Technical Specification

ISO/TS 6268-1

First edition
2025-02

Health informatics — Cybersecurity framework for telehealth environments —

Part 1: Overview and concepts

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

Partie 1: Vue d'ensemble et concepts

Reference number
ISO/TS 6268-1:2025(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 document 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/TS 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 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 can be described as telehealth services because information and communication technology services are being used to support healthcare activities. Telehealth services can 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.[4]

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, it is necessary to consider telehealth actors, interactions between each actor, data flow, service environment, and technology. 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 cybersecurity threats and 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 addresses interactions between multiple actors physically located in environments with different levels of cybersecurity. The cybersecurity policies and processes to be inherited by each actor can also act as variable in the cybersecurity posture.

Another consideration of telehealth cybersecurity framework is the interaction of health information systems with remote medical devices. It would be desirable to present a methodology to assess and respond to the overall risks by integrating the risks of medical devices from a safety perspective and the risks of telehealth services from a cybersecurity perspective.

The cybersecurity framework for telehealth environment is structured as follows:

— Part 1: Overview and concepts;

— Part 2: Cybersecurity reference model of telehealth;

— Part 3: Cybersecurity requirements for telehealth.

This document contains general definitions of concepts applied to the entire document with brief descriptions of the overall document structure. It contains explanations of the main components of each part, and through this, it provides the overall organization and quick understanding of the document.