TECHNICAL REPORT

ISO/TR 22696

First edition
2020-05

Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)

Informatique de santé — Lignes directrices pour l'identification et l'authentification des dispositifs de soins de santé personnels connectables

Reference number
ISO/TR 22696:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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*.

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

An increasing number of Personal Health Devices (PHDs) are designed to exchange information electronically with other health IT systems in the user environment, and such information is frequently exchanged through the internet, which is publicly open to various types of data.

Various PHDs are connected through the network, and the needs for a secure bidirectional connection for the new PHDs are getting more attention. Security threats to PHDs can spread damages to the existing healthcare systems through the networks that are meant to be kept secure for the benefit of the healthcare service users. The threats can cause not only economical damage but also risk to human lives. Currently, there is no proper guidance for identification and authentication of the PHDs in case of the bidirectional connection between the PHDs and the gateway.

Identification and authentication for various connectable personal devices should be consistently applied throughout the lifecycle. This identification and authentication issue should be considered by the manufacturers of the devices and the operators of the healthcare service. The whole identification and authentication process is critical for the successful operation and management of PHDs. Identification and authentication guidance should be set up to secure the healthcare service by providing the interoperability among devices and gateway.

This identification and authentication issue should be both considered by healthcare device manufactures and healthcare delivery organizations. The healthcare device manufacturers and operators should provide users with mutual authentication between the gateway and the connectable devices for a secure bidirectional communication and the integrity of sensitive personal health information.

Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)

1 Scope

The document gives guidance for managing healthcare service security using connectable personal health devices. This document considers unidirectional data uploading from the PHD to the gateway (manager device), however, there are many clinical use cases for bidirectional data exchange.

This document is applicable to identification and authentication between the bidirectionally connected PHDs and gateway by providing possible use cases and the associated threats and vulnerabilities. Since some smart devices with mobile healthcare apps and software might connect to the healthcare service network, these devices will be considered connectable PHDs in this document. This document addresses those devices used in a homecare setting, where the knowledge and capabilities regarding the use of PHDs might not be as advanced as in other healthcare settings.

This document excludes specific protocols, methods and technical solutions for identification and authentication.

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 terminological 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
access control
means to ensure that access to assets is authorized and restricted based on business and security requirements

[SOURCE: ISO/IEC 27000:2018, 3.1]

3.2
attack
assault on a system that comes from an intelligent *threat* (3.18) — i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Note 1 to entry: There are different commonly recognized classes of attack:

— An "active attack" attempts to alter system resources or affect their operation.

— A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.

— An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

— An "outside attack" is initiated from outside the perimeter by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.9]

3.3
authenticate
verify the identity of a *user* (3.20), user device, or other entity, or the *integrity* (3.11) of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.12]

3.4
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.5
authorization
right or permission that is granted to a system entity to access a system resource

[SOURCE: IEC/TS 62443:2009, 3.2.14]

3.6
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.7
bidirectional connection
two-way communication connection between a *personal health device* (3.16) and a *gateway* (3.9) for data exchange

3.8
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.9
gateway
relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other

Note 1 to entry: Also described as an intermediate system that is the translation interface between two computer networks.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.53]

3.10
identification
process of identifying and recognizing a *user* (3.20), *personal health device* (3.16), or home *gateway* (3.9) as a unique entity that establishes connections

3.11
integrity
quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data

Note 1 to entry: In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.60]

3.12
interface
logical entry or exit point that provides access to the module for logical information flows

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.62]

3.13
malicious code
programs or code written for the purpose of gathering information about systems or *users* (3.20), destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel

Note 1 to entry: Malicious code attacks can take the form of viruses, worms, Trojan horses, or other automated exploits.

Note 2 to entry: Malicious code is also often referred to as "malware".

[SOURCE: IEC/TS 62443-1-1:2009, 3.2.70]

3.14
manufacturer
natural or legal person with responsibility for designing, manufacturing, packaging or labelling a *medical device* (3.15), assembling a system, or adapting a medical device before it is placed on the market or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party

3.15
medical device
instrument, apparatus, implement, machine, appliance, implant, in vitro reagent or calibrator, software, material or other similar or related article

a) intended by the *manufacturer* (3.14) to be used, alone or in combination, for human beings for one or more of the specific 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 for medical or diagnostic purposes by means of in vitro examination of specimens derived from the human body; and

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

Note 1 to entry: The definition of a device for in vitro examination includes, for example, reagents, calibrators, sample collection and storage devices, control materials, and related instruments or apparatus. The information provided by such an in vitro diagnostic device may be for diagnostic, monitoring or compatibility purposes. In some jurisdictions, some in vitro diagnostic devices, including reagents and the like, might be covered by separate regulations.

Note 2 to entry: Products which can be considered to be medical devices in some jurisdictions but for which there is not yet a harmonized approach, are:

— aids for disabled/handicapped people;

— devices for the treatment/diagnosis of diseases and injuries in animals;

— accessories for medical devices (see Note 3 to entry);

— disinfection substances;

— devices incorporating animal and human tissues which might meet the requirements of the above definition but are subject to different controls.

Note 3 to entry: Accessories intended specifically by manufacturers to be used together with a 'parent' medical device to enable that medical device to achieve its intended purpose should be subject to the same GHTF procedures as apply to the medical device itself. For example, an accessory will be classified as though it is a medical device in its own right. This may result in the accessory having a different classification than the 'parent' device.

Note 4 to entry: Components to medical devices are generally controlled through the manufacturer's quality management system and the conformity assessment procedures for the device. In some jurisdictions, components are included in the definition of a 'medical device'.

[SOURCE: IEC 80001-1:2010, 2.14]

3.16
personal health device
PHD
connectable *medical device* (3.15) used in the home healthcare environment

3.17
public key infrastructure
PKI
complex security system environment for providing encryption and electronic signature using a public key algorithm

Note 1 to entry: Here, it means the basic technology of the equipment certificate used in the smart health care device.

3.18
threat
potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

3.19
unidirectional connection
one-way communication connection between a *personal health device* (3.16) and a *gateway* (3.9)

Note 1 to entry: This standard does not provide any method to ensure security of data exchange. It assumes that data exchange is secured by other means, for example, a secure transport channel.

3.20
user
entities using *personal health devices* (3.16) to transfer information

4 Abbreviated terms

I&A Identification and Authentication

ICS Industrial Control System

ICU Intensive Care Unit

PHI Personal Health Information

5 Information security objectives in healthcare and PHDs

Information security has been addressed in three security objectives: confidentiality, integrity, and availability. Although in most information technology domains confidentiality has been considered more important than integrity and availability, there is room for debate, depending on the needs of each situation.

For example, when it comes to the ICS, availability is deemed more significant than integrity or confidentiality. Its importance is clear when considering the large amount of loss and high level of impact that the stoppage of national power plants or burning furnaces have.

In the healthcare domain, it is crucial to prioritize confidentiality, integrity and availability according to specific requirements of the domain. Practical guidelines for emergency situations prompt health-care providers to consider human life above any other requirements, i.e. privacy rules.

When it comes to integrity and availability, it is difficult to definitively prioritize one over the other. For example, it is clear that availability would be the priority for a patient in an ICU since a system-off would be fatal and cause death. For a patient who is supported by a pacemaker, the availability of the pacemaker is also critical.

However, if the data that is connected to a patient's critical equipment in ICU or to a pacemaker is manipulated or falsely reported, the patient faces the same risks that those associated with unavailability. Hence, integrity should also be prioritized in the healthcare sector when it comes to the PHD's security and accurate functionality, since contaminated data can pose a threat to human life.

6 Security vulnerabilities and threats of PHDs

6.1 Security vulnerabilities of PHDs

PHDs are defined by the ISO/IEEE 11073 series as a health device that is normally used for measurement by a chronic patient, especially seniors, for telemedicine at home or in other buildings. Currently, the number of medical services and health management programs supported by Medical IoT devices is growing dramatically, which requires the security vulnerabilities of the devices to be sufficiently scrutinized.

Security vulnerabilities of PHDs are related to their projected benefits; usability, real-time interaction, remote access, etc. The common vulnerabilities concerned are as follows:

— unsecure end-point;

— wireless real-time services;

— bidirectional connection.

Data collected from PHDs go to web/app services or medical centres through gateways, which can be divided into dedicated gateways and non-dedicated gateways, such as smart-phones, tablet PCs, or desk-top computers. In many cases, PHDs are operated in private places with unsecure endpoints by a person who manages various networked equipment without deep knowledge of IT.

Wireless real-time service refers to ongoing connection anytime and anywhere. Wireless connection is especially vulnerable to attacks such as packet sniffing and rogue access point. As brand-new vulnerabilities like Blueborne were discovered, WPA2's reputation of being a secure solution was compromised.

PHDs provide more diverse benefits in healthcare services. Unlike traditional unidirectional connexions, which simply upload a user's data (especially very sensitive bio-data of the device user), emerging services should set up a bidirectional connection to manage heartbeats or track doses of insulin according to the PHI provided by the user. This bidirectional connection might produce a new type of vulnerability through malicious gateways, a critical problem that might even cause physical disorders, e.g. insulin shock or heart attack. While there have been no documented examples of this occurring, this remains a potential threat.

6.2 Security threats of PHDs

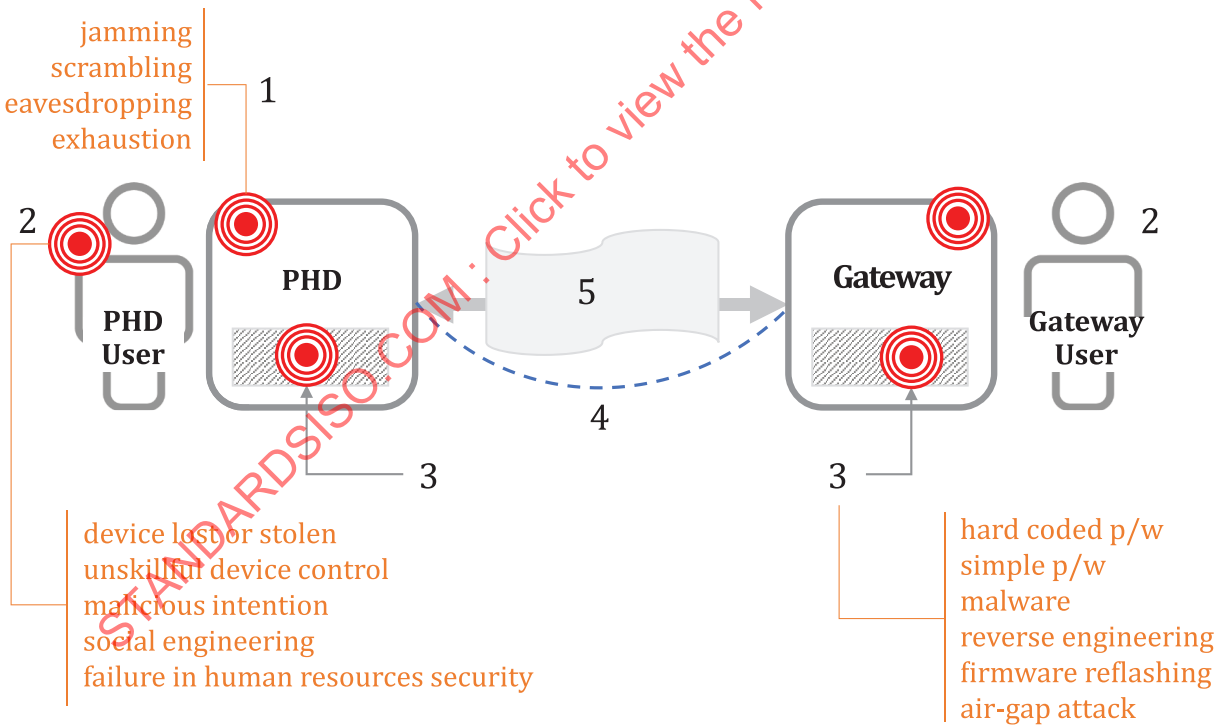
As shown in Figure 1, during data exchange between PHDs and gateways, integrity is likely to fail in five attack surfaces; Physical devices or gateway, Users, Application, which this document focuses on, Network and Data.

This model assumes that

— a user's health data is collected through application of a PHD,

— the two users of the figure below are likely to be the same person, and

— PHD and gateway can be separated respectively or integrated into one device.



Key

1 physical devices or gateway
2 users
3 application
4 network
5 data

Figure 1 — PHD-to-Gateway security threats

7 Identification and authentication for connectable PHDs

7.1 General

Healthcare devices and services using bidirectional connection have emerged and this type of service is expected to be much more popular in the future. Taking into account the tendency in healthcare, mutual device-to-device I&A is an effective means to ensure the data integrity of PHI. This document provides security recommendations in three areas for mutual I&A between PHDs and gateway:

— person or entities (including devices) I&A;

— application I&A;

— access control.

See Annex A for additional information.

7.2 Person or entity identification and authentication

7.2.1 Objectives

To ensure that the person or entity who has access to devices, PHI, or resources is the legitimate user or entity in accordance with the level(s) of access.

7.2.2 User or entity registration procedure

7.2.2.1 Recommendations

To ensure secure connection and communication between PHDs, all users or entities including human users, PHDs, and dedicated or non-dedicated gateways should register or de-register according to formally established procedures. The purpose of the registration and de-registration procedures is to assign access rights that are consistent with the level(s) of access to the device, PHI, or resources. To achieve mutual identification and authentication, gateways should be registered in all PHDs connected and all PHDs should be registered in the connected gateway.

7.2.2.2 Implementation guidance

a) User or entity includes the following:

— human users who use or manage the applicable medical device or gateway;

— medical devices used as a PHD by human users, and are communicated with a gateway;

— application installed in PHDs used by human users which communicates with gateways;

— gateways that communicate with medical devices to address health data.

b) User or entity registration procedure include the following:

— assigning a unique ID to all users or entities;

— providing a user ID with the applicable access rights that are consistent with roles and levels of security;

— managing all accounts of authorized users by ways including adding, activating, modifying, disabling, and removing accounts;

— assigning access rights on the basis of least privilege and duty of segregation.

7.2.3 Device identification and authentication

7.2.3.1 Recommendations

All devices including PHDs and gateway should be uniquely identified and authenticated.

7.2.3.2 Implementation guidance

a) PHDs and gateway should be uniquely identified and authenticated using the defined authentication method before establishing a connection in accordance with applicable security policies and procedures.

b) To achieve mutual authentication, PHDs and gateway should each be authenticated in a secure manner, e.g. using cryptographic mechanism.

c) Dynamic addresses should be assigned to PHDs and gateway with lease information and duration in accordance with applicable security policies and procedures.

7.2.4 Human user identification and authentication

7.2.4.1 Recommendations

All human users should be uniquely identified and authenticated.

7.2.4.2 Implementation guidance

a) Human user identification and authentication should be applied to all interfaces that provide human user access. This capability supports segregation of duties and least privilege in accordance with applicable security policies and procedures.

b) Multifactor authentication should be employed, if necessary, to enhance security.

7.2.5 Authentication information management

7.2.5.1 Recommendations

Authentication information should be managed in a secure manner in accordance with applicable security policies and procedures.

7.2.5.2 Implementation guidance

a) Default vendor passwords should be changed immediately after the installation of devices, services, or applications.

b) If provided initial authentication information by services or applications, the user or entity should be forced to change the initial authentication information on first use.

c) Verification procedure of the user identity should be established prior to providing new, changed, or temporary authentication information.

d) Temporary authentication information should be given to users in a secure manner. Its activation should be limited to a short duration and/or should be disabled automatically after a scheduled time.

e) Authentication information should have sufficient strength against security compromises.

f) Authentication feedback should be provided in an obscure manner to protect the information from exploitation and wrongful use by unauthorized users. Obscure feedback includes, e.g. displaying asterisks when typing passwords.

g) All users should

1) keep authentication information in a secure manner,

2) change authentication information whenever any compromise is indicated, and

3) not share individual user authentication information.

7.3 Application, identification and authentication

7.3.1 Objectives

To ensure accuracy and consistency of applications for PHDs and gateway.

7.3.2 Unique Identification and Authentication

7.3.2.1 Recommendations

Particular applications should be uniquely identified and authenticated in accordance with applicable security policies and procedures.

7.3.2.2 Implementation guidance

a) Particular applications should be uniquely identified and authenticated before establishing communication with devices, users, or other services/applications in accordance with applicable security policies and procedures.

b) Utility programs that affect the system should be strongly managed by a limited number of authorized users and should be separated from application.

7.3.3 Application, firmware and information integrity

7.3.3.1 Recommendations

Unauthorized change of applications, firmware, and information including PHI should be detected, recorded, reported, and protected through integrity verification mechanisms.

7.3.3.2 Implementation guidance

a) Security mechanisms to ensure integrity of software, firmware, and information include but are not limited to parity checks, cyclical redundancy checks, and cryptographic hashes. Integrity verification is an effective countermeasure against detouring the established security mechanism.

b) Monitoring configuration change related to security is recommended to ensure accuracy and consistency.

7.3.4 Secure upgrade

7.3.4.1 Recommendations

Security policies and procedures for application and firmware upgrades should be established.

7.3.4.2 Implementation guidance

a) Reliable mechanisms to ensure secure upgrades of application and firmware should be considered.

b) Security patches to mitigate the possibilities of vulnerabilities should be maintained in the latest version.

c) Testing the mechanism after a secure upgrade is recommended. A successful test will ensure that the upgrade has been completed without unexpected malfunction of the device or application.

7.3.5 Input validation

7.3.5.1 Recommendations

Input data should be verified to prevent malfunction or malicious tampering attempts.

7.3.5.2 Implementation guidance

Invalid input data can be related to security issues such as buffer over flow, SQL injection attack, and cross site scripting. Format and content validity of syntax and semantics, such as character set and length, numerical range, and acceptable values, should be checked.

7.3.6 Information confidentiality

7.3.6.1 Recommendations

Information confidentiality, which is stored in a device or transmitted over networks, should be protected in accordance with applicable security policies and procedures.

7.3.6.2 Implementation guidance

Information to protect includes PHI, system-related information, and information requiring compliance with applicable laws or regulations. System-related information to protect includes, e.g. system configurations, log data, or rule sets for firewalls, gateway, IDS and IPS. Information confidentiality can be achieved through physical protection, encryption, and other mechanisms.

7.4 Access control

7.4.1 Objectives

To allow only authorized people or entities to access devices, PHI, or resources in accordance with level(s) of access. These controls represent the high-level mitigations. Consideration of how these can be implemented in the multiple environments in which they operate should be taken into account. For instance, the capability of the home user might be different from the operation of PHDs in a healthcare organization.

7.4.2 Secure log-on procedures

7.4.2.1 Recommendations

Access to system and applications should be controlled by a secure log-on procedure in accordance with applicable security policies and procedures.

7.4.2.2 Implementation guidance

a) A suitable authentication technique for the level of security assigned to a user should be selected to prove the claimed identity of a user.

b) Where strong authentication and identity verification is required, multifactor authentication that uses additional methods such as cryptographic means, smart cards, tokens, or biometric means should be taken into consideration.

c) log-on procedures should be designed to minimize the risk of unauthorized access. A good log-on procedure should

   1) not display system or application identifiers until the log-on process has been successfully completed,

   2) not provide help messages that would aid an unauthorized user during the log-on procedure,

   3) protect against brute force log-on attempts,

   4) log successful and failed attempts,

   5) display the date and time of the previous successful log-on,

   6) not transmit passwords in clear text over a network, and

   7) terminate inactive sessions after a defined inactive period in accordance with applicable security policies and procedures.

7.4.3 Emergency account

7.4.3.1 Recommendations

Emergency accounts should be established to respond to emergency situations that require immediate access to devices, PHI, services, or applications in accordance with applicable security policies and procedures.

7.4.3.2 Implementation guidance

a) Healthcare providers who intend to help a user in an emergency situation need rapid access to devices, PHI, services, or applications without personal user id and authentication processes. Particular PHDs positioned directly inside the human body (e.g. implanted pacemaker) can cause a fatal risk to a patient if malicious attacks or functional problems occur. Alternative methods to bypass formal identification and authentication processes during emergencies is a critical concern in the health/medical domain (break glass functionality).

b) Emergency accounts should be activated within a limited time period by applying automatic disabling or removal dates.

c) Emergency access should be detected, recorded, and reported through notifications to the system administrator or medical staff.

7.4.4 Automatic log-off

7.4.4.1 Recommendations

A user who has been inactive for a defined time period should not access PHI without re-identification and re-authentication procedures in accordance of applicable security policies and procedures.

7.4.4.2 Implementation guidance

To protect the PHI from unauthorized access when a user leaves behind PHD without sign-off or doesn't use during the pre-defined time period, various methods could be considered, e.g. automatic log-off or activating screen saver.

7.4.5 Device lock

7.4.5.1 Recommendations

Information such as the PHI stored in devices should be secured if the devices are lost or stolen, or if the user is unavailable.

7.4.5.2 Implementation guidance

a) Device lock is a countermeasure to protect PHD by unauthorized users from compromising confidentiality and integrity of information in devices.

b) Device lock is released through re-identification and re-authentication procedures.

c) Access from USB ports should be managed to protect devices from contaminated devices or unauthorized users, since a USB port has a high possibility of being a pathway for malicious code or data leakage. Mobile devices as a PHD or gateway should identify and authenticate any access through a USB port.

d) Removable devices used as a PHD or as a component of a PHD should ensure that sensitive data such as PHI is protected in a secure manner. For example, cryptography mechanism should be applied to the data of the removable device.

Annex A
(informative)

Mapping to other standards

Table A.1 — Mapping to other standards

Category	Sub-category	Related control
7.2 Person or entity identification and authentication	7.2.2 User and entity registration procedure	IEC 62443-3-3:2013: SR1.1, SR 1.2, SR 1.3, SR 1.4 ISO 27799:2016: 9.2.1, 9.2.6, 9.4.2 NIST SP 800-53 rev.4: IA-1, IA-2, IA-4
	7.2.3 Device identification and authentication	IEC 62443-3-3:2013: SR1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 ISO 27799:2016: 9.4.2, 9.4.3 NIST SP 800-53 rev.4: AC-2, IA-1, IA-3, IA-7 IEC/TR 80001-2-2:2012: 4.12
	7.2.4 Human user identification and authentication	IEC 62443-3-3:2013: SR1.1, SR 1.3, SR 1.4, SR 1.5, SR 1.7 ISO 27799:2016: 9.2.4, 9.4.2, 9.4.3 NIST SP 800-53 rev.4: AC-2, IA-1, IA-2, IA-4, IA-5, IA-8 IEC/TR 80001-2-2:2012: 5.12
	7.2.5 Authentication information management	IEC 62443-3-3:2013: SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.9 ISO 27799:2016: 9.2.1, 9.2.4, 9.3.1, 9.4.3 NIST SP 800-53 rev.4: IA-5, IA-6, IA-7 IEC/TR 80001-2-2:2012: 5.12
7.3 Application identification and authentication	7.3.2 Application identification and authentication	IEC 62443-3-3:2013: SR1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7 ISO 27799:2016: 9.4.2, 9.4.3, 9.4.4 NIST SP 800-53 rev.4: AC-2, IA-1, IA-9
	7.3.3 Application, firmware and information integrity	IEC 62443-3-3:2013: SR3.4 ISO 27799:2016: 14.1.2 NIST SP 800-53 rev.4: SC-8, SC-28, SI-7
	7.3.4 Secure upgrade	IEC 62443-3-3:2013: SR 2.1 ISO 27799:2016: 12.5.6, 14.2.4, 14.2.9 NIST SP 800-53 rev.4: CM-3, CM-5, CM-7, CM-11 IEC/TR 80001-2-2:2012: 5.5, 5.11
	7.3.5 Input validation	IEC 62443-3-3:2013: SR3.5 NIST SP 800-53 rev.4: AC-3, SI-10
	7.3.6 Information confidentiality	IEC 62443-3-3:2013: SR 4.1 ISO 27799:2016: 8.2.3, 8.3.1, 12.1.2, 14.2.2, 14.2.3, 14.2.4, 18.1.3 NIST SP 800-53 rev.4: CM-3, CM-5, MP-4, MP-5, SC-28