FINAL DRAFT International Standard

ISO/FDIS 27799

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

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2025-09-18

Voting terminates on:
2025-11-13

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/FDIS 27799:2025(en)

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

Published in Switzerland

Contents

Page

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 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.

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 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).

This third edition cancels and replaces ISO 27799:2016 and ISO/TS 14441:2013, which 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 supplementary guidance on cybersecurity in health organizations and 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 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 Context and background

Factors that affect information security in healthcare include the following:

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

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

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

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) 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) 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 Audience and uses

This document is targeted at organizations that:

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

— supply software, systems, devices, equipment or services that are used to process personal health information;

— are responsible for healthcare regulation, accreditation, inspection, assurance or similar.

Individuals for whom this document is particularly relevant include:

— ICT and medical devices or equipment professionals working in the types of organizations listed above;