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 ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Overview of cybersecurity framework for telehealth **5**
4.1 Concepts of telehealth cybersecurity 5
4.2 Actors of telehealth services 6
4.3 Activities of telehealth services 7
4.4 Environment of telehealth services 8
4.5 Parameters of telehealth cybersecurity 8
Bibliography **10**

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.

Health informatics — Cybersecurity framework for telehealth environments —

Part 1: Overview and concepts

1 Scope

This document provides a concept and overview of the overall cybersecurity framework for systems and services applied to telehealth.

This document contains a general description of:

— concept and introduction of telehealth cybersecurity;

— actors of telehealth services;

— activities of telehealth services;

— environments of telehealth services;

— variables of telehealth security.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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 https://www.electropedia.org/

3.1
care
interactions between a *care recipient* (3.3) and a *healthcare actor* (3.5) to benefit the health state of the care recipient

Note 1 to entry: The term care is frequently used in combination with other words, such as *healthcare* (3.4) or care recipient.

Note 2 to entry: Care also includes interactions between *caregivers* (3.2) who are not healthcare professionals, such as informal caregivers.

[SOURCE: ISO 13131:2021, 3.3.3]

3.2
caregiver
carer
individual who is entrusted with the direct or indirect provision of defined *healthcare services* (3.7) to an individual *subject of care* (3.18) or to populations

[SOURCE: ISO/TS 21089:2018, 3.30]

3.3
care recipient
healthcare actor (3.5) with a person role, who seeks to receive, is receiving or has received *healthcare* (3.4)

[SOURCE: ISO 13131:2021, 3.2.2, modified — Other preferred and admitted terms were removed.]

3.4
healthcare
care activities, services, or supplies related to the health of an individual

[SOURCE: ISO 13940:2015, 3.1.1, modified — "management" removed from definition and Note to entry removed.]

3.5
healthcare actor
organization (3.9) or person participating in *healthcare* (3.4)

Note 1 to entry: An individual person may be regarded as a legal entity in some situations depending on the service being delivered and the relevant national legislation.

[SOURCE: ISO 13940:2015, 5.2]

3.6
healthcare delivery organization
HDO
facility or enterprise such as a clinic or hospital that provides *healthcare services* (3.7)

[SOURCE: ISO 81001-1:2021, 3.1.4]

3.7
healthcare service
service (3.17) that is the result of a *healthcare* (3.4) *process* (3.13)

[SOURCE: ISO 13940:2015, 8.2.6]

3.8
medical device
instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of:

— diagnosis, prevention, monitoring, treatment or alleviation of disease;

— diagnosis, monitoring, treatment, alleviation of or compensation for an injury;

— investigation, replacement, modification, or support of the anatomy or of a physiological process;

— supporting or sustaining life;

— control of conception;

— disinfection of medical devices;

— providing information by means of *in vitro* examination of specimens derived from the human body;

and that does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means

[SOURCE: ISO 13485:2016, 3.11, modified — Note to entry was removed.]

3.9
organization
persons or groups of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: An organization can in some cases be a single health professional.

[SOURCE: ISO 9000:2015, 3.2.1, modified — original Notes to entry were removed and a new note was added.]

3.10
personal health device
PHD
device used in personal health applications

[SOURCE: IEEE 11073-10408:2008, 3.1.11]

3.11
platform
combination of an operating system and hardware that makes up the operating environment in which a program runs

[SOURCE: ISO/IEC/IEEE 26513:2017, 3.30]

3.12
procedure
specified way to carry out an activity or *process* (3.13)

[SOURCE: ISO 9000:2015, 3.4.5, modified — Note to entry was removed.]

3.13
process
set of interrelated or interacting activities that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes to entry were removed.]

3.14
risk
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: The probability of occurrence includes the exposure to a hazardous situation and the possibility to avoid or limit the harm.

[SOURCE: ISO/IEC Guide 51:2014, 3.9, modified — Note 1 to entry was modified.]

3.15
safety
freedom from unacceptable *risk* (3.14)

EXAMPLE Safety measures that maintain the health of *care recipients* (3.3).

[SOURCE: ISO/IEC Guide 63:2019, 3.10]

3.16
security
cybersecurity
state where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification or destruction to a degree that the *risks* (3.14) related to violation of confidentiality, integrity and availability are maintained at an acceptable level throughout the life cycle

[SOURCE: ISO 81001-1:2021, 3.2.13]

3.17
service
output of an organization with at least one activity necessarily performed between the *organization* (3.9) and the customer

[SOURCE: ISO 9000:2015, 3.7.7, modified — Notes to entry were removed.]

3.18
subject of care
person who uses, or is a potential user of, a health care service

Note 1 to entry: Subjects of care may also be referred to as patients or health care consumers.

[SOURCE: ISO 22220:2011, 3.2]

3.19
telehealth platform provider
organization responsible for the telehealth *platform* (3.11)

Note 1 to entry: The platform provider is typically the vendor of the relevant operating system, virtual environment, or application platform.

[SOURCE: ISO/IEC 19770-2:2015, 3.1.2, modified — "telehealth" was added before "platform" in the term, the definition and the note to entry.]

3.20
telehealth service
healthcare (3.4) activity supported at a distance by information and communication technology *service(s)* (3.17)

Note 1 to entry: It is possible that the *subject of care* (3.18) is not directly involved in a telehealth service, e.g. in the case of tele-dermatology where one physician consults another physician who is at a distant location.

Note 2 to entry: Healthcare activities can include healthcare provider activities such as diagnosis, treatment, review or advice, and self-care activities as prescribed or recommended by a health professional, preventive (educational) advice and management of healthcare processes.

Note 3 to entry: Healthcare activities can include both synchronous (real-time) and asynchronous (delayed) interactions between actors. For example, a radiology examination can be transmitted and subsequently reported by a radiologist over a communications network. A discussion on the diagnostic findings can occur in real time over a telephone or video conferencing connection between a care recipient and health professionals.

[SOURCE: ISO 13131:2021, 3.5.2]

3.21
telehealth service provider
entity that delivers *telehealth service* (3.20)

3.22
telehealth service recipient
individual who receives *telehealth service* (3.20)

4 Overview of cybersecurity framework for telehealth

4.1 Concepts of telehealth cybersecurity

The telehealth cybersecurity framework addresses cybersecurity issues in a variety of activities that include care recipients, medical staff, medical facilities and equipment and related environments, for secure delivery of non-face-to-face services with similar quality to general ones.

One of the distinctive features of cybersecurity in telehealth is that there are gaps in the level of cybersecurity between each actor. A typical healthcare service is an interaction conducted by service providers, recipients, and others within a single healthcare institution managed by consistent business goals, visions and policies. On the other hand, telehealth actors interact from different physical spaces for the same goal. Each actor performs telehealth in different environments (including IT and cybersecurity environment), using facilities, equipment, and systems that are allowed for each.

The security level of each actor depends on the security level of the environment in which the actor belongs. The security level of the care recipient tele-monitored at home is different from that of the care recipient tele-monitored in a nursing home.

For example, a physician in a well-organized hospital can provide telehealth services to the care recipients connecting from various places: homes, ambulances, or nursing homes. In this case, the telehealth service provider can maintain a security level relatively higher than that of recipients. Conversely, a physician at home or in a café can advise another physician approaching from a remote hospital, in which case the security level of the telehealth service provider is lower than that of the recipient. Telehealth application providers cannot maintain as stringent security levels as telehealth service providers.

A security gap, which is the difference in cybersecurity level between participants in an activity, can give an opportunity for malware in vulnerable environment to migrate to an actor in a higher secured area. Telehealth, a service where multiple actors are interconnected, can be the most convenient shortcut for an attacker to jump from a vulnerable clinic to a robust hospital system.

“Security gap” typically refers to vulnerabilities or weaknesses in an organization’s cybersecurity framework that can be exploited by cyber threats. In this document, “security gap” can refer to differences in security levels among the three actors involved in telehealth.

For cybersecurity in telehealth, it is important to consider countermeasures to reduce the security gaps between multiple participants in organizational, people, physical and technological aspects.

Figure 1 is a schematic diagram of the actors of the telehealth cybersecurity framework and various factors that influence cybersecurity, and the details are dealt with in 4.2.

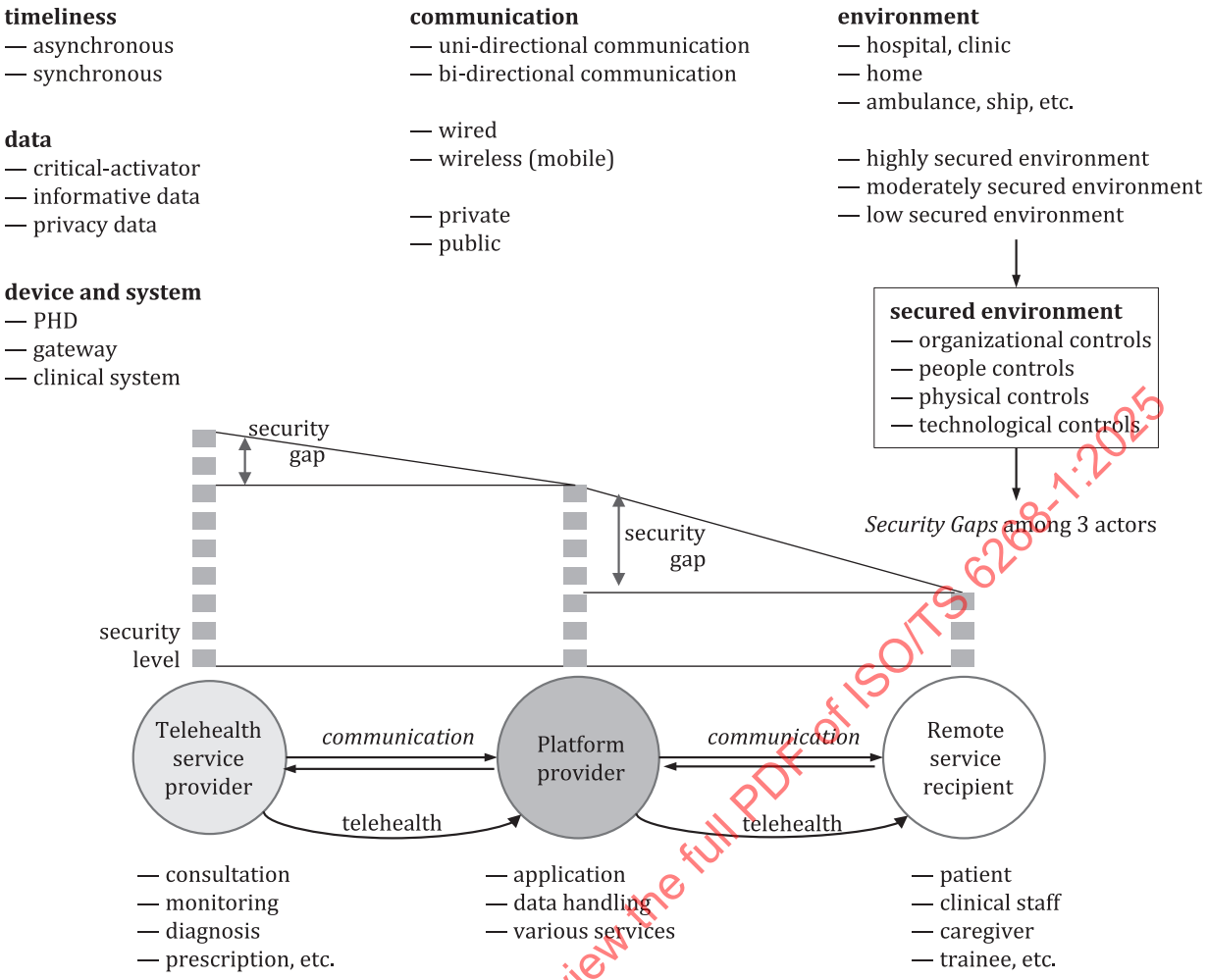

Figure 1 — Concepts of telehealth cybersecurity framework

4.2 Actors of telehealth services

Three main actors are involved in telehealth activities: telehealth service providers, telehealth platforms providers, and telehealth service recipients. To eliminate other variables from a cybersecurity perspective, each actor is assumed to be a participant who directly deals with devices or systems for the telehealth services.

— The telehealth service provider is a subject of telehealth that provides telehealth services by receiving telehealth requests from remote locations. Telehealth service providers can be clinical staff, such as doctors and nurses, or entities providing non-medical information, such as counsellors. They use the clinical information system to issue a diagnosis or prescription order for a remote care recipient, collaborate with remote medical staff, or provide advice for a specific care recipient. In addition, they involve in activities such as providing real-time education to remote trainees or performing operations with remote surgery robots.

— The telehealth platform provider is an actor that mediates telehealth services between telehealth service providers and remote service recipients. It is an actor that connects telehealth participants and supports both parties to achieve their intended purpose while exchanging various data such as texts, audios, images, and videos.

— The telehealth service recipient is an actor who requests telehealth from a remote location; this includes care recipients of telehealth, a caregiver helping the elderly at nursing homes, paramedics in an ambulance in need of first aid, a physician performing surgery with the support of a remote expert, an intern who needs professional training, etc.

4.3 Activities of telehealth services

High level of healthcare activities can be represented as Figure 2 and as follows:

— Encounter: non-healthcare area which includes subscription, log-in, selecting a service, and making an appointment before starting healthcare activities, and making the next appointment, payment, and log-out after healthcare activities.

— Observation: a healthcare service provider sees the health status of a care recipient using medical resources such as EMR, questionnaire, clinical check-up, or test results.

— Intervention; a healthcare service provider makes clinical decisions or performs clinical procedures such as prescription, treatment, or surgery to improve the health status of a care recipient.

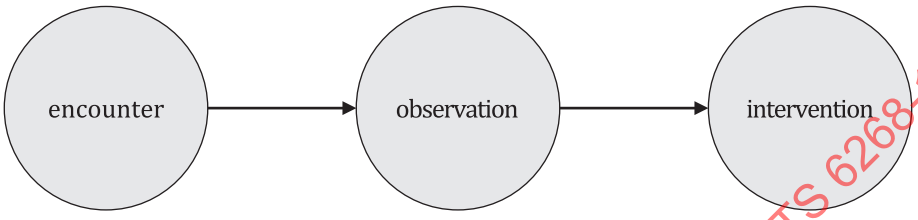

Figure 2 — High-level activities of healthcare services

In telehealth services, a physician who is a telehealth service provider interacts with various remote counterparts involved in clinical practices. The remote counterpart can be a care recipient or user directly receiving telehealth services provided by a telehealth provider, or it can be a caregiver or supporter assisting a care recipient or user who is unable to interface with the telehealth services. Otherwise, it can be a physician who is in the remote place and needs a medical opinion or co-operations to properly treat the care recipient.

For telehealth encounter, each party goes through the steps of subscribing to, scheduling, and accessing a telehealth system based on identification and authorization. Observation activities are performed based on real-time virtual examinations or data collected from the medical devices installed at the remote care recipient's site. After reviewing the observations, the intervention is made according to the decision of the physician.

In the case of the observation using a monitoring device, if the device simply sends the data collected from the care recipient to the system, it is a kind of observation. The physician reviews the data collected and makes the appropriate clinical decision, such as changing medication, dosage or energy delivered to the care recipient. In this case, observation and intervention should be performed using separated routes. If the monitoring device can send the data collected from the care recipient to the system as well as give medication or energy to the care recipient through the same device, the telehealth activity should be considered as intervention rather than observation. In this case, the telehealth activity happens by pre-set algorithm without giving a chance for clinical decision-making to the physician during the process, as shown in Figure 3.

For example, if an implantable sphygmomanometer only collects the heart rate data and alerts the physician to take emergency action at abnormal values, this telehealth activity is defined as an observation. However, if the device is pre-set to automatically control the heart rate with a built-in drug on a specific trigger, the telehealth activity is an intervention, not an observation.

NOTE Telehealth services depend on processes and sub-processes in which at least two healthcare actors are actively involved. It is also possible for one of the actors to be the supervisor of a technical application, as in the case of a remote operation, or a digital diagnostic system. A healthcare organization can provide services or supplies related to the health of an individual with or without the direct involvement of a healthcare professional (see ISO 13131:2021).

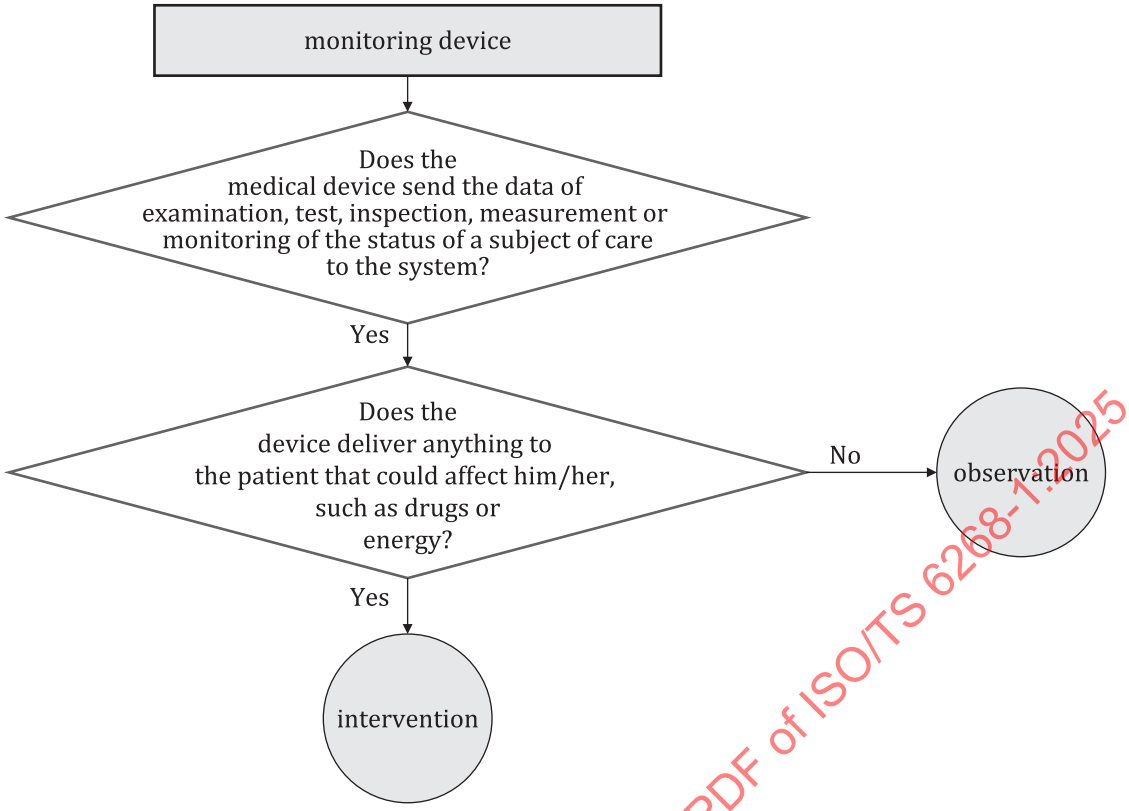

Figure 3 — Telehealth activity using the monitoring device

4.4 Environment of telehealth services

From a cybersecurity perspective, a telehealth environment is a physical or virtual space in which the three main actors conduct telehealth activities. Each actor works in an HDO (health delivery organization), home, medical helicopter, ship, prison, cloud space, etc. In the telehealth cybersecurity framework, the safety issues of medical equipment or facilities are excluded but only the security level of the environment is considered. It can be difficult to address cybersecurity challenges if security levels are determined only by the physical environment. While HDOs can also be low level of security environments, a healthcare provider such as a medical doctor in a private space can also configure significant levels of security to conduct telehealth activities. When it comes to environment of the framework, it seems to be more meaningful to consider security level of place where telehealth is conducted rather than the place itself, regardless of whether it is an HDO or a home.

The telehealth environment is divided into 3 levels:

— highly secured environment;

— moderately secured environment;

— low secured environment.

The level of security in the telehealth environment is derived from the organizational, people, physical, and technological perspectives based on ISO/IEC 27002:2022. The greater the security gap between telehealth actors, the higher the likelihood that the environment of an actor in a higher level of security will be compromised.

4.5 Parameters of telehealth cybersecurity

Parameters affect cybersecurity risk in a telehealth environment, and these can be vulnerabilities of telehealth cybersecurity.