UL 2800-1-1

STANDARD FOR SAFETY

Risk Concerns for Interoperable Medical Products

UL Standard for Safety for Risk Concerns for Interoperable Medical Products, UL 2800-1-1

First Edition, Dated June 10, 2022

Summary of Topics

This is the First Edition of ANSI/AAMI/UL 2800-1-1, the Standard for Risk Concerns for Interoperable Medical Products.

The new requirements are substantially in accordance with Proposal(s) on this subject dated November 5, 2021.

No Text on This Page

AAMI
AAMI 2800-1-1
First Edition

Underwriters Laboratories Inc
UL 2800-1-1
First Edition

Standard for Risk Concerns for Interoperable Medical Products

June 10, 2022

ANSI/UL 2800-1-1-2022

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.

This ANSI/UL Standard for Safety consists of the First Edition. The most recent designation of ANSI/AAMI/UL 2800-1-1 as an American National Standard (ANSI) occurred on June 10, 2022. 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.

CONTENTS

Annex E (Informative) Services for Interoperable Medical Systems

Preface

This is the joint AAMI/UL Standard for Risk Concerns for Interoperable Medical Products, AAMI/UL 2800-1-1. It is the first edition of AAMI 2800-1-1 and the first edition of UL 2800-1-1.

This Joint Standard was prepared by the Joint Committee for Medical Device Interoperability, JC 2800. The standard was formally approved by the Joint Committee and the efforts and support of the Joint Committee are gratefully acknowledged.

This standard has been approved by the American National Standards Institute as an American National Standard.

AAMI/UL Joint Committee for Medical Device Interoperability, JC 2800

Name	Representing
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	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	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

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.

No Text on This Page

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.

Annex A
(Informative)

Interoperability Usability Concepts

A1 Overview

A1.1 This section addresses operator interfaces on constituent interoperable items of an interoperable medical system as well as operator interfaces designed to support system level activities. System-level interfaces may be realized on a computer system that provides hosting of system application logic, notions of monitoring and control of constituent interoperable items, and flexible windowing capabilities allow operator interface contents that are tailored to the specific needs of the application logic.

A1.2 The notion of operator interface elements as used in the following recommendations may include common user interface features such as information displays, dialog boxes, input fields, radio buttons, check boxes, etc.

A1.3 Overall goals for supporting operator interactions with an interoperable medical system include the following:

a) G1. The interoperable medical system should provide user interface controls designed to support operator activities necessary to configure, start, monitor, and complete the delivery of a therapy in a correct and timely fashion.

b) G2. The interoperable medical system should provide output designed to support the operator's understanding of the system status in a correct and timely fashion.

c) G3. The interoperable medical system should provide user interface controls that support clinical workflows complying with recommended and best clinical practices for the delivery of a therapy.

A1.4 With interoperable medical systems, use-related risks can be more complicated for the following reasons:

a) R1: Constituent items that were previously designed with one input pathway for data/control (e.g., a medical device front panel) will now likely have at least two input pathways (e.g., the device front panel and interoperability interface)

b) R2: Constituent items that were previously designed with one output pathway for data/control (e.g., a medical device front panel) will now likely have at least two pathways (e.g., the device front panel and interoperability interface).

c) R3: Interoperable medical systems may be constructed from constituents from different manufacturers – those manufacturers may address use hazards somewhat differently, e.g., they may provide (1) different ways of informing the operator about the current state and (2) different controls for operating their respective devices.

Previous approaches developed by manufacturers to inform operators about the state/operation goals for an individual device may be insufficient for informing operators about the aggregate state/operational goals for the interoperable medical system.

d) R4: Interoperable medical systems may have multiple mechanisms for operators to input data/commands to the system or to receive output from the system (e.g., through operator interfaces of multiple constituent interoperable items and/or through the interoperability interfaces of multiple constituent interoperable items).

e) R5: Interoperable medical systems may have consoles designed to aggregate or combine inputs/output for multiple executing clinical functions.

f) R6: To complete a task effectively with the interoperable medical system, the operator may choose to interleave actions across the operator interfaces of multiple constituent interoperable items.

A2 Recommendations

A2.1 This section presents recommendations that address:

a) Usability for constituent interoperable items when integrated into an interoperable medical system,

b) Usability for operator interfaces of the interoperable medical system that control and monitor the state of constituent interoperable items, and

c) Usability of the overall interoperable medical system including interactions and dependences between operator interfaces of constituent interoperable items and operator interfaces provided by the interoperable medical system.

A2.2 In addition to the interoperability-related issues addressed here, operator interfaces provided by the interoperable medical system should comply with usability design principles described in ISO 62366-2:2016 and recommended or best clinical practices.

A2.3 Conditions under which locus of control transfers from system application logic to a constituent interoperable item should be explicitly disclosed and addressed by the risk management process.

NOTE: Such transfers may be necessary to allow an operator to easily stop, modify, and restart the automated processes controlled by system application logic in case of problems or abnormal situations. disclosure may occur in instructions for use, on operator interface of the interoperable medical system or on the operator interface of the relevant constituent interoperable item as justified by risk management.

A2.4 To allow authorized operators to take over control when necessary, the ability to control critical device settings and modes of operation should be available on both the operator interfaces of constituent interoperable items and operator interfaces of the interoperable medical system.

A2.5 Any time a notion of control over the state of one or more constituent interoperable items is expressed by the operator or by a constituent interoperable item, there should be a mechanism for determining if that control command is recognized and the state change is realized in a timely manner.

NOTE: In clinical settings, the user may become distracted by other tasks or interrupted during interactions with the interoperable medical system or constituents. in such situations, operators may only be able to dedicate limited attention to interactions and for brief periods of time.

A2.6 The same operator actions on operator interface controls with similar purposes should produce equivalent effects in conceptually similar situations on both constituent components and interoperable medical system operator interfaces.

A2.7 Information provided by operator interfaces of constituent interoperable items and the interoperable medical system, including responses to operator commands or state changes across the interoperable medical system should not be conflicting with each other.

NOTE: This recommendation aims to prevent use errors due to ambiguous or conflicting information. Basic usability principles require that users understand the feedback provided to them. For interoperable medical systems, these principles should apply across multiple operator interfaces provided by the system or its constituents.

A2.8 Information provided on the operator interfaces of constituent interoperable items should allow the operator to anticipate the consequences of a control action, even when that constituent is under system control. information provided on the operator interfaces of the system should allow the operator to anticipate the consequences of a control action, regardless if the control action is intended to control the aggregate state of the system or the state of specific constituents of the interoperable medical system.

A2.9 Interoperability status information, including the locus of control (e.g., whether a constituent is controlled by the system), status of interoperability connections, important operational modes of constituent interoperable items, and operational health of constituent interoperable items should be available/perceptible on the operator interfaces of both the constituent interoperable items as well as those of the interoperable medical system.

A2.10 Relevant event and state changes (e.g., control actions performed by a system controller) should be prominent and easy to locate on the operator interfaces of both the relevant constituent interoperable items as well as operator interfaces of the interoperable medical system.

A2.11 Foreseeable use errors within the interoperable medical system should be mitigated to acceptable risk levels.

NOTE: Integrating an interoperable item into an interoperable medical system can change its input/output pathways, and hence induce new use errors that should be mitigated. in some cases, interoperable items should be designed in a manner that allows foreseeable use error to be mitigated by system-level control.

A2.12 Realizations of system-level control should provide a mechanism to log operator actions and other system events with sufficient details as to enable post-hoc reconstruction of user actions in forensic analysis of incidents or system failures.

NOTE: This recommendation seeks to enable accurate reconstruction of human-machine interaction to support incident analysis, incident prevention, and forensic investigations.

A2.13 Frequently used controls and critical controls on a constituent interoperable item should require reasonably simple manipulations and reasonably short sequences of actions when the interoperable item is under system control.

A2.14 Feedback for frequent or important events reported on the front panel of a constituent interoperable item should not require observing and understanding multiple information sources when the interoperable item is under system control.

NOTE: This facilitates prompt observation and interpretation of feedback from the constituent interoperable item. sufficient information needed on the operator interface of the interoperable item may need to be obtained from other system constituents.

A2.15 Informational resources (e.g., operator manuals) necessary to understand feedback or to operate a constituent interoperable item when the interoperable item is under system control should be readily available to the operator.

A2.16 The function of operator interface elements that have the same visual appearance (shape, label, etc.) and their relative position in a collection of widgets should be the same on operator interfaces of both constituent interoperable items and the interoperable medical system.

A2.17 There should be a means for constituent interoperable items to prevent or resolve conflicting commands.

NOTE: A constituent interoperable item in an interoperable medical system can receive multiple inputs through different sources, which may be duplicative or in conflict and result in an unsafe condition for the interoperable system.

A2.18 Usability should be managed to ensure that:

a) Critical functionality / primary operating functions (a subset of intended use) of constituent interoperable items and interoperable medical system should be preserved as justified by risk management in the presence of security controls.

b) The interoperable medical system should support emergency override ("Break the Glass") provisioning (i.e., safety considerations override security considerations in certain cases which are rare and exceptional by definition).

Annex B
(Informative)

Security Properties of Interoperable Medical Systems

B1 Security Elements of SSOs

B1.1 Safety and security objectives (SSOs) need to address issues related to operator identity, authentication, and authorization (similarly for patient identity and component identity). This Annex provides additional guidance on Section 5.5 and related concepts in Section 5.3.

B1.2 In the presence of an active adversary, integrity cannot be achieved without authenticity as there is no mechanism built into most/all integrity protection systems that attests to the identity of the data source.

A concrete example is a "classic" man-in-the-middle attack: Data originated by actor Alice to be sent to Bob, which is routed through and altered by actor Mallory, may pass an integrity check when arriving at Bob from Mallory if Mallory falsifies the integrity metadata at the time of data alteration. Integrity guarantees that data has not been changed between Mallory and the destination Bob, but since Mallory was not the original source, the data may have indeed been altered in a potentially unauthorized manner by Mallory. Bob will be unable (by definition) to detect the change using only an integrity control. Authenticity binds the information to its originator Alice in a non-separable way, therefore authenticity can be used as an integrity control, but not vice versa. Integrity does not attest to the original source, and can be used to handle environmental/random corruption in transit or at rest, but is potentially ineffective for intentional corruption.

B1.3 Integrity prevents environmental/random corruption in transit or at rest, omission, or commission errors, which may cause inappropriate actions to be taken, leading to patient harm through improper information used for treatment (data altered before viewed by clinician) or improper treatment administered (command parameters altered).

B1.4 To use the interoperable medical system (with one exception – emergency override ["Break the Glass"]), an actor must make a claim to an identity and prove that claim. The method of authentication is not specified, i.e., it can take any number of forms, e.g., traditional username/password, biometrics, RFID, etc. As an analogy, an identity claim is the username, and the proof of identity is the password, which the system has recorded as tied to that particular username, and therefore someone claiming to have that username must know the password, and prove that knowledge in order for authentication to take place.

B1.5 Authentication is a proof of ownership of an identity, while authorization is the permission for that identity to perform certain actions within the interoperable medical system. To use a particular component or access a piece of information within the interoperable medical system (with one exception – emergency override ["Break the Glass"]), an actor must be explicitly allowed to perform the action requested. This prevents inappropriate actions by actors who may be unqualified, unsuited, or otherwise ineligible to take certain actions, including accessing certain information. (See "Principle of Least Privilege")

B1.6 Auditing is critical for continued improvement in system safety. Authentication metadata ("tags") provide post-facto means to attribute generation and modification of information to a principal for auditing purposes. Authentication metadata of information should be included in the log.

B1.7 While authentication tags provide post-facto means to attribute generation and modification of information to a principal, full provenance records can be used to trace how information was handled and routed (whether modified or not), achieving a cumulative record of the information's custody within the system. Provenance metadata of information should be included in the log.

B1.8 Inappropriate information disclosure is considered, for the purposes of this document, to represent a hazardous situation. Confidentially may indirectly lead to harm. For example, inappropriate disclosure of mental health information may jeopardize the social or employment standing of a patient. (NOTE that "Patient privacy" is an umbrella term, and a complete treatment is out of scope of this Standard.)

B1.9 Safety functions and information should be considered assets from a security perspective. Attack vectors allowing for the alterations of any of these functions and/or information would allow malicious harm. security is meant to mitigate against intentional but unauthorized, or malicious alteration of information or functions of an item or therapy provided by the item. Security deals with many of the same failure modes as safety, but those failure modes may arrive from intelligent actors rather than the environment. Similar to other mitigating controls, in that it may introduce additional risks into the system. Security should be implemented such as to maximize mitigation and minimize additional risk.

B2 Relationship to UL 2900 Series

B2.1 The UL 2900 series of standards address SSOs from the perspective of an individual interoperable items, including single-vendor systems (“Products” when using UL 2900 series terminology) whereas this Standard approaches these issues from the point of view of system-of-systems, focusing on the aspects of SSOs unique to interoperable and vendor-heterogeneous ecosystems.

B2.2 The reference to the UL 2900 series in this Standard is intended to provide guidance for the generation of objective evidence through repeatable and reproducible testing, which would support the assurance case for safe and secure interoperability. The UL 2900 series requires that all interfaces and associated communication channels be defined (excluding hardware side-channels) and that security risk controls such as authentication mechanisms using cryptography and principles of least privilege be applied in a manner consistent with overall product risk management strategies.

B2.3 The UL 2900 series requires that products be evaluated for all known vulnerabilities and exposures in accordance with the National Vulnerability Database (NVD) and International Telecommunications Union (ITU) Cybex Standards (see UL 2900 series for specific references). However, to avoid the danger of significant differences in outcomes, the UL 2900 series attempts to normalize the characterization of risk and associate verification by referring to common vulnerability levels and notions of coverage. Weaknesses must be addressed (eliminated if possible) per the UL 2900 series. Vulnerabilities should be eliminated, but testing for complete elimination may not be possible. The UL 2900 series also requires that all common weakness enumerations be appropriately dispositioned according to the specifications of UL 2900-1 Annex A (e.g., SANS Top 25, SANS On The Cusp, OWASP Top 10, etc.).

B2.4 Where dispositioning involves the determination of manufacturer-specified acceptable risk, additional structured penetration testing is conducted (consistent with methodologies per industry-standard resources such as the Common Attack Pattern Enumeration and Classification database) for verification of the risk management decisions. Structured penetration testing is a “gray box” activity that leverages both the detailed design documents reviewed for security process verification per the UL 2900 series as well as outputs from other testing activities such as Static Source Code Analysis, Static Binary and Bytecode Analysis, Fuzz Testing, required for compliance with the UL 2900 series. The final output of UL 2900 series compliance with respect to this Standard is objective evidence satisfying these standards demonstrating that component-level risk controls (also including single-vendor systems) have been appropriately implemented and are under lifecycle process surveillance consistent with a consensus-based set of requirements for basic cybersecurity hygiene.

Annex C
(Informative)

Clinical Properties of Interoperable Medical Systems

C1 Semantic Interoperability and Nomenclature

C1.1 Overview

C1.1.1 Interoperable medical systems include constituents (often manufactured by different organizations) that exchange data and control information in support of a medical function. Information input into the system comes from a wide variety of digital sources including medical devices, HIT systems (EHRs, health information data bases, mobile medical apps, pharmacy and laboratory systems and software. In many cases, the information exchanged is highly specialized (from both a clinical and technical perspective) and is open to multiple interpretations. The conventional practice is to have each piece of clinical data be accompanied by a "tag" or meta-data that indicates its medical interpretation. The framework of tags used is usually referred to as a "nomenclature" – collections of meta-data tags developed by domain experts, organized according to some taxonomy, whose goal is to help ensure consistent interpretation of medically related data.

C1.1.2 This section addresses data model and nomenclature design, data manipulation/translation, and nomenclature use issues that manufacturers should address to ensure the correct and consistent interpretation of clinical and technical information as it is exchanged between multiple components in interoperable medical systems and between operators and external HIT systems in the interoperable medical system's context. This may help manufacturers address the following issues:

a) Which data elements should have accompanying nomenclature tags?

b) How might the safety concerns for medical service components that generate or make decisions based on medical data differ from infrastructure components that simply store or transfer data?

c) What issues need to be addressed when integrating components that may use different nomenclatures?

d) What are the properties of a nomenclature that make it acceptable for use in interoperable medical components and systems, and how should the component or system's use specification help determine the precision properties that a nomenclature should possess?

e) What issues do platform manufacturers need to address to coordinate proper use of nomenclature in systems built from their platform asset base?

C1.1.3 Despite having the goal of ensuring consistent interpretations, the semantics of nomenclature is imperfect and imprecise due to the many nuances in physiology and medical care. Therefore, it is often difficult to determine whether or not a given selection of nomenclature is appropriate for a particular medical application. At the system level, the risk management process be used to determine the choice of what data to tag and the precision of the nomenclature tags used.

C1.1.4 Recommended informal process:

Interoperable Item Development Activities:

a) The interoperable item specification activity (see the Annex for Stakeholder Activities of AAMI/UL 2800-1) determines whether or not their product generates medical data, makes decisions based on medical data, or presents medical data through an operator interface so that clinicians can make care-giving decisions based on that data. In such cases, the recommendations in this section are applicable. If an interoperable item is an infrastructure component that is agnostic to the data model and nomenclature, the recommendations in this section are not applicable.

b) The interoperable item specification activity discloses, via data models and nomenclature captured in the Information View of their component, the data elements that correspond to medical data. The manufacturer discloses the nomenclature framework to be used for those data elements. The chosen nomenclature should satisfy a minimal set of quality requirements (e.g., one-to-one association of a tag with a semantic interpretation, appropriate design of machine readable versions of nomenclature tags, definitions of nomenclature, completeness of natural language descriptions providing semantic interpretation of the tags).

c) Interoperable item specification activity discloses risk management arguments that justify the selection of nomenclature tags with respect to the interoperable use specification and interoperable application specification for the interoperable item.

d) The interoperable item realization activity provides implementations of data models, nomenclature and operations on data that enable access to the nomenclature tags and that generate and transform data elements whose semantics conforms to their accompanying nomenclature. Tests plans and artifacts are provided to demonstrate these properties.

e) Realizations should use standard nomenclature(s) when possible. If they do not use standard nomenclatures then they should provide the appropriate mapping, and definition.

C1.1.5 Interoperable Item Integration Activities:

a) The interoperable item integration activity selects a canonical nomenclature for the aggregate of interoperable items being integrated. This is typically necessary for safety – it establishes a single base line or reference point for the interpretation of data as it moves through the component assembly.

b) The interoperable item integration activity examines specifications and disclosures of the components being integrated to assess whether or not there is a consistent use of nomenclature across the set of interoperable items to be integrated and whether or not the nomenclature of the components aligns with the selected canonical nomenclature.

c) If there are inconsistencies, risk controls, typically in the form of data model transformations, are designed and implemented to ensure that the indication of semantic interpretation is preserved across the components. Additional risk controls in the form of labeling that may be necessary to alert operators in situations where the integrated components have individual operator interfaces may use different nomenclatures.

d) Validation evidence is produced to determine the correctness of any nomenclature translation.

e) Test plans and results are generated to demonstrate the correctness of the nomenclature manipulation (including any translations) across the assembly.

C1.1.6 Interoperable Medical System Development Activities:

In addition to the issues addressed in interoperable item development activity, the interoperable medical system development activities should address the following:

a) As part of the system-level risk management activities, use of nomenclature as disclosed in the information view of the system is appropriate for the use specification and interoperable application specification of the system.

b) All nomenclature on information flowing into the system through external interfaces or operator interfaces is aligned with the canonical nomenclature chosen for the system.

NOTE: This may be accomplished through data model transformations implemented at the system boundary.

c) All nomenclature on information flowing out of the system through external interoperability interfaces or operator interfaces is aligned with the canonical nomenclature chosen for the system.

d) Use of standards based nomenclatures and information models should be used when possible. It is possible that multiple nomenclatures will be applied.

C1.1.7 Interoperability Framework Activities:

a) A canonical nomenclature scheme to be used within the interoperability framework is specified.

b) When applicable, secondary nomenclatures may be provided, and model may be established between the canonical nomenclature and secondary nomenclatures.

C1.2 Recommendations

C1.2.1 Interoperable item development

C1.2.1.1 The interoperability specification should include a declaration indicating if the interoperable item is the source of medically-related data.

NOTE: If the interoperable item is the source of medically-related data, this triggers additional responsibilities to ensure that appropriate steps are taken to ensure that users of the data (e.g., clients of the interoperable item) have correct interpretation of the data (e.g., through the use of appropriate nomenclature). This reflects an obligation of the interoperable item to its context.

C1.2.1.2 The interoperability specification should include a declaration indicating if the interoperable item utilizes medically-related data as part of its medical function, and if that data may originate outside of the interoperable item boundary.

NOTE 1: Utilization of such data may include display of data on an operator interface to guide operator decision making, or relying on the content of such data to derive the medical function or algorithmic behavior of the component.

NOTE 2: Infrastructure constituents of interoperable medical systems such as communication frameworks may transmit such data without utilizing it to achieve a medical function.

NOTE 3: If the interoperable item utilizes medically-related data, this triggers additional responsibilities to ensure that appropriate steps are taken to ensure that it has a consistent interpretation of the data. This reflects an assumption by the interoperable item that it is relying on the context to implement an external measure that aims to ensure the actors in the context using its interfaces have established a means to achieve consistent interpretation of such data. Item integration activities should establish appropriate controls to ensure that the external measure is enforced.

C1.2.1.3 When the interoperable use specification indicates that the interoperable item is a source of or uses medically related data, it should be ensured that:

a) All transmittal and storage of such data within the interoperable item is associated with nomenclature metadata where the nomenclature and nomenclature association mechanism satisfies the quality attributes C1.2.5 and recommendations on association of data to nomenclature.

b) The use of nomenclature within the interoperable item supports a consistent and unambiguous interpretation of the associated data to a degree justified by the risk management process.

C1.2.1.4 The association mechanism used within the interoperable item shall enable data displayed on operator interfaces to have the human readable representation of the term available for display to a degree justified by the risk management process.

NOTE: The use of nomenclature has little value in supporting real-time display of information unless the operator has access to the nomenclature information.

C1.2.1.5 The nomenclature association mechanism should enable all data provided through interoperability interface shall enable the interoperable item's context to programmatically access the nomenclature associated with the data.

NOTE: The use of nomenclature has little value in supporting consist interpretation of data across interoperability interfaces if system constituents that consume the data cannot access the associated nomenclature information.

C1.2.2 Interoperable item integration

C1.2.2.1 A canonical nomenclature scheme should be specified to ensure a consistent use of nomenclature across all integrated interoperable items.

NOTE: A nomenclature scheme may be the selection of a single nomenclature or a combination of multiple nomenclatures used in a consistent manner.

C1.2.2.2 Controls should be established to ensure that all medical data flowing across the boundary of the enclosing interoperable item has an interpretation aligned with the chosen canonical nomenclature scheme.

C1.2.2.3 Any secondary nomenclatures used by integrated interoperable items and associated mappings between the secondary nomenclature and the canonical nomenclature scheme should be declared.

C1.2.2.4 The interoperable item integration activity should ensure that each integrated interoperable item that utilizes medical data according to its interoperable application specification is receiving that information with the nomenclature indicated by that interoperable item in is use specification.

C1.2.2.5 Any automated nomenclature translation function used to satisfy the recommendations above should be should be subjected to verification to ensure the correctness of the translation.

C1.2.3 Interoperable medical system development

C1.2.3.1 The suitability of the canonical nomenclature scheme for the interoperable medical system with respect to the use and interoperable application specification of the interoperable medical system should be established.

C1.2.3.2 Controls should be established to ensure that any medically related data flowing into the interoperable medical system through an external interface is appropriately associated with the canonical nomenclature scheme of the interoperable medical system before it flows to the medical function of any integrated items of the interoperable medical system.

C1.2.4 Interoperability framework

C1.2.4.1 The interoperability framework should specify a canonical nomenclature scheme and should provide infrastructure for translation to and from this scheme when appropriate.

C1.2.5 Supporting concepts

C1.2.5.1 This section provides recommendations for quality attributes of any nomenclature used within the interoperable item. For each term defined in a nomenclature, the nomenclature specification should include the following:

a) A human readable representation of the term;

b) A machine readable representation; and

c) A definition of the term suitable for communicating with operators.

NOTE: The essence of the contents of a nomenclature and identifies the basic entities needed to establish the desired relationship between machine readable meta-data providing ontological categories and human interpretation of those categories.

C1.2.5.2 The provenance of the nomenclature and the process used to validate of the human readable representation and description of the meaning of the term should be documented.

NOTE: Designing a good nomenclature (whose goal is to establish common interpretation of data across stakeholders) typically requires extensive collaboration and consensus building across stakeholders. In addition, it should be argued that users of the nomenclature will find the nomenclature acceptable. The guidance above asks manufacturers to indicate the degree to which the nomenclature used in their product has be constructed and validated in an appropriate multi-stakeholder consensus-building process.

C1.2.5.3 For each term defined in the nomenclature, the nomenclature design should ensure that there is a 1-to-1 correspondence between the human-readable representation of the term and the machine-readable representation of the term.

NOTE: Failure to achieve this property will introduce ambiguity in the nomenclature, which in turn will lead to potential safety problems.

C1.2.5.4 For each term defined in the nomenclature, the nomenclature design should ensure that the meaning of the term describes a concept that is unique with respect to the rest of the nomenclature or is explicitly designed and documented to be a refinement or specialization of other terms in the nomenclature.

NOTE: Failure to achieve this property will introduce ambiguity in the nomenclature, which in turn will lead to potential safety problems.

C2 Patient Identity and Association

C2.1 Overview

C2.1.1 This section contains recommendations that relate to identification of patients and linking of patient identity to medical data – in order to assure that the correct patient receives the correct treatment; and that the patient data is tied to the correct patient. Important concepts here also include the notion of associating interoperable items to a patient, the notion of disassociating the interoperable items to a patient, and the notion of a patient episode (which may roughly be understood as the time/activities between patient association and disassociation).

C2.2 Recommendations

C2.2.1 Interoperable item development activities

C2.2.1.1 The information view of the interoperable item should include declaration of whether or not its medical function includes the use of patient identity information for each of the following purposes:

a) Display of patient identity to an operator.

b) Use of patient identity information to create information that may be transferred outside of the interoperable item boundary.

c) Use of patient identity information to determine or influence the medical function of the interoperable item.

d) Storage of patient identity information within the state of the interoperable item.

NOTE: This is typically necessary to determine which recommendations for patient identity should apply to the interoperable item. some interoperable items (e.g., network infrastructure) are agnostic to the purpose of data that receive or transmit. This may lead to a determination of when the other recommendations of this section may apply.

C2.2.1.2 The information view of the interoperable item should include a declaration of whether or not its technical function may support communication of patient identity information, including identity information linked to medical data.

NOTE: This is typically necessary to determine if confidentiality objectives may apply to the interoperable item.

C2.2.1.3 The information view of the interoperable item should include a declaration that indicates if patient identity information is neither used nor communicated by the interoperable item.

C2.2.1.4 If the interoperable item uses the patient identity information in support of medical function as indicated above, the information view should have a declaration of content, nomenclature, usage and data format of patient identity information.

NOTE: This is the information that needs to be interpreted consistently across all interoperable items in the interoperable medical system. Thus, the information needs to be declared and disclosed to ensure consistent interpretation and usage.

C2.2.1.5 If the interoperable item uses the patient identity information in support of a medical function as indicated above, the computational view should indicate each of interactions of the interoperable item's interoperable interface that operates on patient identity information as part of its medical function.

NOTE: This information is used to establish risk controls regarding security properties of patient identity information (e.g., each point where the information is communicated outside of the interoperable item should require an analysis to determine if communication over that interaction point appropriately safeguards the information).

C2.2.1.6 If the interoperable item transfers or stores the patient identity information in support of technical function, the computational view should indicate:

a) Each interaction on the interoperability interface that transmits patient identity information as part of its technical function; and

b) Each flow path of patient identity information through the interoperable item.

NOTE: This information is used to establish risk controls regarding security properties of patient identity information when information is simply communicated. This would pertain primarily to the privacy and integrity of the patient ID information.

Additional issues to consider may include:

c) Declaration of the information fields use to establish patient identity (or better yet, definition of a patient identifier)

d) Maintenance of the integrity of those fields across all constituents of the interoperable item

e) Declarations of any translations between representations of patient identity information

f) Disclosure of the information used to establish patient identity

g) Uniqueness properties of patient identity information

C2.2.1.7 The interoperable use specification should document the following states:

a) Not associated with a patient (describe characteristics, conditions that must be met to be said to be in that state, indications visible via network interface when in that state); and

b) Associated with a patient (describe characteristics, conditions that must be met to be said to be in that state, indications visible to operator on device when in that state, indications visible via network interface when in that state).

C2.2.1.8 The interoperable item interoperable use specification should document how the following activities are reflected in its interoperability-exposed functions:

a) Transitioning the interoperable item from a non-patient associated state to a patient associated state (with pre-conditions, post-conditions); and

b) Transitioning the interoperable item from a patient associated state to a patient non-associated state (with pre-conditions, post-conditions)

C2.2.1.9 The notion of a patient episode for the interoperable item that reflects the association of the interoperable item to the patient should be expressed in terms of the transitions described above.

C2.2.1.10 The medical functions of the interoperable item should only be invoked once the patient episode has been established.

NOTE: This ensures that patient identity information necessary to link medical data to patient identity is present during the medical function of the interoperable item.

C2.2.1.11 The medical functions of the interoperable item directed to a particular patient under care should not continue past the end of the patient episode.

C2.2.1.12 After the end of the patient episode, no patient identity information should exist in the interoperable item unless properly controlled.

C2.2.2 Interoperable medical system development activities

C2.2.2.1 While an interoperable medical system is supporting care-giving for a patient, all constituents of interoperable medical systems that have a patient identity storage capability should hold an identifier corresponding to organization's patient identifier for the patient under care.

C2.2.2.2 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.

C2.2.2.3 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 constituents except for (a) forensic information that is the subject of confidentiality risk management or (b) data held in storage designed as a patient information system that is the subject of appropriate controls.

C2.2.2.4 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.

C2.2.2.5 The instructions for use of the interoperable medical system should 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.

C3 Operator Identification, Authentication, and Authorization

C3.1 Overview

C3.1.1 Deployment of security solutions must consider operations and safety of the interoperable medical system. Security implementation that hinders operation tend to be circumvented by the operators, making them ineffective. Security controls that frequently generate false-positive security alerts, require repeated user authentication or prevent the operator from operating in the expected manner impede clinical care and could be a patient safety issue. Security capabilities must be efficient, accurate and provide demonstrable value. The interoperable medical system security should rely on automation as much as possible, but people must be able to interact with the security implementation to monitor status, review analytics, make decisions when needed and plan modifications and improvements.

Issues below should be considered in each of the indicated activities (See the Annex for Stakeholder Activities of AAMI/UL 2800-1) as approaches to managing risk concerns and achieving the SSOs of Section 5.2.3.

C3.2 Recommendations

C3.2.1 Interoperable item development

C3.2.1.1 The risk assessment and threat modeling of the interoperable item may include the concept of an operator/user.

NOTE: The actions of an operator impact patient safety and confidentiality of the patient's information. Therefore, the possibility of a malicious operator or an operator not medically qualified to perform actions via the system need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. In addition, Attribution and accountability properties needed to support forensic analysis also require tracking of operator identities.

C3.2.1.2 The extent to which the interoperable item may consume, record, implement, and enforce the operator identity should be disclosed and verified.

NOTE: The interoperable item should either receive operator identity and operator authentication and operator authorization information through its own interface, authenticating and authorizing the operator with the rest of the interoperable medical system, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system.

C3.2.1.3 The extent to which the interoperable item may consume, record, implement, and enforce an operating organization's policy of operator privilege/authorization (e.g. RBAC) separation should be disclosed.

NOTE: Not all interoperable items may provide support for operator identity, authentication, and authorization, so these notions may vary across different interoperable items within the interoperable medical system. This guidance asks manufacturers to disclose the extent to which their interoperable item is designed to support enforcement of separation of role/privilege which comes with operator authorization, and consequently whether (and to what extent) the rest of the interoperable medical system and other interoperable items should perform these duties instead. If the interoperable item is intended to provide support for these notions, the manufacturer needs to comply with the rest of the enforcement-related supporting requirements for operator authorization.

C3.2.1.4 Every operator within the interoperable medical system should be authenticated with the system before being allowed to interact with a constituent interoperable item. Utility with respect to patient safety should be considered as part of the selection of the authentication mechanism (and levels) and accounted for in risk management.

NOTE: The term "login" is essentially synonymous with authentication.

C3.2.1.5 Authentication algorithms, methods, and protocol implementations should be disclosed and verified. Any deviation from interoperability framework supported algorithms, methods, and protocols should be disclosed along with the risk management ramifications. If no authentication is supported, this should be disclosed along with the risk management ramifications.

NOTE: A particular method for authentication is not mandated. However, since authentication is a risk control the ability to of the chosen mechanism to achieve the control should be addressed in the assurance arguments.

C3.2.1.6 If the interoperable item receives operator identity and operator authentication information over its own user interface, the means, method, and implementation of operator identification and operator authentication should be disclosed and verified, and the next recommendation should apply.

NOTE: The interoperable item should either receive operator identity and operator authentication and operator authorization information through its own user interface, authenticating and authorizing the operator with the rest of the interoperable medical system, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system. It may only serve as a "pass-through" for this information, but this should be disclosed and the safety of the resulting protocol verified as well.

C3.2.1.7 Interoperable items should enforce operator separation of privilege policy based on operator authorization credentials in the interoperable medical system.

NOTE 1: The separation of privilege policy may be stated in terms of user roles.

NOTE 2: Authorization concepts such as role-based access control may be used to enforce a separation of privilege policy.

NOTE 3: Even though the manufacturer may have no knowledge of the particular operator privilege policy of the operating organization, the risk management activities for the interoperable medical system should include an analysis the criticality/vulnerability of operator interactions with the system with respect to the system's medical function. Based on this analysis, the interoperable medical system manufacturer can recommend appropriate access policies based on a general understanding of care-giving roles in the medical domain in general. Asking the manufacturer to carry out this activity prevents the operating organization from having to "start from scratch" (e.g., to perform a detailed criticality and risk analysis of the system/operator interactions) when configuring the system to organization operator privilege policy.

C3.2.1.8 Failure modes and the operator separation of privilege policy to be adopted/enforced in different modes, such as operator-based and time-based, should be identified/disclosed.

NOTE: This is intended to address scenarios such as emergency override ("Break the Glass").

C3.2.1.9 If the interoperable item is carrying out the task of operator identification and operator authentication, but the interoperable item is not intended as the responsible logical component for operator authentication within the interoperable medical system, the algorithms, methods, protocols, and implementation for delegating operator authentication to the responsible component in the interoperable medical system should be disclosed and verified, and the rest of this guidelines does not apply. If, however, the interoperable item serves as the responsible agent for operator authentication in the interoperable medical system, the algorithms, methods, protocols, and implementation for operator identity and operator authentication should be disclosed and verified. The interoperable item should then perform or delegate operator authorization, and the next recommendation should apply.

NOTE: The interoperable item should either receive operator identity and operator authentication and operator authorization information through its own interface, authenticating and authorizing the operator with the rest of the interoperable medical system, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system.

C3.2.1.10 The interoperable item intended as the responsible agent for operator authentication in the interoperable medical system should perform or delegate operator authorization. If the component has direct access to the authorization control policy as specified by the operating facility, the means, methods, protocols, and implementation for performing operator authorization and communicating the results of operator authorization to other components in the interoperable medical system should be disclosed and verified, and the rest of this requirement does not apply. If operator authorization is delegated, the methods, protocols, and implementation for communicating the authorization database/entity (which may or may not be a constituent of interoperable medical system) should be disclosed and verified, and the means, methods, protocols, and implementation of communicating the operator authorization results to other components in the interoperable medical system should be disclosed and verified.

NOTE: The component should either receive operator identity and operator authentication and operator authorization information through its own interface, authenticating and authorizing the operator with the rest of the interoperable medical system, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system.

C3.2.1.11 An interoperable item may request the interoperable medical system to re-authenticate and re-authorize the operator.

NOTE: Operator may change during network outage. If operator identity fails verification, the operator should be automatically logged out or restricted access to certain functionality. Specific clinical application logic may allow only specific roles to complete tasks and require re-authorization of the user. The consequences of failure of authentication and authorization should take patient safety into consideration.

C3.2.1.12 If the interoperable item receives operator identity and operator authentication information over its own user interface, the component should have a process for an operator to manually log out of the interoperable medical system.

NOTE: The system needs to be protected from unauthorized access when an operator is not physically present or currently interacting with the system (e.g., avoid the system being used by an unauthorized party when the system has recently been used by an authorized user). This mechanism allows operators to manually indicate when they are no longer viewing information from, or interacting with, the system. This addresses both confidentiality of data and control of unauthorized actions.

C3.2.2 Interoperable item integration

C3.2.2.1 The communication protocols of the interoperable medical system should facilitate authenticated communication of operator identity, operator authentication status, and operator authorization status between interoperable items.

NOTE: The actions of an operator impact patient safety and confidentiality of the patient's information. Therefore, the possibility of a malicious operator or an operator not medically qualified to perform actions via the interoperable medical system need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. Since not all individual interoperable items may support operator log-in/authentication, an inter-item communication facility for this information should be in place.

C3.2.2.2 The interoperable item(s) within the interoperable medical system that do not provide complete support for services that consume, record, implement, and enforce an operating organization's policy of operator privilege/authorization (e.g. RBAC) separation should be integrated such that another component performs that function on behalf of the non-supporting interoperable item. The responsibility delegation relationship should be disclosed.

NOTE 1: Not all interoperable items may provide support for operator identity, authentication, and authorization. If an interoperable item does not provide support for these notions, another interoperable item within the interoperable medical system should perform these duties on behalf of the non-supporting interoperable item. Identification of these types of interoperable items should be disclosed to ensure that integration has not occurred such that some interoperable items neither enforce privilege separation nor delegate that function to another responsible interoperable items. This helps reason about the safety and security properties of the overall system, even when not all interoperable items implement all safety/security services themselves.

NOTE 2: The intention is to specify who/what does the reporting, and not that the reporting should be done, which needs to be a separate requirement. This type of information is needed to support forensic analysis of operators present, operator accountability, and security monitoring.

C3.2.2.3 The system integrator should disclose the alignment of the deployed system with the system manufacturer's recommended separation of privilege policy for the interoperable medical system and its constituent components and justify any misalignment through a risk management process.

NOTE 1: The separation of privilege policy may be stated in terms of defined user roles.

NOTE 2: Authorization concepts such as role-based access control may be used to enforce a separation of privilege policy.

NOTE 3: Even though the manufacturer may have no knowledge of the particular operator privilege policy of the operating organization, the risk management activities for the system should include an analysis the criticality/vulnerability of operator interactions with the system with respect to the system's medical function. Based on this analysis, the system manufacturer can recommend appropriate access policies based on a general understanding of care-giving roles in the medical domain in general. Asking the manufacturer to carry out this activity prevents the operating organization from having to "start from scratch" (e.g., to perform a detailed criticality and risk analysis of the system/operator interactions) when configuring the system to organization operator privilege policy.

C3.2.3 Interoperable medical system development

C3.2.3.1 The risk assessment and threat modeling of the interoperable medical system should include the concept of an operator/user. The current operator identity should be communicated to all system components.

NOTE: The actions of an operator impact patient safety and confidentiality of the patient's information. Since not all individual components may support operator log-in/authentication, an inter-component communication system for this information should be in place. To allow for heterogeneous interoperable items to exchange this information in a consistent, interoperable way, the protocols and data formats for this should be defined at the ecosystem level and implemented at the interoperable system development level.

C3.2.3.2 Every operator that interacts with the interoperable medical system (any of its constituent components) should have a persistent unique operator identity within the scope of the system. The identity may be globally unique.

NOTE: Uniqueness of identity within the system (in relation to the facility where the system is deployed) is necessary to support authorization as well as attribution. Current random key generation technology can support generation of identifiers that are guaranteed to be unique up to a value that is acceptable per the risk management process. While this requirement does not mandate

the use of specific techniques nor specify the “level” or scope of uniqueness (e.g. per-facility, globally, etc.), it recognizes the effectiveness of those techniques. The optional nature of the second sentence of the requirements enable compliance when the system uses identity management of the organization, which may not achieve the global uniqueness property. Truly globally unique identities would facilitate transition of this information across facilities and allow multi-facility attribution and accountability during forensic analysis or auditing.

C3.2.3.3 If only one potential generation and representation of the operator identity is supported by an interoperability framework, its implementation should be verified and the responsible interoperable item should be disclosed. If multiple options are available, their methods, algorithms, and implementations should be disclosed and verified and the responsible interoperable item should be disclosed.

NOTE: A particular method for generating identifiers is not mandated. however, the ability to achieve the uniqueness properties of identification should be addressed in the assurance arguments.

C3.2.3.4 Every operator within the interoperable medical system (any of its constituent interoperable items) should authenticate with the system before being allowed to perform any interactions. Utility with respect to patient safety should be considered as part of the selection of the authentication mechanism (and levels) and accounted for in risk management.

NOTE: The term “login” is essentially synonymous with authentication.

C3.2.3.5 If only one potential authentication method/protocol is supported by an interoperability framework, its implementation should be verified and the responsible component should be disclosed. If multiple options are available, their methods, algorithms, and implementations should be disclosed and verified and the responsible interoperable item within the interoperability architecture should be disclosed.

C3.2.3.6 The interoperable medical system should have the ability to re-authenticate and re-authorize the operator. This may occur at the system level, or at the request of a component.

NOTE: Operator may change during network outage. If operator identity fails verification, the operator will be automatically logged out or restricted access to certain functionality. Specific clinical apps may allow only specific roles to complete tasks and require re-authorization of the user. The consequences of failure of authentication and authorization should take patient safety into consideration.

C3.2.3.7 The interoperable medical system should have a process for an operator to manually log out of the interoperable medical system. Upon logout, the operator should lose their authenticated status with respect to the system and its components. And this event should be communicated to all components using the same protocols used to facilitate authenticated communication of operator identity between components (earlier requirement).

NOTE: The system needs to be protected from unauthorized access when an operator is not physically present or currently interacting with the system (e.g., avoid the system being used by an unauthorized party when the system has recently been used by an authorized user). This mechanism allows operators to manually indicate when they are no longer viewing information from, or interacting with, the system. This addresses both confidentiality of data and control of unauthorized actions.

C3.2.3.8 The interoperable medical system should automatically log out the operator(s) after a certain period of inactivity. The length of the inactivity period should be defined as part of the selection of the authentication mechanism and accounted for in risk management. The following points should be considered as part of determining the inactivity period leading to logout:

a) Patient safety;

b) Operating environment (whether intended or reasonably foreseeable) including accessibility by unauthorized parties;

c) Potential mobility of the system; and

d) Operator workflows.

NOTE: This requirement has similar motivations to the previous one, but addresses situations where an operator may forgets to manually logout. The designation of an appropriate timeout time should take into account patient safety considerations.

C3.2.3.9 Where a password is used as a part of the operator authentication process, the interoperable medical system should require a change in password periodically at intervals consistent with use environment policies/requirements.

NOTE: The requirement is necessary to achieve effectiveness of password-based access controls to the interoperable medical system.

C3.2.3.10 The constituent interoperable items of the interoperable medical system should have all factory-set default Operator authentication information changed before initial deployment and use (as part of installation/integration).

C3.2.3.11 The extent to which the interoperable medical system (and which constituent component(s)) provides supporting services that consume, record, implement, and enforce an operating organization's policy of operator privilege/authorization (e.g. RBAC) separation should be disclosed.

NOTE: Not all components may provide support for operator identity, authentication, and authorization. In some cases, due to the variability of the system instances that conform to the system reference architecture, the capabilities of components to support these notions may vary across different instances of the system. This requirement asks manufacturers to disclose the extent to which the system is designed to support operator identification and separation of privilege. If a component does not provide support for these notions, another component within the interoperable medical system should perform these duties on behalf of the non-supporting component. That component should be disclosed to help reason about the safety and security properties of the overall system, even when not all components implement all safety/security services themselves.

C3.2.3.12 The interoperable items responsible for operator identification, operator authentication, and operator authorization should be identified.

NOTE: This helps reason about the safety and security properties of the overall system, even when not all components implement all safety/security services themselves. It provides a simple "sanity check" to see if any component required for safety and security may have been omitted during integration, or not configured to perform its proper function.

C3.2.3.13 The interoperable medical system should have the ability to enforce separation of operator privileges in terms of which actions are allowed for each operator at what time (mode-based, operator-based, and time-based limitations).

NOTE: Access to the interoperable medical system clinical, administrative, and service functions should be inaccessible without operator authentication (e.g., login) followed by authorization in order to protect sensitive information from unauthorized access.

C3.2.3.14 The interoperable medical system should have the ability to enforce limitations on which information can be accessed by each actor (interoperable item or operator) at what time (mode-based, operator-based, and time-based limitations).

NOTE: The interoperable medical system should support confidentiality objectives for patient data.

C3.2.3.15 Failure modes and the operator separation of privilege policy to be adopted/enforced in different modes, such as operator-based and time-based, should be identified/disclosed.

NOTE: This is also intended to address other scenarios such as emergency override ("Break the Glass").

C3.2.3.16 The system manufacturer should disclose a recommended separation of privilege policy for the interoperable medical system and its constituent components justified by risk management.

NOTE 1: The separation of privilege policy may be stated in terms of user roles.

NOTE 2: Authorization concepts such as role-based access control may be used to enforce a separation of privilege policy.

NOTE 3: Even though the manufacturer may have no knowledge of the particular operator privilege policy of the operating organization, the risk management activities for the system should include an analysis the criticality/vulnerability of operator interactions with the system with respect to the system's medical function. Based on this analysis, the system manufacturer can recommend appropriate access policies based on a general understanding of care-giving roles in the medical domain in general. Asking the manufacturer to carry out this activity prevents the operating organization from having to "start from scratch" (e.g., to perform a detailed criticality and risk analysis of the system/operator interactions) when configuring the system to organization operator privilege policy.

C3.2.3.17 The interoperable medical system should report all (both successful and unsuccessful) operator authentication, operator authorization, disconnect/logout, and role changing events to the data logger and security monitoring.

C3.2.4 Interoperability framework

C3.2.4.1 If only one potential authentication method/protocol is supported by an interoperability framework, its implementation should be verified and the responsible interoperable item should be disclosed. If multiple options are available, all supported options, their methods, algorithms, protocols, and implementations within an individual component should be disclosed and verified.

C3.2.4.2 The interoperability framework should include the concept of a persistent and unique operator identity, and associated data representation and communication protocols (potentially more than one, selectable at system instantiation or system integration) to facilitate their communication of operator identity between components.

NOTE: The actions of an operator impact patient safety and confidentiality of the patient's information. Therefore, the possibility of a malicious operator or an operator not medically qualified to perform actions via the system need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. Component agreement as to the operator identity will support many other requirements such as operator authentication, operator authorization, and attribution. Uniqueness of identity within the system can be in global or in relation to specific organizations (e.g., facilities) or even individual system deployments. Higher levels of uniqueness allow for greater support for attribution and more effective forensic investigation and auditing.

C3.2.4.3 If only one potential generation and representation of the operator identity is supported by an interoperability framework, it should be disclosed and verified. If multiple options are available, they should be disclosed.

NOTE: A particular method for generating identifiers is not mandated. However, the ability to achieve the uniqueness properties of identification should be addressed in the assurance arguments.

C3.2.4.4 The interoperability framework should support mandatory operator authentication prior to allowing interaction with the interoperable medical system (any of its constituent items). If multiple algorithm and/or protocol options are available, they should be disclosed.

NOTE: The term "login" is essentially synonymous with authentication.

C3.2.4.5 If multiple algorithm and/or protocol options for operator authentication are available, they should be disclosed.

NOTE: A particular method for authentication is not mandated. However, since authentication is a risk control the ability to of the chosen mechanism to achieve the control should be addressed in the assurance arguments.

C3.2.4.6 The communication protocols of the interoperability framework should support authenticated communication of operator identity and operator authorization status (credentials) between constituent interoperable items.

NOTE: Not all individual components may support operator log-in/authentication, an inter-component communication system for this information should be in place. To allow for heterogeneous components to exchange this information in a consistent, interoperable way, the protocols and data formats for this should be defined at the ecosystem level and implemented at the interoperable system development level.

C3.2.4.7 Authorization control policy languages / databases / file formats supported by the interoperability framework should be disclosed.

NOTE: Not all interoperable systems and subcomponents may provide support for operator identity, authentication, and authorization. In some cases, due to the variability of the system instances that conform to the system reference architecture, the capabilities of components to support these notions may vary across different instances of the system. This requirement asks manufacturers to disclose the extent to which the system is designed to support operator identification and separation of privilege. If the system is intended to provide support for these notions, the manufacturer needs to comply with the rest of the requirements in this section. Otherwise the requirements do not apply.

C3.2.4.8 Failure modes and the operator separation of privilege policy to be adopted/enforced in different modes, such as operator-based and time-based, should be identified/disclosed.

NOTE: This is intended to accommodate scenarios such as emergency override (“Break the Glass”).

C4 Item Identification, Authentication, and Authorization

C4.1 Recommendations

C4.1.1 Interoperable item development activities

C4.1.1.1 The risk assessment and threat modeling of the interoperable item should include the concept of interactions with other interoperable items within an interoperable medical system.

NOTE: Information exchanged with other interoperable items impact patient safety and confidentiality of the patient’s information. Therefore, the possibility of a connected malicious interoperable item or an interoperable item performing a task not within its intended use need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. In addition, attribution and accountability properties needed to support forensic analysis also require tracking of item and the source and destination of information used and produced by the item.

C4.1.1.2 The risk assessment and threat modeling of the interoperable item should include the concept of interoperable item actions as initiated by and its direct or indirect operator/user.

NOTE: (See note above). In addition, attribution and accountability properties needed to support forensic analysis also require tracking of item and item direct or indirect operator/user identities.

C4.1.1.3 The extent to which the interoperable item may consume, record, implement, and enforce the operator identity should be disclosed and verified.

NOTE: The interoperable item should either receive operator identity and operator authentication and operator authorization information through its own interface, authenticating and authorizing the operator with the rest of the interoperable medical system, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system.

C4.1.1.4 The extent to which the interoperable item may consume, record, implement, and enforce the interoperable item identity of other interoperable items with which it exchanges information should be disclosed and verified.

NOTE: The interoperable item should either receive item identity and item authentication and item authorization information which it has been provisioned to independently verify, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system.

C4.1.1.5 The extent to which the interoperable item may consume, record, implement, and enforce an operating organization’s policy of operator privilege/authorization (e.g. RBAC) separation should be disclosed.

NOTE: Not all interoperable items may provide support for operator identity, authentication, and authorization, so these notions may vary across different items within the interoperable medical system. This requirement asks manufacturers to disclose the extent to which their component is designed to support enforcement of separation of role/privilege which comes with operator authorization, and consequently whether (and to what extent) the rest of the interoperable medical system and other items should perform these duties instead. If the item is intended to provide support for these notions, the manufacturer needs to comply with the rest of the enforcement-related supporting requirements for operator authorization. Otherwise only this requirement applies.

C4.1.1.6 The extent to which the interoperable item may consume and comply with an operating organization’s policy of item privilege/authorization (e.g. RBAC) separation should be disclosed.

C4.1.1.7 Every interoperable item within the interoperable medical system should be authenticated with the system before being allowed to interact with a constituent interoperable item. Utility with respect to patient safety should be considered as part of the selection of the authentication mechanism (and levels) and accounted for in risk management.

C4.1.1.8 The interoperable item should be capable of receiving and consuming item identity and item authentication information with respect to other interoperable items in the interoperable medical system over its machine-to-machine (interoperability) interface, and the means, method, and implementation of item identification and item authentication should be disclosed and verified.

C4.1.1.9 Authentication algorithms, methods, and protocol implementations should be disclosed and verified. Any deviation from standard ecosystem supported algorithms, methods, and protocols should be disclosed along with the risk management ramifications.

NOTE: While the existence of an authentication capability is required, no particular method for authentication is mandated. However, since authentication is a risk control the ability to of the chosen mechanism to achieve the control should be addressed in the assurance arguments.

C4.1.1.10 If the interoperable item receives operator identity and operator authentication information over its own user interface, the means, method, and implementation of operator identification and operator authentication should be disclosed and verified, and the next requirement should apply.

NOTE: The item should either receive operator identity and operator authentication and operator authorization information through its own interface, Authenticating and authorizing the operator with the rest of the interoperable medical system, or it should implement a synchronization mechanism and protocols to receive this information from the rest of the interoperable medical system. It may only serve as a “pass-through” for this information, but this should be disclosed and the safety of the resulting protocol verified as well.

C4.1.1.11 Interoperable items should enforce sibling interoperable item's privilege based on interoperable item authorization credentials and facility policy in the interoperable medical system.

NOTE 1: The separation of privilege policy may be stated in terms of user roles.

NOTE 2: Authorization concepts such as role-based access control may be used to enforce a separation of privilege policy.

NOTE 3: Even though the manufacturer may have no knowledge of the particular network privilege policy of the operating organization, the risk management activities for the system should include an analysis the criticality/vulnerability of interoperable item interactions with the system with respect to the system's medical function. based on this analysis, the system manufacturer can recommend appropriate access policies based on a general understanding of the interoperable item’s intended use within the interoperable medical system and care-giving roles in the medical domain in general. Asking the manufacturer to carry out this activity prevents the operating organization from having to “start from scratch” (e.g., to perform a detailed criticality and risk analysis of the system/item/operator interactions) when configuring the system to organization network privilege policy.

C4.1.1.12 An interoperable item may request the interoperable medical system to re-authenticate and re-authorize another item.

NOTE: Interoperable items may change (e.g. be swapped out) during network outage. If item authentication fails, the interoperable item will be automatically restricted in its use of certain network services, QoS, etc. The consequences of failure of authentication and authorization should take patient safety into consideration.

C4.1.2 Interoperable item integration activities

C4.1.2.1 The communication protocols used in integrating interoperable items should facilitate authenticated communication of operator identity, operator authentication status, and operator authorization status between interoperable items.

NOTE: The actions of an operator impact patient safety and confidentiality of the patient’s information. Therefore, the possibility of a malicious operator or an operator not medically qualified to perform actions via the system need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. Since not all individual items may support operator log-in/authentication, an inter-component communication system for this information should be in place.

C4.1.2.2 The communication protocols used in integrating interoperable items should facilitate authenticated communication of interoperable item identity, interoperable item authentication status, and interoperable item authorization status between interoperable items.

NOTE: The actions of an interoperable item impact patient safety and confidentiality of the patient’s information. Therefore, the possibility of a malicious item or an item with insufficient/inappropriate capabilities to perform actions via the system need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. This requirement

serves to cross-check suitability of the item for the assigned task(s) and prevent items of unknown authenticity/provenance from being integrated into the interoperable medical system.

C4.1.3 Interoperable medical system development activities

C4.1.3.1 The risk assessment and threat modeling of the item designed for use in an interoperable medical system should include the concept of other interoperable items within the interoperable medical system.

NOTE: The actions of an item impact patient safety and confidentiality of the patient's information. To allow for heterogeneous components to exchange this information in a consistent, Interoperable way, the protocols and data formats for this should be defined at the ecosystem level and implemented at the interoperable system development level.

C4.1.3.2 The risk assessment and threat modeling of the item designed for use in an interoperable medical system should include the concept of an item and its direct or indirect operator/user. The current operator identity should be communicated to all other items.

NOTE: The actions of an item impact patient safety and confidentiality of the patient's information. Therefore, the possibility of a malicious Item or an Item performing a task not within its intended use need to be considered in risk assessment, and appropriate risk controls need to be designed to prevent associated harms. To allow for heterogeneous components to exchange this information in a consistent, interoperable way, the protocols and data formats for this should be defined at the ecosystem level and implemented at the interoperable medical system development level.

C4.1.3.3 Every item that interacts with the interoperable medical system (any of its other items) should have a persistent unique item identity within the scope of the system. The identity may be globally unique.

NOTE: Uniqueness of identity within the system (in relation to the facility where the system is deployed) is necessary to support authorization as well as attribution. Current random key generation technology can support generation of identifiers that are guaranteed to be unique up to a value that is acceptable per the risk management process. while this requirement does not mandate the use of specific techniques nor specify the "level" or scope of uniqueness (e.g. per-facility, globally, etc.), it recognizes the effectiveness of those techniques. The optional nature of the second sentence of the requirements enable compliance when the system uses organization-specific provisioning and credential management, which may not achieve the global uniqueness property. Truly globally unique identities would facilitate transition of this information across facilities and allow multi-facility attribution and accountability during forensic analysis or auditing.

C4.1.3.4 If only one potential representation of the interoperable item identity is supported by an ecosystem, its implementation should be verified. If multiple options are available, their methods, algorithms, and implementations should be disclosed and verified.

NOTE: A particular method for generating identifiers is not mandated. However, the ability to achieve the uniqueness properties of identification should be addressed in the assurance arguments.

C4.1.3.5 Every interoperable item within the interoperable medical system) should authenticate with the system before being allowed to perform any interactions with other interoperable items. Utility with respect to patient safety should be considered as part of the selection of the authentication mechanism (and levels) and accounted for in risk management.

C4.1.3.6 The interoperable items within the interoperable medical system that do not provide complete support for services that consume, record, implement, and enforce an operating organization's policy of operator privilege/authorization (e.g. RBAC) separation should be integrated such that another component performs that function on behalf of the non-supporting item. The responsibility delegation relationship should be disclosed.

NOTE: This dependence relationship should be disclosed to ensure that integration has not occurred such that some items neither enforce privilege separation nor delegate that function to another responsible item. This helps reason about the safety and security properties of the overall system, even when not all items implement all safety/security services themselves.

C4.1.3.7 The interoperable items within the interoperable medical system that do not provide complete support for services that consume and enforce an operating organization's policy of network privilege (e.g. QoS) separation should be integrated such that another component performs that function on behalf of the non-supporting item. The responsibility delegation relationship should be disclosed.

NOTE: This dependence relationship should be disclosed to ensure that integration has not occurred such that some items neither enforce privilege separation nor delegate that function to another responsible item. This helps reason about the safety and security properties of the overall system, even when not all items implement all safety/security services themselves.

C4.1.3.8 Interoperable medical system should report all (both successful and unsuccessful) item authentication, item authorization, and role changing events to the data logger and security monitoring.

NOTE 1: The intention is to specify who/what does the reporting, and not that the reporting should be done, which needs to be a separate requirement.

NOTE 2: This type of information is required to support forensic analysis of operators present, operator accountability, and security monitoring.

C4.1.3.9 The interoperable medical system should have the ability to re-authenticate and re-authorize the item. This may occur at the system level, or at the request of another item.

NOTE: Items may change (e.g. be swapped out) during network outage. If item authentication fails, the item will be automatically restricted in its use of certain network services, QoS, etc. The consequences of failure of authentication and authorization should take patient safety into consideration.

C4.1.3.10 The interoperable medical system should automatically revoke the access credentials of an item after a certain period of inactivity. The length of the inactivity period should be defined as part of the selection of the authentication mechanism and accounted for in risk management. The following points should be considered as part of determining the inactivity period leading to logout:

a) Patient safety;

b) Operating environment (whether intended or reasonably foreseeable) including accessibility by unauthorized parties;

c) Potential mobility of the system; and

d) Operator workflows.

NOTE: This requirement prevents potentially failed or removed items from maintaining active credentials – an important safety and SECURITY “sanity check”. The designation of an appropriate timeout time should take into account patient safety considerations.

C4.1.3.11 The interoperable items of the interoperable medical system should have all factory-set unique authentication information of sufficient length to meet current cryptographic safety standards.

NOTE: The requirement is necessary to achieve effectiveness of key-based access controls to the interoperable medical system.

C4.1.3.12 The extent to which the item may consume, record, implement, and enforce an operating organization’s policy of operator privilege/authorization (e.g. RBAC) separation should be disclosed.

NOTE: Not all items may provide support for operator identity, authentication, and authorization, so these notions may vary across different items within the interoperable medical system. This requirement asks manufacturers to disclose the extent to which their component is designed to support enforcement of separation of role/privilege which comes with operator authorization, and consequently whether (and to what extent) the rest of the interoperable medical system and other items should perform these duties instead. If the item is intended to provide support for these notions, the manufacturer needs to comply with the rest of the enforcement-related supporting requirements for operator authorization.

C4.1.3.13 The extent to which the item may consume and comply with an operating organization’s policy of item privilege/authorization (e.g. RBAC) separation should be disclosed.

C4.1.3.14 The components responsible for item identification, item authentication, and item authorization should be identified.

NOTE: This helps reason about the safety and security properties of the overall system, even when not all items implement all safety/security services themselves. It provides a simple “sanity check” to see if any component required for safety and security may have been omitted during integration, or not configured to perform its proper function.

C4.1.3.15 The interoperable medical system should have the ability to enforce separation of item network privileges in terms of QoS and which actions are allowed for each item (operator-based and time-based limitations).

NOTE: Unauthorized or excessive use of interoperable medical system resources and service functions should be inaccessible without item authentication followed by authorization.

C4.1.3.16 The interoperable medical system should have the ability to enforce limitations on which resources and sibling items can be accessed by each item at what time (mode-based, operator-based, and time-based limitations).

NOTE: The interoperable medical system should support confidentiality objectives and least-privilege for patient data and system resources.

C4.1.3.17 Failure modes and the item separation of privilege policy to be adopted/enforced in different modes, such as operator-based and time-based, should be identified/disclosed.

NOTE: This is intended to accommodate scenarios such as emergency override (“Break the Glass”)

C4.1.3.18 The alignment of the deployed system with the originating organizations recommended separation of privilege policy for the interoperable medical system and its constituent items and justify any misalignment through a risk management process.

NOTE: Network access control policies and QoS may be enforced by mechanisms out of scope of the interoperable medical system , e.g. manually configured VLANs.

NOTE: Even though the manufacturer may have no knowledge of the particular network privilege policy of the operating organization, the risk management activities for the system should include an analysis the criticality/vulnerability of item interactions with the system with respect to the system’s medical function. Based on this analysis, the system manufacturer can recommend appropriate access policies based on a general understanding of the item’s intended use within the interoperable medical system and care-giving roles in the medical domain in general. Asking the manufacturer to carry out this activity prevents the operating organization from having to “start from scratch” (e.g., to perform a detailed criticality and risk analysis of the system/item interactions) when configuring the system to organization network privilege policy.

C4.1.3.19 The system manufacturer should disclose a recommended separation of privilege policy for the interoperable medical system interoperable items justified by risk management.

NOTE: Network access control policies and QoS may be enforced by mechanisms out of scope of the interoperable medical system , e.g. manually configured VLANs.

NOTE: Even though the manufacturer may have no knowledge of the particular network privilege policy of the operating organization, the risk management activities for the system should include an analysis the criticality/vulnerability of item interactions with the system with respect to the system’s medical function. Based on this analysis, the system manufacturer can recommend appropriate access policies based on a general understanding of the item’s intended use within the interoperable medical system and care-giving roles in the medical domain in general. Asking the manufacturer to carry out this activity prevents the operating organization from having to “start from scratch” (e.g., to perform a detailed criticality and risk analysis of the system/item/operator interactions) when configuring the system to organization network privilege policy.

C4.1.4 Interoperability framework activities

C4.1.4.1 If only one potential authentication method/protocol is supported by an interoperability framework, its implementation should be verified and the responsible item should be disclosed. If multiple options are available, their methods, algorithms, and implementations should be disclosed and verified and the responsible item should be disclosed.

NOTE: A particular method for authentication is not mandated. However, since authentication is a risk control the ability to of the chosen mechanism to achieve the control should be addressed in the assurance arguments.

Annex D
(Informative)

Engineering Properties of Interoperable Medical Systems

D1 Interoperable Item Connectivity

D1.1 Overview

D1.1.1 This topic generates recommendations that relate to the safety and security aspects of connectivity of the interoperable items of an interoperable medical system. Connectivity failure modes identified should be addressed in risk management. For example, interoperable items that depend on connections that are detected as failing would need to indicate how they respond/mitigate such failures.

D1.1.2 This topic also addresses tracking the health of active connections, using interoperable item IDs to track the identity of interoperable items that are connected or disconnected. While this issue is narrowly scoped, the broader topic of connectivity management also includes interoperable items discovery, association, creating data structures that record the current/previously connected interoperable items (and associated meta-data interoperable item descriptions), and techniques for managing the connectivity life cycle.

D1.1.3 The ability of the interoperable medical system to detect the health of connectivity may also provide the information needed to drive the operator displays/notifications addressed by Usability recommendations (see Annex A), which will include (among other things) how to produce indicators and notifications to operators that an interoperable item is currently associated/connected to and/or under the control of the interoperable medical system.

D1.1.4 In many cases, interoperable item technical alarms indicate that something is problematic with the interoperable item's medical function – they are some indicator of the "health" of the interoperable item. When used in interoperability contexts, such alarms typically need to be propagated through the interoperable item's network interface, e.g. every technical alarm expressed through the interoperable item's Operator interface should also be expressed through the interoperable item's network interface. Thus, connectivity failures (as addressed in this section) may impact the ability of an interoperable item to notify its context of failures originating within the interoperable item.

D1.1.5 The recommendations help manufacturers to address the following issues:

a) Hazard analysis needs to identify dependence relationships between all interoperable items in an interoperable medical system. That analysis may be supported/aided by identifying system-theoretic roles of interoperable items (sensor, actuator, controller). Those dependence relationships would be stated in terms of data/control flow.

1) For each interoperable item, hazard analysis should identify other interoperable items on which it depends for information or control, and identify other interoperable items that it controls.

2) Transitive (indirect) notions of dependence and control should be addressed. There can be different levels of connectivity within the interoperable medical system, including differences between intermittent and permanent loss of connectivity.

3) The manufacturer should disclose the reliability required for safe interoperable medical system performance. Timing requirements need to be considered (latency, jitter).

b) How can the interoperable medical system integrator allocate responsibilities for detection/mitigation to different manufacturers (roles), and how may this be reported in the disclosures. This may depend on whether the manufacturers of individual interoperable items have validated their interoperable item for use in a system in compliance with this Standard (see Use Cases)

c) How can the interoperable medical system integrator reason about the “states” of the system and the transitions between them, e.g.:

1) State where interoperable item is able to successfully communicate with other interoperable items.

2) State where interoperable item is unable to successfully communication with other interoperable items (need to distinguish intentional vs. unintentional breaking of the communication).

NOTE: Hazard being addressed is what happens when an interoperable item either locks up (failure to deliver its service) or disconnects from the interoperable medical system.

d) Which interoperable item/interoperable medical system can monitor and detect the states above, and to what degree.

e) Should an internal (to the interoperable medical system) interoperable item become detached, degraded or otherwise inoperative, the risks from this behavior should be addressed, including determining a safe state for the interoperable medical system. Information relevant to safe interoperable operation of the interoperable item within the larger interoperable medical system should be considered, including information disclosed by externally provisioned/sourced interoperable items related to safe and unsafe states as well as the controls necessary to control the states. This information may be presented in machine-readable form and may include information necessary for machine-machine interactions as well as human-machine interactions.

f) What is the role of each interoperable item in responding to the loss of connectivity, and how is this information disclosed.

g) If the interoperable item is a sensor or actuator, its behavior when disconnected should be disclosed such that the manufacturer of an interoperability framework or app/interoperable item can reason about what to do to maintain a safe interoperable medical system.

h) If the interoperable item is a coordinating software application, then the responsible supervisory function can reason about how to respond to an inoperative interoperable item.
i) The interoperable medical system integrator/app must promulgate the requirements needed for safe interoperability, including all the safe states; an interoperable item that does not meet these cannot be safely integrated.

j) Each interoperable item manufacturer discloses how their interoperable item behaves upon disconnect (violation of connectivity contract). interoperable medical system integrator must understand those disclosures.

NOTE: External interoperable medical system is not in a position to receive a disclosure.

k) What issues do interoperability framework manufacturers need to address to coordinate proper use of nomenclature in interoperable medical systems built from their platform asset base.

D1.2 Recommendations

D1.2.1 Interoperable item development

D1.2.1.1 The interoperable item manufacturer’s architectural description should indicate a declaration of the control and data dependences for all interoperability points declared in the item interoperability specification.

NOTE: If an interoperable item is only sending data and is not dependent on data or under the control of an interoperable medical system context for a particular interoperability point it need not be responsible for (or responsibility is reduced) for monitoring the health of that connection. In general, an interoperable item needs to monitor the health of connections when its functions depend on data / control (this may be qualified in terms of safety-related functions).

D1.2.1.2 For each interoperability interface addressed in the interoperable item’s computational view, the criteria to be used for determining the connectivity health of the interface should be specified. The

specification should include criteria characterizing each of the binding states of the connection(s) associated with the interface.

D1.2.1.3 For each interoperability interface, the relationship between declared connectivity health criteria for the interface and the success and failure modes with respect to the declared quality of service specification in associated interface contracts should be specified.

D1.2.1.4 For each interoperability interface, the programmatic methods by that may be used for recognizing satisfaction of and failure to satisfy the health connectivity criteria should be indicated.

D1.2.1.5 For each interoperability interface, the notifications associated with degradation of the connectivity health associated with the interface should be indicated including:

a) Programmatic methods by which peer interoperable items bound to interface are notified of connectivity health degradation as well as information included in such notifications.

b) Technical alarms to be raised as well as associated alarm conditions pertaining to the degradation of connectivity health.

It should be indicated if the interoperable item is providing a connectivity service which has a goal of managing the connectivity of interoperable items.

NOTE: Middleware and interoperability hubs are examples of potential interoperable items that manage connectivity.

D1.2.1.6 [Testing, Assurance Evidence] For each interoperability interface, the interoperable item verification methods used to determine the correctness of the interoperable item's realization of health connectivity monitoring and notification with respect to the specification of those capabilities should be indicated.

D1.2.1.7 [Risk Management] The hazard analysis for the interoperable item should address how degradation of connectivity health for each interoperability interaction point may impact:

a) The ability of the interoperable item to perform sensing and actuation over its physiological interaction points in accordance with the item interoperability specification.

b) The display or acquisition and processing of information associated its Operator Interfaces in accordance with the item interoperability specification.

c) The ability to perform operations on all its interoperability interfaces in accordance with the item interoperability specification.

D1.2.1.8 [Risk Management, Fallback State] One or more fallback states, which are intended to support engineering of safe behavior of the interoperable item within the context of any interoperable medical system into which it may be integrated should be indicated.

D1.2.1.9 [Risk Management, Fallback State, Hazard Analysis] For each indicated fallback state, hazard analysis for the interoperable item should include an analysis of the interoperable item ability to achieve its SSOs when in that fallback state.

NOTE: The additional hazard analysis for this step would include both bottom up and top-down aspects.

D1.2.1.10 [Fallback State Behavior] For each indicated fallback state, the interoperable item manufacturer should include:

a) Ability for a system context to programmatically select a particular fallback state to use as an interoperable item safe state for that particular system context.

b) The ability for a system context to programmatically determine the currently selected fallback state.