ISO/FDIS 27799~~:2025(en)~~

ISO/TC 215~~/ WG 4~~

Secretariat: ANSI

Date: 2025-~~07-15~~09-03

Health informatics — Information security controls in health based on ISO/IEC 27002

FDIS stage

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/FDIS 27799
https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-fdis-27799

Edited DIS - MUST BE USED FOR FINAL DRAFT

© ISO 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11
~~Email~~E-mail: copyright@iso.org
Website: www.iso.org

Published in Switzerland

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/FDIS 27799
https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-fdis-27799

Contents

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms, definitions and abbreviated terms 1
3.1 Terms and definitions 2
3.2 Abbreviated terms 3

4 General 3
4.1 Structure of this document 3
4.2 Safety 4
4.3 Selecting and applying controls 4

5 Organizational controls 5
5.1 Policies for information security 5
5.2 Information security roles and responsibilities 7
5.3 Segregation of duties 8
5.4 Management responsibilities 8
5.5 Contact with authorities 8
5.6 Contact with special interest groups 8
5.7 Threat intelligence 8
5.8 Information security in project management 9
5.9 Inventory of information and other associated assets 9
5.10 Acceptable use of information and other associated assets 10
5.11 Return of assets 10
5.12 Classification of information 10
5.13 Labelling of information 11
5.14 Information transfer 11
5.15 Access control 12
5.16 Identity management 13
5.17 Authentication information 14
5.18 Access rights 14
5.19 Information security in supplier relationships 14
5.20 Addressing information security within supplier agreements 15
5.21 Managing information security in the ICT supply chain 15
5.22 Monitoring, review and change management of supplier services 15
5.23 Information security for use of cloud services 15
5.24 Information security incident management planning and preparation 16
5.25 Assessment and decision on information security events 16
5.26 Response to information security incidents 16
5.27 Learning from information security incidents 16
5.28 Collection of evidence 16
5.29 Information security during disruption 16
5.30 ICT readiness for business continuity 17
5.31 Legal, statutory, regulatory and contractual requirements 17
5.32 Intellectual property rights 17
5.33 Protection of records 17
5.34 Privacy and protection of PII 18
5.35 Independent review of information security 19
5.36 Conformance with policies, rules and standards for information security 19
5.37 Documented operating procedures 20

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/FDIS 27799
https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-fdis-27799

© ISO 2025 – All rights reserved

5.38 HLT – Information security requirements analysis and specification 20
5.39 HLT – Uniquely identifying subjects of care 21
5.40 HLT – Validation of displayed/printed data 22
5.41 HLT – Publicly available health information 23
5.42 HLT – Emergency communication 23
5.43 HLT – External incident reporting 24

6 People controls 25
6.1 Screening 25
6.2 Terms and conditions of employment 25
6.3 Information security awareness, education and training 26
6.4 Disciplinary process 26
6.5 Responsibilities after termination or change of employment 26
6.6 Confidentiality or non-disclosure agreements 27
6.7 Remote working 27
6.8 Information security event reporting 27
6.9 HLT – Management training 28

7 Physical controls 28
7.1 Physical security perimeters 28
7.2 Physical entry 29
7.3 Securing offices, rooms and facilities 29
7.4 Physical security monitoring 29
7.5 Protecting against physical and environmental threats 29
7.6 Working in secure areas 29
7.7 Clear desk and clear screen 30
7.8 Equipment siting and protection 30
7.9 Security of assets off-premises 30
7.10 Storage media 30
7.11 Supporting utilities 31
7.12 Cabling security 31
7.13 Equipment maintenance 32
7.14 Secure disposal or re-use of equipment 32

8 Technological controls 33
8.1 User endpoint devices 33
8.2 Privileged access rights 33
8.3 Information access restriction 33
8.4 Access to source code 33
8.5 Secure authentication 33
8.6 Capacity management 34
8.7 Protection against malware 34
8.8 Management of technical vulnerabilities 34
8.9 Configuration management 34
8.10 Information deletion 35
8.11 Data masking 35
8.12 Data leakage prevention 36
8.13 Information backup 36
8.14 Redundancy of information processing facilities 36
8.15 Logging 36
8.16 Monitoring activities 36
8.17 Clock synchronization 36
8.18 Use of privileged utility programs 36
8.19 Installation of software on operational systems 37
8.20 Networks security 37
8.21 Security of network services 37

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/FDIS 27799
https://standards.iteh.ai/catalog/standards/iso/e4938c7-6fa0-484e-8fa1-8913515796ed/iso-fdis-27799

8.22 Segregation of networks 37
8.23 Web filtering 37
8.24 Use of cryptography 38
8.25 Secure development life cycle 38
8.26 Application security requirements 38
8.27 Secure system architecture and engineering principles 38
8.28 Secure coding 38
8.29 Security testing in development and acceptance 39
8.30 Outsourced development 39
8.31 Separation of development, test and production environments 39
8.32 Change management 39
8.33 Test information 39
8.34 Protection of information systems during audit testing 40
8.35 HLT – Zero trust principles 40
Annex A (informative) Information security controls for health reference 41
Annex B (informative) Correspondence of this document with ISO 27799:2016 43
Annex C (informative) Information security in health organizations 44
Annex D (informative) Example security and privacy requirements for health information systems and their mapping to the ISO 27799 controls and IEC/TS 81001-2-2 security capabilities 56
Bibliography 82

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/FDIS 27799
https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-fdis-27799

© ISO 2025 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO ~~document~~documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ~~ISO's~~ISO’s adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

https://standards.iteh.ai/catalog/standards/iso/ce4938c7-6fa0-484e-8fa1-8913515796ed/iso-fdis-27799

This third edition cancels and replaces ~~the second edition (~~ISO 27799:2016~~)~~, and ISO/TS 14441:2013, which ~~has~~have been technically revised.

The main changes are as follows:

- ~~—~~alignment with the new structure of ISO/IEC 27002:2022 and other changes to that standard from the previous version;
- ~~—~~revision and addition of controls specific to health;
- ~~—~~removal of material that was originally only in the second edition of this document but was subsequently included in ISO/IEC 27002:2022;
- ~~—~~addition of informative Annexes providing ~~i)~~ supplementary guidance on cybersecurity in health organizations and ~~ii)~~ example security and privacy requirements for health information systems.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 ~~0.1~~ General

This document contains a set of information security controls for health organizations. It considers all the controls in ISO/IEC 27002:2022 and, in some cases, supplements the controls or provides guidance on their application in health. There are also some additional controls specific to health which are not derived from any in ISO/IEC 27002:2022.

0.2 ~~0.2~~ Context and background

Factors that affect information security in healthcare include the following:

a) ~~a)~~ Use of equipment that relies on digital technologies for its operation and is deployed exclusively or predominantly in the healthcare domain. Medical devices incorporating health software are the prime example.

b) ~~b)~~ The need to balance clinical safety and effectiveness with information security.

c) ~~c)~~ Maintaining the privacy of subjects of care while ensuring access to relevant personal health information for diagnosis and treatment.

d) ~~d)~~ The distributed nature of personal health information both within and between organizations (possibly in different jurisdictions) resulting in the need for high levels of interoperability between diverse systems, applications and devices.

e) ~~e)~~ Users of many different kinds including doctors, nurses, other clinicians, trainees, students, healthcare assistants, technicians, administrative staff and volunteers as well as subjects of care and their proxies.

f) ~~f)~~ The multiple interdependencies and information flows between and within organizations responsible for one or more of: healthcare, clinical research, teaching, education and training.

g) ~~g)~~ The need for some healthcare services to be available on a continuous basis (24 hours a day every day) under normal circumstances. In addition, natural disasters and other unusual events that can lead to surges in demand for healthcare services.

h) ~~h)~~ Organizations providing health services as well as manufacturers or suppliers of systems, devices and equipment are all subject to a wide range of legal, statutory, regulatory and contractual requirements which can vary between jurisdictions.

i) ~~i)~~ Overlapping or incomplete requirements for accountability and professional responsibility between different professions (such as ICT and medical devices staff) for ensuring security and safety of systems, devices and equipment.

Given this overall context, healthcare has a number of sector-specific, if not unique, information security requirements. However, the controls in ISO/IEC 27002:2022 are intentionally generic, hence the need for this document.

0.3 ~~0.3~~ Audience and uses

This document is targeted at organizations that:

— ~~—~~ provide healthcare services or are custodians of personal health information for other reasons;

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/FDIS 27799

© ISO 2025 – All rights reserved

Edited DIS - MUST BE USED FOR FINAL DRAFT