

# American National Standard

## ANSI/AAMI/ UL 2800-1-1: 2022

Standard for Risk Concerns  
for Interoperable Medical  
Products





# Standard for Risk Concerns for Interoperable Medical Products

Approved 20 May 2022 by  
**AAMI**

Approved 10 June 2022 by  
**American National Standards Institute, Inc.**

**Abstract:** Specifies a baseline set of requirements for assuring safe and secure interoperability for Interoperable Medical Systems.

**Keywords:** interoperability requirements, medical systems, medical devices, interoperable systems

## Commitment for Amendments

This Standard is issued jointly by the Association for the Advancement of Medical Instrumentation (AAMI) and Underwriters Laboratories Inc. (UL). Comments or proposals for revisions or any part of the standard may be submitted to AAMI and/or UL at any time. Revisions to this Standard will be made only after processing according to the Standards development procedures of AAMI and UL.

*Published by*

AAMI  
901 N. Glebe Road, Suite 300  
Arlington, VA 22203  
[www.aami.org](http://www.aami.org)

© 2022 by the Association for the Advancement of Medical Instrumentation

All Rights Reserved

This publication is subject to copyright claims of AAMI. No part of this publication may be reproduced or distributed in any form, including an electronic retrieval system, without the prior written permission of AAMI. All requests pertaining to this document should be submitted to AAMI. It is illegal under federal law (17 U.S.C. § 101, *et seq.*) to make copies of all or any part of this document (whether internally or externally) without the prior written permission of the Association for the Advancement of Medical Instrumentation. Violators risk legal action, including civil and criminal penalties, and damages of \$100,000 per offense. For permission regarding the use of all or any part of this document, contact the Copyright Clearance Center.

---

Copyright © 2022 Underwriters Laboratories Inc.

UL's Standards for Safety are copyrighted by UL. Neither a printed nor electronic copy of a Standard should be altered in any way. All of UL's Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of UL.

This ANSI/UL Standard for Safety consists of the Second Edition. The most recent designation of ANSI/UL 2800-1 as an American National Standard (ANSI) occurred on February 25, 2019. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page (front and back), or the Preface.

Comments or proposals for revisions on any part of the Standard may be submitted to UL at any time. Proposals should be submitted via a Proposal Request in UL's On-Line Collaborative Standards Development System (CSDS) at <https://csds.ul.com>.

To purchase UL Standards, visit UL's Standards Sales site at <http://www.shopulstandards.com/HowToOrder.aspx> or call toll-free 1-888-853-3503.

---

Printed in the United States of America

**ISBN 978-1-57020-844-7**

## Contents

Page

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Committee representation.....                                                      | iv |
| AAMI Standard .....                                                                | v  |
| Standard for Risk Concerns for Interoperable Medical Products.....                 | 1  |
| 1 Introduction .....                                                               | 1  |
| 2 Scope .....                                                                      | 2  |
| 3 Referenced Publications .....                                                    | 2  |
| 4 Terms and Definitions .....                                                      | 3  |
| 5 Risk Concerns .....                                                              | 3  |
| Annex A (Informative) Interoperability Usability Concepts .....                    | 11 |
| Annex B (Informative) Security Properties of Interoperable Medical Systems .....   | 15 |
| Annex C (Informative) Clinical Properties of Interoperable Medical Systems.....    | 17 |
| Annex D (Informative) Engineering Properties of Interoperable Medical Systems..... | 37 |
| Annex E (Informative) Services for Interoperable Medical Systems .....             | 48 |

## Committee representation

### Association for the Advancement of Medical Instrumentation AAMI/UL Joint Committee for Medical Device Interoperability, JC 2800

The publication of AAMI/UL 2800-1-1:2022 as a new American National Standard was initiated by the AAMI/UL Joint Committee for Medical Device Interoperability, JC 2800.

This list represents the membership at the time the Committee balloted on the final text of this edition. Since that time, changes in the membership may have occurred.

*Cochairs:* Diana P. Jordan  
Ovidiu Munteanu

*Members:* Dave Arney, CIMIT (MGH Anesthesia & Biomedical Engineering)  
Oliver Christ, Prosystem AG  
R Cooper, Eurofins E&E North America  
Holly Drake, Dexcom Inc.  
Sherman Eagles, SoftwareCPR  
Scott Eaton, Mindray DS USA Inc  
Kenneth Fuchs, Draeger Medical Systems Inc.  
Julian Goldman, Massachusetts General Hospital  
Pamela K. Gwynn, UL LLC  
John Hatcliff, Kansas State University  
Jacob Johnson, Kaiser Permanente  
Diana Pappas Jordan (JC Cochair), Underwriters Laboratories Inc.  
Edmund Kienast, National E-Health Transition Authority (NEHTA)-Australia  
Todd Konieczny, Intertek Testing Services  
Patty Krantz, Medtronic Inc.  
Insup Lee, University of Pennsylvania  
Marina Lee, Staubli Electrical Connectors, Inc.  
Ovidiu Munteanu JC Cochair, AAMI  
Steve Nichols, GE Healthcare  
Geetha Rao, Springborne Life Sciences  
Tracey Rausch, DocBox Inc.  
Daniel Rubery, NxStage Medical, Inc.  
Patricia A. Sena (JC Project Manager), Underwriters Laboratories Inc.  
Elliot Sloane, Center for Healthcare Information Research & Policy  
Erin Sparnon, ECRI  
Sandy Weininger, US FDA/CDRH

---

NOTE—Participation by federal agency representatives in the development of this technical information report does not constitute endorsement by the federal government or any of its agencies.

---

## AAMI Standard

This Association for the Advancement of Medical Instrumentation (AAMI) standard implies a consensus of those substantially concerned with its scope and provisions. The existence of an AAMI standard does not in any respect preclude anyone, whether they have approved the standard or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standard. AAMI standards are subject to periodic review, and users are cautioned to obtain the latest editions.

CAUTION NOTICE: This AAMI standard may be revised or withdrawn at any time. AAMI procedures require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of publication. Interested parties may obtain current information on all AAMI standards by calling or writing AAMI.

All AAMI standards, recommended practices, technical information reports, and other types of technical documents developed by AAMI are voluntary, and their application is solely within the discretion and professional judgment of the user of the document. Occasionally, voluntary technical documents are adopted by government regulatory agencies or procurement authorities, in which case the adopting agency is responsible for enforcement of its rules and regulations.



# Standard for Risk Concerns for Interoperable Medical Products

## 1 Introduction

1.1 The AAMI/UL 2800 series of standards covers the interoperability of medical products. AAMI/UL 2800-1 is the general standard that specifies a baseline set of requirements for assuring safe and secure interoperability for interoperable medical systems. The requirements in the AAMI/UL 2800-1 standard are supplemented by the requirements in additional AAMI/UL 2800 standards. These additional standards are intended to be used in conjunction with the general standard and applied as needed. While this introduction applies to all of the AAMI/UL 2800 series of standards, the scope section of each additional standard describes what is covered by that standard.

1.2 Multiple stakeholders may participate in the development, deployment, assembly, and operation of a medical system with interoperable elements. Such a system, referred to as an interoperable medical system, should minimize patient risks, maintain clinical effectiveness, ensure timely and adequate access to data while protecting its security, and enable adequate provision of care. In order to facilitate alignment of stakeholders around these aims, the AAMI/UL 2800 series of standards establishes a baseline set of requirements for assuring safe and secure interoperability.

1.3 Each stakeholder will need to determine the specific level and manner in which interoperability will be specified and assured for its interoperable medical products. However, a specific system may be developed, assembled, deployed, and operated through a range of processes undertaken by multiple stakeholders. Specific activities in these processes assure interoperability. In order for stakeholders to collectively accomplish this, the processes need to be linked effectively.

1.4 Effective linkage of processes across multiple stakeholders is a core focus of the AAMI/UL 2800 series of standards. This first requires that each stakeholder adequately assesses and manages safety and security vulnerabilities of its interoperable medical products. Secondly, it requires that each stakeholder understands and conforms with interoperability aspects of disclosed specifications of an interoperable medical product which it acquires or with which it interoperates, including the consequent safety and security characteristics. Finally, it requires that each stakeholder clearly communicates to the other stakeholders the information required to assure interoperability.

1.5 The requirements in the AAMI/UL 2800 series of standards are intended to apply to medical devices, as well as other connected infrastructure elements, and interoperable medical systems constructed from these. The AAMI/UL 2800 series of standards is intended to be used by individual stakeholders.

1.6 The AAMI/UL 2800 series of standards employ a lifecycle process approach to organizing requirements. In addition to a set of broad management functions, the standards provide for a set of interoperability planning, realization, deployment, and monitoring activities. These activities also incorporate cross-cutting requirements for security and risk management. The standards recognize that a given organization may be responsible for only a part of the full range of activities required for an interoperable medical system. Furthermore, the organization's interoperable medical products may provide only a specific or limited functionality. To accommodate this, the standards provide for flexibility in the scope, sequence, and interaction of these activities. Finally, the standards provide requirements and supplementary guidance on key clinical and engineering properties of an interoperable medical system that are essential to assuring safe and secure interoperability and provide guidance on lifecycle activities.

1.7 The requirements provide a baseline for assuring safe and secure interoperability throughout the lifecycle of the interoperable medical system. In order to meet these requirements, a set of lifecycle processes needs to be established.

It is anticipated that many organizations in the interoperability ecosystem will also have requirements for formal quality and risk management processes, as well as those related to specific aspects of product development, such as usability, software development, electrical and biological safety. The lifecycle processes in the AAMI/UL 2800 series of standards may be integrated into the organization's processes previously established for meeting quality and risk management and product-specific requirements.

1.8 As part of complying with the AAMI/UL 2800 series of standards, an organization will need to understand its specific role in the interoperability ecosystem, as well the role of the various other stakeholders. It is essential that responsibilities for meeting specific requirements are unambiguously communicated to other stakeholders. The standards include requirements for disclosure and other communications. These may be helpful in for identifying contractual requirements with other stakeholders.

1.9 The establishment of processes for assuring safe and secure interoperability should take into account the role of the organization in the interoperability ecosystem, and regulatory requirements applicable to the organization's activities. It is not the intent of the AAMI/UL 2800 series of standards to imply the need for uniformity in the structure of different processes for assuring interoperability, uniformity of documentation or alignment of documentation to the clause structure of these Standards.

1.10 The above approach enables an organization to establish processes that are consistent with the role it plays in the interoperability ecosystem. It also enables the organization to manage its activities in a manner appropriate to the scope of its interoperable medical products.

## 2 Scope

2.1 This Standard is applicable to interoperable medical products, including assembled systems of interoperable medical products that comprise or are intended to be incorporated into interoperable medical systems within an interoperable environment.

2.2 This Standard specifies a baseline set of risk concerns for assuring safe and secure interoperability for interoperable medical systems.

## 3 Referenced Publications

3.1 Any undated reference to a code or standard appearing in the requirements of this Standard shall be interpreted as referring to the latest edition of that code or standard.

3.2 The following standards are referenced in this Standard:

AAMI/UL 2800-1, *Medical Device Interoperability*

AAMI/UL 2800-1-2, *Interoperable Item Development Life Cycle*

AAMI/UL 2800-1-3, *Interoperable Item Integration Life Cycle*

IEC 60601-1, *Medical Electrical Equipment – Part 1: General Requirements for Basic safety and Essential Performance*

IEC 60601-1-8, *Medical electrical equipment – Part 1-8: General requirements for basic safety and essential performance – Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems*

IEC 80001-1, *Application of Risk Management for IT-Networks Incorporating Medical Devices – Part 1: Roles, Responsibilities and Activities*

ISO 14971, *Medical Devices – Application of Risk Management to Medical Devices*

UL 2900-1, *Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements*

UL 2900-2-1, *Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare Systems*

UL 2900-2-2, *Outline for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems*

UL 2900-2-3, *Software Cybersecurity for Network- Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems*

## 4 Terms and Definitions

4.1 Defined terms are located in AAMI/UL 2800-1.

## 5 Risk Concerns

### 5.1 General

5.1.1 Candidate risk concerns and SSOs described in this Standard shall be considered in the risk management and development life-cycle for an interoperable item.

### 5.2 Clinical properties

NOTE: See Annex C for candidate item requirements that support these objectives.

#### 5.2.1 Semantic interoperability

5.2.1.1 The following interoperable medical system-level risk concerns shall be considered in interoperable item risk management:

- a) Data presented to the operator for use in care-giving has an unclear interpretation (with respect medical / caregiving needs of the patient) leading to potentially harming actions or instructions by the operator.
- b) Mechanisms (such as nomenclatures) used to provide a semantic interpretation of data are inappropriate for the intended use of the product, leading the operator to have unwarranted trust in the in the data or to find the information insufficient for care-giving objectives while in the middle of patient care activities.
- c) The semantic interpretation of data is ambiguous due to uses of inconsistent or conflicting nomenclature.

5.2.1.2 The following interoperable medical system-level objectives shall be considered in the formation of the interoperable item SSOs:

- a) All medical data used within the interoperable medical system and provided to external clients of the interoperable medical system has accompanying meta-data and/or labeling ensuring the consistent and correct interpretation/use of the data as appropriate for the use specification of the interoperable medical system.

## 5.2.2 Patient identity

5.2.2.1 The following interoperable system-level risk concerns shall be considered in interoperable item risk management:

- a) Medical data, including physiological readings, gathered by an interoperable medical system and supplied to the operator or external systems to support present or future care-giving is not linked to a patient identity or is linked to an incorrect patient identity, causing care-givers to provide inappropriate care based on incorrect assumptions about the patient's current state or history.
- b) The patient data and associated patient identity is inappropriately disclosed to actors that are not authorized to acquire the patient identity, leading to loss of confidentiality for the patient.

5.2.2.2 The following interoperable system-level objectives shall be considered in the formation of the interoperable item SSOs:

- a) While an interoperable medical system is supporting care-giving for a patient, all constituents of the interoperable medical system that have a patient identity storage capability, hold an identifier corresponding to the organization's patient identifier for the patient under care.
- b) Caregiving decisions (either by an interoperable medical system operator or by an interoperable medical system constituent) are based on patient data that has accompanying context information that correctly identifies the patient to which the data pertains.
- c) When the interoperable medical system is not associated with a patient, no patient data or identifier for the patient is held in the state of the interoperable medical system or its constituent components, except for:
  - 1) Forensic information that is the subject of confidentiality risk management; or
  - 2) Data held in storage designed as a patient information system that is the subject of appropriate controls.
- d) When the interoperable medical system is associated with a patient, no identity-linked patient data within the system is communicated to actors that are not authorized to access identity-linked data for the patient under care.
- e) The instructions for use of the interoperable medical system include documentation concerning assumed identity management objectives within the operating organization that may produce a machine-readable identifier that uniquely identifies the patient within the scope of patients managed by the organization.

## 5.2.3 Operator identity, authentication, and authorization

5.2.3.1 The following interoperable medical system-level risk concerns shall be considered in interoperable item risk management:

- a) The specific operator responsible for particular actions that gives rise to patient harm or uncontrolled information disclosure cannot be identified during or after the action (e.g., inappropriate or malicious);
- b) Unauthenticated operators may, lacking appropriate physical access controls, gain access to the interoperable medical system and claim any identity, leading to actions (e.g., inappropriate or malicious) that give rise to patient harm or uncontrolled information disclosure;
- c) Unauthorized commands or access to data may, lacking appropriate physical access controls, allow unqualified or inappropriate operators to issue commands (e.g., inappropriate or malicious) that give rise to patient harm, or access data which is beyond the scope of their responsibilities, leading to uncontrolled

information disclosure;

d) Data (e.g., physician orders or patient notes), metadata (e.g., timestamps, attesting to the freshness of information), and/or commands (e.g., direct device commands to start, stop, or change treatment parameters), whose integrity and authenticity has not been verified (and therefore of unknown provenance), may be inappropriate or missing as a result of random or malicious corruption, omission, or commission, and give rise to immediate (commands, orders) or delayed (patient notes, metadata) patient harm or uncontrolled information disclosure;

e) Access control policies which are excessively strict or lack manual override capability (e.g., during emergency scenarios) may prevent individual operators from performing their duties or obtaining necessary information for patient treatment, preventing timely action to prevent patient harm; and

NOTE: The concept of least privilege is, by design, reflected more strongly in interoperable item id requirements than in operator ID requirements. This is meant to allow added operator flexibility, as appropriate and consistent with human-readable facility policies, but such latitude is not needed for interoperable items which have formally specified roles and responsibilities and perform authentication automatically;

f) Insufficiently strict access control policies (e.g. large access control rule-sets which become difficult to manage, especially with changing duties and operator turnover), leading to potential over- or under-specified authorization policies, may allow unqualified or inappropriate operators to act beyond the scope of necessity for patient treatment, leading to actions (e.g., inappropriate or malicious) that give rise to patient harm or uncontrolled information disclosure.

5.2.3.2 The following interoperable medical system-level objectives shall be considered in the formation of the interoperable item SSOs:

a) Operators of the interoperable medical system are uniquely identified;

b) Operators of the interoperable medical system are authenticated;

c) Operators within the interoperable medical system are prevented from performing unauthorized actions;

NOTE 1: Authorization is only meaningful if interoperable items are uniquely identified.

NOTE 2: Identification is trustworthy only if authentication has been successful.

d) All data and metadata and commands [information] (in transit and at rest) originated by the operator in the interoperable medical system are authenticated and therefore:

1) Is traceable to the operator; and

2) Has not been changed, or destroyed, or lost in an unauthorized or accidental manner;

e) Operator responsibility segregation is enforced using appropriate authentication and authorization mechanisms, e.g., as achieved by role-based access control (RBAC)

f) Interoperable medical system security controls of this section does not prevent the interoperable medical system from achieving its Safety Objectives;

g) The interoperable medical system identities and authentication are consistent with the identification policy necessary for achieving attribution goals of the organization associated with the deployment context of use; and

h) The interoperable medical system RBAC policies are consistent with the responsibility policies of the organization associated with the deployment context of use.

## 5.2.4 Interoperable item id, authentication, and authorization

5.2.4.1 The following interoperable medical system-level risk concerns shall be considered in interoperable item risk management:

a) The specific interoperable item responsible for particular actions that gives rise to patient harm or uncontrolled information disclosure cannot be identified during or after the action (e.g., inappropriate or malicious);

NOTE: The Organization associated with the deployment context of use cannot then to take corrective action in the form of, e.g., notifying correct manufacturers, or revoking specific device access privileges.

b) Unauthenticated items, (e.g., any medical or consumer electronic component (non-interoperable item)) may, lacking appropriate physical access controls, be attached by anyone, and thereby gain access to the interoperable medical system and claim any identity, leading to actions (e.g., inappropriate or malicious) that give rise to patient harm or uncontrolled information disclosure;

c) Unauthorized commands or unauthorized data access or manipulation may, lacking appropriate physical access controls, allow interoperable items to issue commands (e.g., inappropriate or malicious either through interoperable item malfunction, malicious action, or problematic integration) outside of their intended purpose and responsibilities within a particular interoperable medical system configuration, that give rise to patient harm, or access data outside of their intended purpose and responsibilities within a particular interoperable medical system configuration, leading to uncontrolled information disclosure;

d) Data (e.g., physician orders or patient notes), metadata (e.g., timestamps, attesting to the freshness of information), and/or commands (e.g., direct device commands to start, stop, or change treatment parameters), whose integrity and authenticity has not been verified (and therefore are of unknown provenance), may be inappropriate or missing as a result of random or malicious corruption, omission, or commission, and give rise to immediate (commands, orders) or delayed (patient notes, metadata) patient harm or uncontrolled information disclosure.

e) Access control policies which lack manual override capability (e.g. during emergency scenarios) may prevent individual interoperable items from being included in the interoperable medical system, preventing timely action to prevent patient harm; and

f) Insufficiently strict access control policies, i.e., overly permissive authorization policies, may allow inappropriate interoperable items to act beyond the scope of necessity for patient treatment, leading to actions (e.g., inappropriate or malicious) that give rise to patient harm or uncontrolled information disclosure.

5.2.4.2 The following interoperable medical system-level objectives shall be considered in the formation of the interoperable item SSOs:

a) Interoperable items within the interoperable medical system are uniquely identified;

b) Interoperable items within the interoperable medical system are authenticated;

c) Interoperable items within the interoperable medical system are prevented from performing unauthorized actions;

NOTE 1: Authorization is only meaningful if interoperable items are uniquely identified.

NOTE 2: Identification is trustworthy only if authentication has been successful.

d) All data and metadata and commands (in transit and at rest) originated by the interoperable item in the interoperable medical system is authenticated, and therefore traceable to the interoperable item, and not changed, destroyed, or lost in an unauthorized or accidental manner;

e) If the interoperable item's user interface and capabilities support operator authentication, all data and metadata and commands (in transit and at rest) originated by the interoperable item on behalf of the interoperable item's operator in the interoperable medical system is authenticated, and therefore traceable to the interoperable item's operator, and not changed, destroyed, or lost in an unauthorized or accidental manner;

f) Authentication and authorization mechanisms enforce interoperable item responsibility segregation, e.g., as achieved by Role-Based Access Control (RBAC);

g) Interoperable medical system security controls of this section do not prevent the interoperable medical system from achieving its Safety Objectives;

h) The interoperable item identity and authentication are consistent with the organization's inventory management and tracking in deployment context of use life-cycle activities; and

NOTE: Inventory management may address onboarding, provisioning, deployment, repair, retirement, and destruction of the interoperable item.

i) The interoperable item rbac policies are consistent with the access control and resource use policies of organization's infrastructure both within and outside of the context of interoperable medical systems with which the interoperable item is intended to be used.

### 5.3 Engineering properties

NOTE: See Annex [D](#) for guidance that supports these objectives.

#### 5.3.1 Interoperability item connectivity

5.3.1.1 The following interoperable medical system-level risk concerns shall be considered in interoperable item risk management:

a) Failures or performance degradations of the interoperability function of the interoperable medical system may result in inability to communicate information between constituents of the interoperable medical system, which may lead to the inability to achieve SSOs.

b) Failure to detect interoperability failures or performance degradations and subsequently notify other actors within the interoperable medical system or operators of the interoperable medical system may lead to the inability to move the system to a safe state.

5.3.1.2 The following interoperable medical system-level objectives shall be considered in the formation of the interoperable item SSOs:

a) Each constituent interoperable item's connectivity to the interoperable medical system is confirmed to be performing according to the interoperable use specification before medical functions of the interoperable medical system are activated to support care of the patient.

b) Controls are established to determine when the connectivity between each constituent interoperable item in the interoperable medical system is failing to perform according to the interoperable use specification while supporting care of the patient.

c) Controls are established to notify appropriate actors including operators and constituent interoperable items of the interoperable medical system of failure of the connectivity to perform according to the connectivity requirements of the interoperable use specification. notifications include information to support appropriate actors to move the interoperable medical system into a safe state.

d) The reliability, quality of service, and risk controls for connectivity within the interoperable medical system as

required for its medical purpose and defined in its interoperable use specification shall be determined by the risk management process.

e) Any function of the interoperable medical system that depends on communication with, and reliable performance of, external systems is documented in the interoperable use specification, justified by the risk management process, and reflected in instructions to establish appropriate risk controls within the deployment context of use.

### 5.3.2 Safe states

5.3.2.1 The following interoperable medical system-level risk concerns shall be considered in interoperable item risk management:

a) Lack of identification of safe states for the interoperable medical system in terms of states of system constituents and lack of reliable controls for moving safe state can lead directly to patient harm.

5.3.2.2 The following interoperable medical system-level objectives shall be considered in the formulation of the SSOs:

a) The safe states of the interoperable medical system are specified and expressed in terms of the states of its constituent interoperable items.

b) The conditions, including interoperability related failures and performance degradations, under which the interoperable medical system will transition to a safe state are specified.

c) The extent to which operator intervention is required, including none, for the interoperable medical system and its constituent interoperable items to transition to a safe state is disclosed.

d) The mechanisms and expected transition times by which the interoperable medical system will achieve transition to a safe state, including commands sent to constituent interoperable items and notifications to the operator are specified.

e) Upon notification to move the interoperable medical system and its constituent interoperable items to a safe state, actions to be taken by the operator are specified in instructions for use.

### 5.3.3 Time synchronization

5.3.3.1 The following interoperable medical system-level risk concerns shall be considered in interoperable item risk management:

a) Care-givers may incorrectly interpret physiological data from the interoperable medical system that is not linked to time or is incorrectly linked to the reference time of the care-giving organization. Incorrect interpretations may include belief that the data pertains to the patient's physiological state at a point in time other than then it was actually acquired, leading to an incorrect care-giver mental model of the patient's state (the state could be better or worse than it actually is/was), which could lead to inappropriate care-giving actions that result in patient harm.

b) Multiple constituents within the interoperable medical system with different notions of time may each produce time-linked data that should be understood as applying to the patient's state at the same point in time, but cannot be properly assembled by the system into a composite reading of the patient's health at a particular point in time. The inability to produce true composite assessments of the patient's physiological state may lead to harmful care-giving decisions either when operating the system or when reviewing its output at a later point in time.

c) Care-giving actions taken by the interoperable medical system or the operator which are not linked or incorrectly linked to the reference time of the operating organization and subsequently logged cannot be

accurately assessed in future caregiving activities or forensic activities, leading to an incorrect understanding of the history of the system's actions or the history of care-giving for the patient, which may lead to failure to correct inappropriate actions or failure to take required actions.

5.3.3.2 The following interoperable system-level objectives shall be considered in the formation of the interoperable item ssos:

- a) The interoperable medical system adheres to a disclosed policy for determining and representing a system reference time. All the interoperable components within the interoperable medical system adhere to the policy and have a common time reference up to a tolerance justified by the interoperable medical system risk management.
- b) Patient physiological readings are associated to a system-aligned time reference that indicates the point in time that the readings were acquired.
- c) Controls are established to record the associated to a system-aligned time reference that indicates the point in time at which an action was taken by operators or interoperable items acting on or within the interoperable medical system.
- d) The interoperable medical system-wide reference time is in correspondence with the operational context of use reference time up to a tolerance justified by the system risk management policy.
- e) Labelling for the interoperable item and interoperable medical system indicates an assumption that the operating organization adheres to a policy for determining an operating context reference time that provides all users of the system with common understanding of time.

#### 5.3.4 Shared resources, and data/time partitioning

5.3.4.1 The following interoperable medical system-level risk concerns shall be considered in the formation of the interoperable item SSOs:

- a) Execution of interoperability-related functions realizing risk controls may not have adequate computational resources to perform to specification due to unanticipated interference with other functions, leading to potential patient harm.
- b) Execution of interoperability-related functions realizing risk controls may not have adequate access to shared resources and services needed to perform to specification due to resource contention or inappropriate design of access controls, leading to potential patient harm.
- c) Communication over interoperability mechanisms between constituents of the interoperable medical system or between the interoperable medical system and systems in its context of use may not have adequate communication resources to perform to specification due to unanticipated interference with other communication, leading to potential patient harm.

5.3.4.2 The following interoperable system-level objectives shall be considered in the formation of the interoperable item SSOs:

- a) Dependences on shared resources, dependences of constituent interoperable items on each other, and non-interference objectives in the interoperable medical system is specified in terms of the interoperability architecture.

NOTE: Specified non-interference objectives may be informed by goals related to:

- 1) Composing interoperable items without resulting in unanticipated emergent properties,

2) Achieving fault containment and security objectives, and

3) Facilitating assurance in the presence of changes to the interoperable medical system and its constituent interoperable items.

b) The interoperable medical system and its constituent interoperable items specify and realize controls, including space partitioning and time partitioning, that enforce non-interference properties based on resource allocation strategies, in terms of priority/criticality of functions for achieving SSOs, as justified by the risk management process.

c) The interoperable medical system and its constituent interoperable items mediate access to shared resources in a manner that enables predictable and timely access as needed for medical functionality while achieving SSOs.

d) The interoperable medical system and its constituent interoperable items signal current or impending failure or degradation of its medical function or violation of SSOs due to lack of access or scarcity of shared resources.

## 5.4 Service properties

5.4.1 The following interoperability properties related to provisioning, deployment, and operational services shall be addressed:

a) Alarms and alarm handling;

b) Data logging; and

c) Data store.

NOTE: See Annex E for detailed requirements.

## 5.5 Security properties

5.5.1 The following security properties shall be addressed:

a) All data and metadata and commands (in transit and at rest) in the interoperable medical system are authenticated.

b) The interoperable medical system ensures that information is not changed, destroyed, or lost in an unauthorized or accidental manner.

c) Actors within the interoperable medical system are authenticated.

d) Actors within the interoperable medical system are prevented from performing unauthorized actions. Actors within the system are authenticated to perform actions.

e) The interoperable medical system should provide a capability for post-facto analysis to determine the actor responsible for generating and modifying information within the system.

f) The interoperable medical system should provide a capability for post-facto root cause analysis to determine the actor responsible for any action on information within the system.

g) The confidentiality of all data and metadata (in transit and at rest) in the interoperable medical system is maintained.