sup>2</sup> ISO/WD 27799 18.1.5 Regulation of cryptographic controls ..... | 90  |
| 18.2                                                                                           | Information security reviews .....                                                                                        | 90  |
| 18.2.1                                                                                         | Independent review of information security .....                                                                          | 90  |
| 18.2.2                                                                                         | Compliance with security policies and standards .....                                                                     | 90  |
| 18.2.3                                                                                         | Technical compliance review .....                                                                                         | 91  |
| Annex A Threats to health information security (informative) .....                             |                                                                                                                           | 92  |
| Annex B Practical action plan for implementing ISO/IEC 27002 in healthcare (informative) ..... |                                                                                                                           | 96  |
| B.1                                                                                            | Taxonomy of the 27001 and 27002 standards .....                                                                           | 96  |
| B.2                                                                                            | Management commitment to implementing ISO/IEC 27002 .....                                                                 | 96  |
| B.3                                                                                            | Establishing, operating, maintaining and improving the ISMS .....                                                         | 97  |
| B.4                                                                                            | Planning: establishing the ISMS .....                                                                                     | 97  |
| B.4.1                                                                                          | Selecting and defining a compliance scope .....                                                                           | 97  |
| B.4.2                                                                                          | Gap analysis .....                                                                                                        | 99  |
| B.4.3                                                                                          | Establishing or enhancing a health information security forum .....                                                       | 99  |
| B.4.4                                                                                          | Assessing risks to health information .....                                                                               | 99  |
| B.4.5                                                                                          | Risk management .....                                                                                                     | 101 |
| B.4.6                                                                                          | Security improvement planning .....                                                                                       | 102 |
| B.4.7                                                                                          | Statement of applicability .....                                                                                          | 102 |
| B.4.8                                                                                          | ISMS document set .....                                                                                                   | 102 |
| B.4.9                                                                                          | Potential for facilitation by the use of tools .....                                                                      | 103 |
| B.4.10                                                                                         | Summary .....                                                                                                             | 104 |
| B.5                                                                                            | Doing: implementing and operating the ISMS .....                                                                          | 104 |
| B.6                                                                                            | Checking: monitoring and reviewing the ISMS .....                                                                         | 106 |
| B.6.1                                                                                          | Need for on-going assurance .....                                                                                         | 106 |
| B.6.2                                                                                          | Compliance assessment .....                                                                                               | 106 |
| B.6.3                                                                                          | Summary .....                                                                                                             | 107 |
| B.7                                                                                            | Acting: maintaining and improving the ISMS .....                                                                          | 107 |
| Annex C Checklist for 27799 (informative) .....                                                |                                                                                                                           | 109 |
| C.1                                                                                            | Instructions for completing the checklist .....                                                                           | 109 |
| Bibliography .....                                                                             |                                                                                                                           | 112 |
| Related standards in health information security .....                                         |                                                                                                                           | 112 |
| Other information security standards .....                                                     |                                                                                                                           | 113 |
| Other standards .....                                                                          |                                                                                                                           | 114 |