



Technical Specification

ISO/TS 6268-3

Health informatics — Cybersecurity framework for telehealth environments —

Part 3: Cybersecurity controls of telehealth

*Informatique de santé — Cadre en matière de cybersécurité pour
les environnements de télésanté —*

Partie 3: Contrôles de cybersécurité en télésanté

**First edition
2026-10**

Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

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: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	2
4 Cybersecurity controls for telehealth services	2
4.1 General	2
4.2 Organizational controls	3
4.2.1 Cybersecurity alignment and gap management	3
4.2.2 Contact with authorities and support systems	3
4.2.3 Asset identification and management	4
4.2.4 Cybersecurity level alignment	5
4.2.5 Secure exchange of telehealth information	5
4.2.6 Shared identity management	6
4.2.7 Telehealth incident management planning and preparation	7
4.2.8 Differences in legal, statutory, regulatory and contractual requirements	7
4.2.9 Protection of records	8
4.2.10 Documented operating procedures	8
4.2.11 Unique identification and authentication	9
4.3 People controls	10
4.3.1 Identification of participating persons	10
4.3.2 Awareness, education and training for persons participating in telehealth services	10
4.3.3 Social engineering	11
4.4 Physical controls	12
4.4.1 Physical security perimeters	12
4.4.2 Telehealth services in private non-clinical spaces	13
4.4.3 Protecting real-time services against physical and environmental threats	13
4.4.4 Telehealth equipment management	14
4.5 Technological controls	15
4.5.1 Personally-managed telehealth devices	15
4.5.2 Authentication of authorized patient assistants	15
4.5.3 Home monitoring devices in telehealth environments	16
4.5.4 Configuration for critical telehealth services	17
Annex A (informative) Alignment of telehealth cybersecurity controls with ISO 27799:2025	18
Bibliography	20

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*.

A list of all parts in the ISO 6268 series can be found on the ISO website.

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

Telehealth once provided a limited range of services to subjects of care in specific environments. However, the scope of telehealth services is rapidly expanding through advanced information and communication technologies (ICT) such as mobile-based, cloud-based and other network-based applications. Additionally, emerging global pandemics have acutely increased the need to diagnose, prevent, monitor, treat or mitigate diseases and injuries without face-to-face, in-person contact between subjects of care and care providers, making telehealth a more commonly-accepted medical practice.

These services are described as telehealth services because they use ICT services to support healthcare activities. Telehealth services include, but are not limited to, telemedicine, telecare, mHealth (healthcare supported by mobile devices), remote use of medical applications, tele-monitoring, tele-diagnostics and virtual care. Examples of health services include, but are not limited to, tele-pathology, tele-dermatology, tele-cardiology, tele-rehabilitation, tele-oncology and tele-orthopaedics. Healthcare activities that directly or indirectly support care recipients include, but are not limited to, teleconsultation, telephone advice, health alarm systems and health status monitoring at home. Telehealth services can support immediate healthcare activities using synchronous communications services such as a telephone or video conversation, or delayed health care activities using asynchronous communications services such as messaging services.

Furthermore, depending on the perspective from which telehealth is viewed, the subcategories of telehealth can vary. Physicians are familiar with the division of telehealth into medical departments. Medical IT experts will look at telehealth according to system topology and network. When it comes to telehealth in cybersecurity, telehealth actors, interactions between each actor, data flow, service environment and technology should be considered. Therefore, establishing concept and models of telehealth cybersecurity would be the first step to build a framework for cybersecurity in telehealth environment.

Telehealth cybersecurity concepts and models serve as a baseline for the analysis of cybersecurity threats and to determine countermeasures. Telehealth cybersecurity countermeasures need to consider not only technical aspects, but also management and physical approaches to operating telehealth services. This is because telehealth cybersecurity involves interactions between multiple actors situated in environments with different levels of cybersecurity. The cybersecurity policies and processes act as variables that influence the overall cybersecurity posture of telehealth.

People-related and physical security controls require particular consideration in telehealth cybersecurity because telehealth service participants can operate in physically separate and uncontrolled environments. Unlike conventional healthcare environments, telehealth service participants can have limited ability to directly observe, verify, intervene in, or physically respond to situations occurring in remote environments.

Ensuring that telehealth services achieve levels of safety, security and reliability comparable to conventional healthcare services can require additional operational, organizational, physical and cybersecurity controls. Telehealth service participants should consider risks arising from limited visibility and limited physical control over remote environments, including situations occurring outside the camera view or beyond the direct awareness of telehealth service participants. Physical intrusion, theft, vandalism, unauthorized observation, device disconnection, impersonation, deception or tampering can present significant risks in telehealth environments and should be addressed through appropriate countermeasures.

The cybersecurity framework for telehealth environment is structured as follows:

- Part 1: Overview and concepts;
- Part 2: Cybersecurity reference models of telehealth;
- Part 3: Cybersecurity controls of telehealth.

This document provides telehealth cybersecurity controls of the overall security framework for systems and services applied to telehealth.

Sample Document

get full document from standards.iteh.ai

Health informatics — Cybersecurity framework for telehealth environments —

Part 3: Cybersecurity controls of telehealth

1 Scope

This document provides telehealth cybersecurity controls of the overall security framework for systems and services applied to telehealth, specifically addressing cybersecurity controls uniquely applicable to telehealth, while general elements relevant to health delivery organizations (HDOs) can be referenced from ISO 27799.

It also includes [Annex A](#), which, for informative purposes, provides a mapping of the controls in [4.2](#) to [4.5](#) of this document to the security controls in ISO 27799:2025¹⁾.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TS 6268-1, *Health informatics — Cybersecurity framework for telehealth environments — Part 1: Overview and concepts*

ISO/TS 6268-2, *Health informatics — Cybersecurity framework for telehealth environments — Part 2: Cybersecurity reference model of telehealth*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 6268-1, ISO/TS 6268-2 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1.1

cybersecurity gap

disparity in cybersecurity maturity levels among participants in telehealth services

Note 1 to entry: Cybersecurity gaps enable attackers to exploit vulnerabilities and compromise organizations with robust security policies and processes, for example, attackers targeting a hospital with an advanced security management framework can first breach a less secure clinic connected to the hospital's network through telehealth services. Therefore, compensating for the cybersecurity gap among telehealth service participants is critical to ensuring the safety and security of telehealth services.