

# ISO 27799:2016-07 (E)

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

| <b>Contents</b>    |  | <b>Page</b> |
|--------------------|--|-------------|
| Foreword .....     |  | vii         |
| Introduction ..... |  | viii        |
| 1                  | Scope .....  | 1           |
| 2                  | Normative references .....                                   | 2           |
| 3                  | Terms and definitions .....                                  | 2           |
| 4                  | Structure of this International Standard .....               | 3           |
| 5                  | Information security policies .....                          | 4           |
| 5.1                | Management direction for information security .....          | 4           |
| 5.1.1              | Policies for information security .....                      | 4           |
| 5.1.2              | Review of the policies for information security .....        | 5           |
| 6                  | Organization of information security .....                   | 6           |
| 6.1                | Internal organization .....                                  | 6           |
| 6.1.1              | Information security roles and responsibilities .....        | 6           |
| 6.1.2              | Segregation of duties .....                                  | 7           |
| 6.1.3              | Contact with authorities .....                               | 7           |
| 6.1.4              | Contact with special interest groups .....                   | 7           |
| 6.1.5              | Information security in project management .....             | 8           |
| 6.2                | Mobile devices and teleworking .....                         | 8           |
| 6.2.1              | Mobile device policy .....                                   | 8           |
| 6.2.2              | Teleworking .....  | 9           |
| 7                  | Human resource security .....                                | 9           |
| 7.1                | Prior to employment .....                                    | 9           |
| 7.1.1              | Screening .....  | 9           |
| 7.1.2              | Terms and conditions of employment .....                     | 10          |
| 7.2                | During employment .....                                      | 11          |
| 7.2.1              | Management responsibilities .....                            | 11          |
| 7.2.2              | Information security awareness, education and training ..... | 11          |
| 7.2.3              | Disciplinary process .....                                   | 11          |
| 7.3                | Termination and change of employment .....                   | 12          |
| 7.3.1              | Termination or change of employment responsibilities .....   | 12          |
| 8                  | Asset management .....                                       | 12          |
| 8.1                | Responsibility for assets .....                              | 12          |
| 8.1.1              | Inventory of assets .....                                    | 12          |
| 8.1.2              | Ownership of assets .....                                    | 13          |
| 8.1.3              | Acceptable use of assets .....                               | 13          |
| 8.1.4              | Return of assets .....                                       | 13          |
| 8.2                | Information classification .....                             | 14          |
| 8.2.1              | Classification of information .....                          | 14          |
| 8.2.2              | Labelling of information .....                               | 15          |
| 8.2.3              | Handling of assets .....                                     | 15          |
| 8.3                | Media handling .....   | 16          |
| 8.3.1              | Management of removable media .....                          | 16          |
| 8.3.2              | Disposal of media .....                                      | 16          |

|        |   |    |
|--------|---|----|
| 8.3.3  | Physical media transfer .....   | 17 |
| 9      | Access control .....  | 17 |
| 9.1    | Business requirements of access control .....                         | 17 |
| 9.1.1  | Access control policy .....   | 17 |
| 9.1.2  | Access to networks and network services .....                         | 18 |
| 9.2    | User access management .....  | 18 |
| 9.2.1  | User registration and de-registration .....                           | 18 |
| 9.2.2  | User access provisioning .....  | 19 |
| 9.2.3  | Management of privileged access rights .....                          | 19 |
| 9.2.4  | Management of secret authentication information of users .....        | 20 |
| 9.2.5  | Review of user access rights .....                                    | 20 |
| 9.2.6  | Removal or adjustment of access rights .....                          | 21 |
| 9.3    | User responsibilities .....   | 21 |
| 9.3.1  | Use of secret authentication information .....                        | 21 |
| 9.4    | System and application access control .....                           | 22 |
| 9.4.1  | Information access restriction .....                                  | 22 |
| 9.4.2  | Secure log-on procedures .....  | 22 |
| 9.4.3  | Password management system .....                                      | 22 |
| 9.4.4  | Use of privileged utility programs .....                              | 23 |
| 9.4.5  | Access control to program source code .....                           | 23 |
| 10     | Cryptography .....  | 23 |
| 10.1   | Cryptographic controls .....  | 23 |
| 10.1.1 | Policy on the use of cryptographic controls .....                     | 23 |
| 10.1.2 | Key management .....  | 24 |
| 11     | Physical and environmental security .....                             | 24 |
| 11.1   | Secure areas .....  | 24 |
| 11.1.1 | Physical security perimeter .....                                     | 24 |
| 11.1.2 | Physical entry controls .....   | 25 |
| 11.1.3 | Securing offices, rooms and facilities .....                          | 25 |
| 11.1.4 | Protecting against external and environmental threats .....           | 25 |
| 11.1.5 | Working in secure areas .....   | 25 |
| 11.1.6 | Delivery and loading areas .....                                      | 25 |
| 11.2   | Equipment .....   | 26 |
| 11.2.1 | Equipment siting and protection .....                                 | 26 |
| 11.2.2 | Supporting utilities .....  | 26 |
| 11.2.3 | Cabling security .....  | 27 |
| 11.2.4 | Equipment maintenance .....   | 27 |
| 11.2.5 | Removal of assets .....   | 27 |
| 11.2.6 | Security of equipment and assets off-premises .....                   | 27 |
| 11.2.7 | Secure disposal or reuse of equipment .....                           | 28 |
| 11.2.8 | Unattended user equipment .....                                       | 28 |
| 11.2.9 | Clear desk and clear screen policy .....                              | 28 |
| 12     | Operations security .....   | 29 |
| 12.1   | Operational procedures and responsibilities .....                     | 29 |
| 12.1.1 | Documented operating procedures .....                                 | 29 |
| 12.1.2 | Change management .....   | 29 |
| 12.1.3 | Capacity management .....   | 30 |
| 12.1.4 | Separation of development, testing and operational environments ..... | 30 |
| 12.2   | Protection from malware .....   | 30 |
| 12.2.1 | Controls against malware .....  | 30 |
| 12.3   | Backup .....  | 31 |
| 12.3.1 | Information backup .....  | 31 |
| 12.4   | Logging and monitoring .....  | 31 |
| 12.4.1 | Event logging .....   | 31 |
| 12.4.2 | Protection of log information .....                                   | 32 |
| 12.4.3 | Administrator and operator logs .....                                 | 33 |
| 12.4.4 | Clock synchronisation .....   | 34 |

|        |   |    |
|--------|---|----|
| 12.5   | Control of operational software .....                                   | 34 |
| 12.5.1 | Installation of software on operational systems .....                   | 34 |
| 12.6   | Technical vulnerability management .....                                | 34 |
| 12.6.1 | Management of technical vulnerabilities .....                           | 34 |
| 12.6.2 | Restrictions on software installation .....                             | 35 |
| 12.7   | Information systems audit considerations .....                          | 35 |
| 12.7.1 | Information systems audit controls .....                                | 35 |
| 13     | Communications security .....   | 35 |
| 13.1   | Network security management .....                                       | 35 |
| 13.1.1 | Network controls .....  | 35 |
| 13.1.2 | Security of network services .....                                      | 36 |
| 13.1.3 | Segregation in networks .....   | 36 |
| 13.2   | Information transfer .....  | 36 |
| 13.2.1 | Information transfer policies and procedures .....                      | 36 |
| 13.2.2 | Agreements on information transfer .....                                | 37 |
| 13.2.3 | Electronic messaging .....  | 37 |
| 13.2.4 | Confidentiality or non-disclosure agreements .....                      | 38 |
| 14     | System acquisition, development and maintenance .....                   | 38 |
| 14.1   | Security requirements of information systems .....                      | 38 |
| 14.1.1 | Information security requirements analysis and specification .....      | 38 |
| 14.1.2 | Securing application services on public networks .....                  | 40 |
| 14.1.3 | Protecting application services transactions .....                      | 40 |
| 14.2   | Security in development and support processes .....                     | 40 |
| 14.2.1 | Secure development policy .....   | 40 |
| 14.2.2 | System change control procedures .....                                  | 41 |
| 14.2.3 | Technical review of applications after operating platform changes ..... | 41 |
| 14.2.4 | Restrictions on changes to software packages .....                      | 41 |
| 14.2.5 | Secure system engineering principles .....                              | 42 |
| 14.2.6 | Secure development environment .....                                    | 42 |
| 14.2.7 | Outsourced development .....  | 42 |
| 14.2.8 | System security testing .....   | 42 |
| 14.2.9 | System acceptance testing .....   | 43 |
| 14.3   | Test data .....   | 43 |
| 14.3.1 | Protection of test data .....   | 43 |
| 15     | Supplier relationships .....  | 43 |
| 15.1   | Information security in supplier relationships .....                    | 43 |
| 15.1.1 | Information security policy for supplier relationships .....            | 43 |
| 15.1.2 | Addressing security within supplier agreements .....                    | 44 |
| 15.1.3 | Information and communication technology supply chain .....             | 44 |
| 15.2   | Supplier service delivery management .....                              | 44 |
| 15.2.1 | Monitoring and review of supplier services .....                        | 45 |
| 15.2.2 | Managing changes to supplier services .....                             | 45 |
| 16     | Information security incident management .....                          | 45 |
| 16.1   | Management of information security incidents and improvements .....     | 45 |
| 16.1.1 | Responsibilities and procedures .....                                   | 45 |
| 16.1.2 | Reporting information security events .....                             | 45 |
| 16.1.3 | Reporting information security weaknesses .....                         | 46 |
| 16.1.4 | Assessment of and decision on information security events .....         | 47 |
| 16.1.5 | Response to information security incidents .....                        | 47 |
| 16.1.6 | Learning from information security incidents .....                      | 47 |
| 16.1.7 | Collection of evidence .....  | 47 |
| 17     | Information security aspects of business continuity management .....    | 48 |
| 17.1   | Information security continuity .....                                   | 48 |
| 17.1.1 | Planning information security continuity .....                          | 48 |
| 17.1.2 | Implementing information security continuity .....                      | 49 |
| 17.1.3 | Verify, review and evaluate information security continuity .....       | 49 |
| 17.2   | Redundancies .....  | 49 |

|  |   |    |
|--|---|----|
| 17.2.1   | Availability of information processing facilities .....                     | 49 |
| 18   | Compliance .....  | 50 |
| 18.1   | Compliance with legal and contractual requirements .....                    | 50 |
| 18.1.1   | Identification of applicable legislation and contractual requirements ..... | 50 |
| 18.1.2   | Intellectual property rights .....  | 50 |
| 18.1.3   | Protection of records .....   | 50 |
| 18.1.4   | Privacy and protection of personally identifiable information .....         | 51 |
| 18.1.5   | Regulation of cryptographic controls .....                                  | 52 |
| 18.2   | Information security reviews .....  | 52 |
| 18.2.1   | Independent review of information security .....                            | 52 |
| 18.2.2   | Compliance with security policies and standards .....                       | 52 |
| 18.2.3   | Technical compliance review .....   | 53 |
| Annex A (informative) Threats to health information security .....                             |   | 54 |
| Annex B (informative) Practical action plan for implementing ISO/IEC 27002 in healthcare ..... |   | 59 |
| Bibliography .....   |   | 98 |