

Subject 2800

September 21, 2018

SUMMARY OF TOPICS

The following is being proposed:

1. Proposed First Edition of the Standard for Medical Device Interoperability, AAMI/UL 2800-1

STP BALLOTS AND ALL COMMENTS DUE: November 5, 2018

If you are interested in applying for JC 2800 membership or are aware of potential candidates for this STP, please contact the STP Project Manager, patricia.a.sena@ul.com.

1. Proposed First Edition of the Standard for Medical Device Interoperability, AAMI/UL 2800-1

RATIONALE

Proposal submitted by: AAMI/UL 2800 Joint Committee (JC) Working Group

The use of technology in health care delivery previously relied upon stand-alone medical devices. The combined use of a collection of multi-vendor devices to support broader care-giving goals has not involved technical and engineering integration steps -- rather, clinicians themselves were responsible for manually collecting information from devices and coordinating device use. In today's health care environment, manufacturers are increasingly incorporating different forms of network connectivity into medical devices. The ability to create integrated clinical systems by connecting medical devices, information systems, and other supporting clinical products provides new opportunities for improving safety, creating innovative functionality, and increasing efficiencies within the clinical environment. These opportunities, in the form of future integrated systems, can provide enhanced clinical utility including, for example, multi-device smart alarms and safety interlocks, clinical decision support, automation of clinical workflows, and command and control of devices in the local patient environment.

However, there are a number of challenges preventing the health care community from realizing the full potential of device interoperability. Interoperability is the ability to safely, securely, and effectively exchange and use information among one or more devices, products, technologies, or systems. This exchanged information can be used in a variety of ways including display, store, interpret, analyze, and automatically act on or control another product[§]. Interoperability-related challenges include technical issues (the mechanics of interoperability), systems engineering issues (repeatable processes for correctly and efficiently integrating devices into larger systems), and overarching reliability, safety, and security challenges.

In many cases, only limited device functionality is enabled to connect to network interfaces, thereby preventing full functionality of the device in a broader integrated clinical system. Even with useful interface protocols from the existing work from IHE, IEEE, HL7 and others, the ability to exchange one integrated device for another with similar functionality (i.e. "plug and play") remains a challenge. Health delivery organizations (HDOs) and health care system integration companies are making efforts to build and maintain integrated systems, but it is costly due to the level of customization required. Large

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM**



Documents

Document Sharing Hub

amounts of money are being spent on connecting medical device data to EHRs, using existing interfaces, but much greater progress is needed to provide high-assurance real-time aware technology and the safety/security and risk management techniques to support the full vision of INTEROPERABLE systems that includes device control and automated cross-device coordination.

§This characterization of interoperability is adapted from the US FDA Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices - Guidance for Industry and Food and Drug Administration Staff (issued September 6, 2017).

The lack of broadly applied, well-designed, and well-architected integration platforms is hampering innovation and making it more difficult to build systems that result in improved care and reduced costs. The health care community has yet to fully develop mature platform architecture approaches that help improve safety and security by limiting unanticipated interactions between devices, network communication, and simultaneously-executing applications. This lack of platform architecture makes it difficult to control and mitigate hazards associated with undesired emergent behaviors.

A number of relevant international standards already successfully address segments of this technology space. The Standard for Medical Devices – Application of Risk Management to Medical Devices, ISO 14971, and the Standard for Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance, IEC 60601-1, were developed to support general safety and risk management. However, they do not address the specific safety and technology challenges of INTEROPERABLE systems. The Application of Risk Management for IT-Networks Incorporating Medical Devices, IEC 80001 series adds additional criteria for addressing technology-specific risk of integrating medical devices into hospital IT networks. Additional technology-specific standards exist and serve to aid in the development of INTEROPERABLE devices including the Health Informatics, IEEE 11073 series, and other standards and supporting documents from HL7, IEEE, and IHE. Standards such as the Standard for Medical Devices and Medical Systems – Essential Safety Requirements for Equipment Comprising the Patient-Centric Integrated Clinical Environment (ICE) – Part 1: General Requirements and Conceptual Model, ASTM F2761-09 (2013) provide general requirements and a high-level architecture for an integration platform (Integrated Clinical Environment, or “ICE”). However, this series is still being developed and does not yet include the technical components necessary to achieve standardized interoperability.

The Association for the Advancement of Medical Instrumentation (AAMI) and Underwriters Laboratories Inc. (UL) have formed a joint committee to develop the Standard for Medical Device Interoperability, AAMI/UL 2800-1 to support the development and assurance of safe and secure INTEROPERABLE MEDICAL SYSTEMS. The AAMI/UL 2800 effort works to address safety, security and real-time constraints to enable INTEROPERABLE solutions that can successfully integrate the target devices. This framework will rely, in part, on systems engineering principles intended to enable the ability to interchange devices within the network, supporting the concept of “reusable components.”

AAMI/UL 2800-1 does not prescribe specific technologies or interface specifications for achieving integration and interoperability. The general requirements of 2800-1 are technology-neutral and architecture-neutral: they allow vendors to use existing implementation standards or to innovate with new solutions, provided the chosen implementation approach satisfies the overall safety and security objectives. The standard does not focus on safety and security requirements for individual medical devices. Instead, it focuses on the issues associated with the integration of those devices (via their network interfaces) into broader clinical systems, while normatively referencing existing device- and network- centric standards such as the Standard for Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance, IEC 60601-1; the Standard for Medical Devices – Application of Risk Management to Medical Devices, ISO 14971; and the Application of Risk Management for IT-Networks Incorporating Medical Devices, IEC 80001 series. In addition, AAMI/UL 2800-1 compliance does not necessarily guarantee a safe and secure system. Instead, AAMI/UL 2800-1

should be viewed as defining the minimum set of requirements that are needed to repeatedly achieve a baseline of safety and security when developing integrated systems from reusable devices and infrastructure.

It is anticipated that the users of AAMI/UL 2800-1 will include a range of stakeholders across the health care ecosphere. Interoperability platform providers can use AAMI/UL 2800-1 to design infrastructure and processes that support the development of safe and secure interoperable systems. Device and health information system manufacturers can use AAMI/UL 2800-1 to understand how to implement their interfacing and network communication functionality so as to best support safety and security when integrated into larger systems. Clinical application developers can use AAMI/UL 2800-1 to understand how to perform risk management and assurance activities as they develop integrated clinical systems. HDOs can use AAMI/UL 2800-1 to develop procurement requirements and to understand how clinical processes support the safety and security of deployed integrated systems. The AAMI/UL 2800-1 standard provides a set of minimum safety and security requirements to support regulatory reviews. Moreover, the principles spelled out should provide guidance and testing objectives for compliance of INTEROPERABLE systems to AAMI/UL 2800-1.

The AAMI/UL 2800 Joint Committee provided the Proposed First Edition of the Standard for Medical Device Interoperability, AAMI/UL 2800-1, as a first draft in a CSDS Preliminary Review Work Area opened 11-20-2017 with comments due 12-18-2017 and as a second draft in a CSDS Preliminary Review Work Area opened 07-13-18 with comments due 08-03-18. The Joint Committee has reviewed the comments received and has updated the Proposed Standard to address comments and is now providing the Proposed Standard for ballot.

PROPOSAL

CONTENTS

1	Introduction	11
2	Scope	12
3	References	12
4	Terms and Definitions	14
5	(Leadership) Management Responsibility	29
6	Interoperability Information	29
6.1	Controlled information	29
6.2	INTEROPERABILITY FILE	30
6.3	DISCLOSURE and communication	30
6.3.1	General	30
6.3.2	Information to be disclosed	31
6.3.3	Required DISCLOSURE	32
7	Interoperability Management	32
7.1	Scope of interoperability management	32
7.2	The INTEROPERABLE ENVIRONMENT	32
7.3	Processes for assuring safe and secure interoperability	34
8	Interoperability Realization Processes	35
8.1	Interoperability realization planning	35
8.2	RISK MANAGEMENT	36
8.3	Candidate SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVES	37
8.3.1	General	37
8.3.2	Clinical properties	37
8.3.3	Engineering properties	42
8.3.4	Service properties	45
8.3.5	SECURITY properties	45
9	Design, Development and Implementation of Interoperability	46
9.1	Interoperability context of use	46
9.1.1	General	46
9.1.2	Deployment aspects in context of use	46
9.1.3	Development aspects in context of use	48
9.1.4	INTEROPERABLE USE SPECIFICATION	49
9.2	INTEROPERABILITY SPECIFICATION	49
9.3	Interoperability topology	51
9.3.1	General	51
9.3.2	Architecture specification	51
9.3.3	INTERFACE SPECIFICATION	52
9.3.4	INTERACTION SPECIFICATIONS	52
9.4	Implementation for reusability	53
9.4.1	General	53
9.4.2	Reusability	54
10	Interoperability of EXTERNALLY SOURCED PRODUCTS	55
10.1	Control of EXTERNALLY SOURCED PRODUCTS	55
10.2	Sourcing specifications	55
10.3	VERIFICATION and VALIDATION of externally sourced products	56
10.4	Responsibility for ongoing operation and maintenance	56
10.4.1	General	56
10.4.2	Responsibility agreement	56
11	Provisioning, Deployment, and Operation	57
11.1	Provisioning, deployment and operation specifications	57
11.2	Clinical deployment	57
11.3	Operation	58

UL COPYRIGHTED MATERIAL –
 NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
 DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents

Document Sharing Hub

12	Testing and Review	58
12.1	Testing to interoperability specifications	58
12.1.1	VERIFICATION of product	58
12.1.2	VERIFICATION of CONSTITUENT INTEROPERABLE ITEMS	59
12.1.3	VERIFICATION of configurations with EXTERNAL PRODUCTS	59
12.1.4	VERIFICATION of externally sourced product	59
12.1.5	VERIFICATION of applications	59
12.2	Testing for suitability to context of use	60
12.2.1	VALIDATION of PRODUCT	60
12.2.2	VALIDATION of EXTERNAL PRODUCTS	60
12.2.3	VALIDATION of externally sourced product	60
12.3	Interoperability implementation review and change control	60
13	Traceability and Release	61
13.1	General	61
13.2	INTEROPERABLE APPLICATION SPECIFICATION	62
14	Interoperability Performance Monitoring and Control of Changes	62
14.1	Performance evaluation and monitoring	62
14.2	Information from monitoring	63
14.3	Incident response	64
15	Improvement of Processes	64

Annex A (Informative) Stakeholder Activities

A1	Development Context Activities	66
A1.1	INTEROPERABLE ITEM development	66
A1.2	INTEROPERABLE ITEM integration	67
A1.3	INTEROPERABLE MEDICAL SYSTEM development	68
A1.4	INTEROPERABILITY FRAMEWORK management	69
A2	Deployment Context Activities	70
A2.1	INTEROPERABLE ITEM acquisition/business management	70
A2.2	INTEROPERABLE ITEM technical administration	71
A2.3	Interoperable item assembly	71
A2.4	INTEROPERABLE ITEM clinical administration	72
A2.5	INTEROPERABLE ITEM operation	72

Annex B (Informative) Guidance on Declaration of Products and Services

B0	Interoperability Ecosystem	73
B1	Entities Subject to Compliance Claims	73
B2	Categories of Claims of Compliance	75
B3	Attributes Establishing Relationships Between Compliance and ASSURANCE	76

Annex C (Informative) Guidance on INTEROPERABILITY FILE

C1	Background	79
C2	Listing of Named Work Products	80

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents
Document Sharing Hub

Annex D (Informative) Guidance on DISCLOSURE

D1 Background	99
D2 Key Disclosures	99
D3 Example Disclosure Content	100

Annex E (Normative) Interoperability Realization Life-cycle Process

E1 INTEROPERABLE ITEM Development Life-Cycle Activities	102
E1.1 INTEROPERABLE ITEM concept and context of use development	102
E1.1.1 INTEROPERABLE ITEM synopsis and scope	102
E1.1.2 INTEROPERABLE ITEM OPERATIONAL CONTEXT OF USE description	103
E1.1.3 INTEROPERABLE ITEM DEVELOPMENT CONTEXT OF USE description	103
E1.1.4 IDENTIFICATION of INTEROPERABLE ITEM medical and SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVES	104
E1.1.5 Specification of INTEROPERABLE ITEM-context interactions	104
E1.1.6 Item SAFETY and SECURITY process initiation	105
E1.1.7 Work products	107
E1.2 Development of item requirements and external interoperability specifications	107
E1.2.1 Specification of item boundary	107
E1.2.2 Development of INTEROPERABLE ITEM requirements	108
E1.2.3 INTEROPERABLE ITEM level analysis and RISK MANAGEMENT activities	108
E1.2.4 Development of RELEASE CRITERIA plan	111
E1.2.5 Initiation of INTEROPERABLE ITEM VERIFICATION plan	112
E1.2.6 Initiation of item VALIDATION plan	112
E1.2.7 Initiation of INTEROPERABLE ITEM operating procedures, labeling, and DISCLOSURES	112
E1.2.8 Work products	113
E1.3 INTEROPERABLE ITEM realization	114
E1.3.1 Requirements for implementing interoperability related functionality	114
E1.3.2 Implementation of INTEROPERABLE ITEM without internal interoperability	114
E1.3.3 Implementation of INTEROPERABLE ITEM with internal interoperability	115
E1.3.4 Work products	116
E1.4 INTEROPERABLE ITEM ASSURANCE	116
E1.4.1 INTEROPERABLE ITEM VERIFICATION	116
E1.4.2 INTEROPERABLE ITEM VALIDATION	117
E1.4.3 INTEROPERABLE ITEM Release Criteria Substantiation	117
E1.4.4 Work products	117
E2 INTEROPERABLE ITEM Integration Life-Cycle Activities	117
E2.1 Architecture and INTEROPERABLE ITEM integration concept development	117
E2.1.1 ITEM INTEROPERABILITY ARCHITECTURE and domain asset instantiation	118
E2.1.2 INTEROPERABLE ITEM internal interoperability management	118
E2.1.3 Internal item interoperable component interactions (use cases)	119
E2.1.4 Item preliminary hazard analysis – interoperability-related hazard analysis	119
E2.1.5 Refinement of INTEROPERABLE ITEM SSEPOS and development of FUNCTIONAL SAFETY CONCEPT	120
E2.1.6 Work products	120
E2.2 Architecture and integration specification	121
E2.2.1 Development of internal INTEROPERABILITY ARCHITECTURE and INTERFACE SPECIFICATION	121
E2.2.2 Development of internal interoperability requirements	122
E2.2.3 Item architecture analysis and RISK MANAGEMENT activities	123
E2.2.4 Development of RELEASE CRITERIA plan for INTEROPERABLE ITEM integration	125
E2.2.5 Initiation of integration VERIFICATION plan	126

E2.3	Constituent INTEROPERABLE ITEM development	126
E2.3.1	Internally sourced CONSTITUENT INTEROPERABLE ITEMS	126
E2.3.2	Externally sourced constituent INTEROPERABLE ITEMS	127
E2.4	INTEROPERABLE ITEM integration engineering	128
E2.4.1	INTEROPERABLE ITEM integration	128
E2.4.2	INTEROPERABLE ITEM integration RISK MANAGEMENT	128
E2.5	INTEROPERABLE ITEM integration ASSURANCE	129
E2.5.1	Internal integration testing	129
E2.5.2	Completion of INTEROPERABLE ITEM integration ASSURANCE	129
E3	Domain Engineering Life-Cycle Processes	129

Annex F (Informative) GUIDANCE ON RELEASE CRITERIA

F1	General	130
F1.1	INTEROPERABLE ITEM development activity RELEASE CRITERIA	130
F1.1.1	INTEROPERABLE ITEM Specification Activity RELEASE CRITERIA	130
F1.1.2	INTEROPERABLE ITEM Realization Activity RELEASE CRITERIA	131
F1.1.3	Interoperable Item ASSURANCE Activity RELEASE CRITERIA	132
F1.1.4	INTEROPERABLE ITEM EXTERNAL MEASURES RELEASE CRITERIA	132
F1.2	INTEROPERABLE ITEM Integration Activity RELEASE CRITERIA	132
F1.2.1	INTEROPERABLE ITEM Integration Activity RELEASE CRITERIA	132
F1.2.2	INTEROPERABLE ITEM Integration ASSURANCE Activity RELEASE CRITERIA	133
1.3	INTEROPERABLE MEDICAL SYSTEM RELEASE CRITERIA	133
F1.3.1	INTEROPERABLE MEDICAL SYSTEM Specification RELEASE CRITERIA	133
F1.3.2	INTEROPERABLE MEDICAL SYSTEM Realization Activity RELEASE CRITERIA	134
1.3.3	Interoperable Medical System ASSURANCE Activity RELEASE CRITERIA	134

Annex G (Informative) Testing Guidance

G1	General	135
G2	Scope of Testing	135
G3	Definitions and Abbreviations	135
G4	Prerequisites for Testing	135
G5	Component Testing	135
G6	System Testing (Integration Testing)	137
G7	Regression Testing (For addressing modifications to the system and/or a component)	139
G7.1	More Granular Testing Details for Consideration	139
G7.2	SAFETY-Related Component Testing	140
G7.4	Basic SECURITY-related Testing	140

Annex H (Informative) RISK MANAGEMENT Guidance

H1	Overview	142
H2	Relationships to ISO 14971	144

Annex I (Informative) Common Fault Types

Annex J (Informative) Interoperability Usability Concepts

J1 Overview	150
J2 Recommendations	151

Annex K (Informative) SECURITY Principles

K1 SECURITY Elements of SSEPOs	154
K2 Relationship to UL 2900	155

Annex L (Informative) Clinical Context Concepts

L1 Requirements that Need to be Supported	157
L2 Informative Content	157

Annex M (Informative) Clinical Properties of INTEROPERABLE MEDICAL SYSTEMS

M1 Semantic Interoperability and Nomenclature	161
M1.1 Overview	161
M1.2 Recommendations	163
M1.2.1 INTEROPERABLE ITEM Development	163
M1.2.2 INTEROPERABLE ITEM Integration	164
M1.2.3 INTEROPERABLE MEDICAL SYSTEM Development	165
M1.2.4 INTEROPERABILITY FRAMEWORK	165
M1.2.5 Supporting Concepts	165
M2 PATIENT IDENTITY AND ASSOCIATION	166
M2.1 Overview	166
M2.2 Recommendations	166
M2.2.1 INTEROPERABLE ITEM Development Activities	166
M2.2.2 INTEROPERABLE MEDICAL SYSTEM Development Activities	168
M3 OPERATOR IDENTIFICATION, AUTHENTICATION, and AUTHORIZATION	169
M3.1 Overview	169
M3.2 Recommendations	169
M3.2.1 INTEROPERABLE ITEM Development	169
M3.2.2 INTEROPERABLE ITEM Integration	172
M3.2.3 INTEROPERABLE MEDICAL SYSTEM Development	173
M3.2.4 INTEROPERABILITY FRAMEWORK	176
M4 Operator IDENTIFICATION, AUTHENTICATION, and AUTHORIZATION	177
M4.1 Recommendations	177
M4.1.1 INTEROPERABLE ITEM DEVELOPMENT Activities	177
M4.1.2 INTEROPERABLE ITEM Integration Activities	179
M4.1.3 INTEROPERABLE MEDICAL SYSTEM Development Activities	179
M4.1.4 INTEROPERABILITY FRAMEWORK Activities	183

Annex N (Informative) Architecture Definition Guidance

N1 Overview	184
N2 Topological Vocabulary Overview	185
N3 Examples	187
N3.1 INTEROPERABLE ITEM	187
N3.2 INTEROPERABLE MEDICAL SYSTEM	189

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents

Document Sharing Hub

N3.3 INTEROPERABILITY FRAMEWORK	191
4 Summary of Architectural Viewpoints	192
5 Guidance on Use of Architecture Modeling Notations	193

Annex O (Informative) INTEROPERABILITY ARCHITECTURE SPECIFICATION

O1 Interoperability Viewpoint Guidance	195
O1.1 General guidance on interoperability view specification	195
O1.2 External interoperability – Specifying relationships between the product and its context	195
O1.3 Internal interoperability – Specifying the product’s CONSTITUENT INTEROPERABLE ITEM and their interoperability relationships	195
O2 Computational, Engineering, and Technology Viewpoint Guidance	196
O2.1 General	196
O2.2 COMPUTATIONAL VIEW – Computational objects	196
O2.3 COMPUTATIONAL VIEW – INTEROPERABILITY INTERFACES	196
O2.4 Guidance on decomposing interoperability view interoperability INTERACTION POINTS into COMPUTATIONAL VIEW interfaces and interactions	197
O2.5 INTERACTION SPECIFICATIONS	197
O2.6 Behavioral descriptions	198
O2.9 Engineering view – Node structure	198
O2.10 Engineering view – Channel structure	199
O3 Interactions with External Systems	199

Annex P (Informative) Engineering Properties of INTEROPERABLE MEDICAL SYSTEMS

P1 INTEROPERABLE ITEM Connectivity	201
P1.1 Overview	201
P1.2 Recommendations	203
P1.2.1 INTEROPERABLE ITEM Development	203
P1.2.2 INTEROPERABLE ITEM Integration	205
P2 Safe States	207
P2.1 Overview	207
P2.2 Recommendations	207
P2.2.1 INTEROPERABLE ITEM Development	207
P2.2.2 INTEROPERABLE ITEM Integration	208
P2.2.3 INTEROPERABLE MEDICAL SYSTEM Development	208
P3 Time Synchronization	208
P3.1 Overview	208
P3.2 Recommendations	209
P4 Shared Resources and Data and Time Partitioning	210
P4.1 Overview	210
P4.2 Recommendations	211

Annex Q (Informative) Services for INTEROPERABLE MEDICAL SYSTEMS

Q1 General	213
Q1.1 ALARM SYSTEM Considerations	213
Q1.2 Management of ALARM CONDITIONS in an INTEROPERABLE MEDICAL SYSTEM	213
Q2 ALARM SIGNALING to OPERATOR	214
Q3 ALARM SYSTEM characteristics	214

Q3.1 Logging	214
Q3.2 Acknowledgment	215
Q3.3 Quality of service	215
Q3.4 Security	215
Q4 Intelligent ALARM SYSTEM	215
Q5 INTEROPERABLE ITEM Capabilities	215
Q6 INTEROPERABLE MEDICAL SYSTEM Maintenance and Diagnostics	216

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents
Document Sharing Hub

1 Introduction

1.1 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, this Standard establishes a baseline set of requirements for assuring safe and secure interoperability.

1.2 The requirements in this Standard may be applied to medical devices, as well as other connected infrastructure elements, and interoperable medical systems constructed from these. The Standard can be used by an ORGANIZATION as detailed in Annex A.

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 this Standard. This first requires that each stakeholder adequately assesses and manages SAFETY, SECURITY AND ESSENTIAL PERFORMANCE 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, SECURITY AND ESSENTIAL PERFORMANCE characteristics. Finally, it requires that each stakeholder clearly communicates to the other stakeholders the information required to assure interoperability.

1.5 This Standard employs a lifecycle process approach to organizing requirements. In addition to a set of broad management functions, the Standard provides for a set of interoperability planning, realization, deployment, and monitoring activities. These activities also incorporate cross-cutting requirements for SECURITY and risk management. The Standard recognizes that a given ORGANIZATION may be responsible for only a part of the full range of activities required for an INTEROPERABLE MEDICAL SYSTEM. Furthermore, its INTEROPERABLE MEDICAL PRODUCTS may provide only a specific or limited functionality. To accommodate this, the Standard provides for flexibility in the scope, sequence, and INTERACTION of these activities. Finally, the Standard provides requirements and supplementary guidance on key clinical and engineering properties of an INTEROPERABLE MEDICAL SYSTEM that are essential to assuring effective interoperability and provides guidance on lifecycle activities and artifacts to be generated.

1.6 Annex A lists activities within the INTEROPERABILITY ECOSYSTEM and indicates important process steps for assuring interoperability.

1.7 As part of complying with this Standard, an ORGANIZATION will need to understand its specific role in the INTEROPERABILITY ECOSYSTEM, as well the role of the various other stakeholders. Collectively, stakeholders that intend their products to be interoperable have shared responsibility for assuring interoperability for a particular INTEROPERABLE MEDICAL SYSTEM. Assuring this will require collaboration among all the stakeholders in the INTEROPERABILITY ECOSYSTEM. Hence it is essential that responsibilities for meeting specific requirements are unambiguously communicated among the stakeholders. This Standard also includes requirements for DISCLOSURE and other communications. These may be used for identifying contractual requirements among the stakeholders.

1.8 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 this Standard may be integrated into the ORGANIZATION'S processes previously established for meeting quality and RISK MANAGEMENT and product-specific requirements.

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 this Standard 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 this Standard.

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 requirements for assuring safe and secure interoperability for INTEROPERABLE MEDICAL SYSTEMS.

3 References

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 Standards

AAMI TIR57

Technical Information Report: Principles for Medical Device security – Risk Management

AAMI TIR69

Technical Information Report Risk management of radio-frequency wireless coexistence for medical devices and systems

ANSI Standards

ANSI IEEE C63.27

American National Standard for Evaluation of Wireless Coexistence

ASTM Standards

ASTM F2761

Standard for Medical Devices and Medical Systems – Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE) – Part 1: General requirements and conceptual model

IEC Standards

IEC 60601-1

Standard for Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance

IEC 60601-1-2

Standard for Medical Electrical Equipment – Part 1-2: General Requirements for Basic Safety and Essential Performance – Collateral Standard: Electromagnetic Disturbances – Requirements and Tests

IEC 60601-1-8

Standard for 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 60601-1-11

Standard for Medical Electrical Equipment – Part 1-11: General Requirements for Basic Safety and Essential Performance – Collateral Standard: Requirements for Medical Electrical Equipment and Medical Electrical Systems Used in the Home Healthcare Environment

IEC 62304

Standard for Medical Device Software – Software Life Cycle Processes

IEC 80001-1

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

IEC TR 80001-2-2

Application Guidance – Guidance for the Disclosure and Communication of Medical Device security Needs, Risks and Controls

IEC TR 80001-2-3

Application Guidance – Guidance for Wireless Networks

IEC TR 80001-2-4

Application Guidance – General Implementation Guidance for Healthcare Delivery Organizations

IEC TR 80001-2-5

Application Guidance – Guidance on Distributed Alarm Systems

IEC TR 80001-2-6

Application Guidance – Guidance for Responsibility Agreements

ISO Standards

ISO 14971

Standard for Medical Devices – Application of Risk Management to Medical Devices

NIST Standards

NIST Special Publication 800-66

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) security Rule

NIST 800-92

Guide to Computer security Log Management

4 Terms and Definitions

4.1 ACTOR – An active or passive entity, human or non-human, capable of initiating action or providing data, potentially in response to commands.

NOTE 1: An INTEROPERABLE ITEM is a special case of non-human ACTOR.

NOTE 2: Health IT systems including Electronic Medical Record systems or Physician Order Entry systems are examples of non-human ACTORS that may not be INTEROPERABLE ITEMS.

NOTE 3: Medical devices are examples of non-human actors (which may or may not comply with the requirements of this Standard, i.e., may or not be INTEROPERABLE ITEMS).

NOTE 4: OPERATORS and PATIENTS are examples of human ACTORS.

NOTE 5: ACTORS may be distinguished by context of use including DEVELOPMENT CONTEXT OF USE ACTORS (e.g., interoperable medical system manufacturers), DEPLOYMENT CONTEXT OF USE ACTORS (e.g., clinicians, bio-medical engineers, etc.)

4.2 ALARM CONDITION – State of the ALARM SYSTEM when it has determined that a potential or actual HAZARDOUS SITUATION exists for which OPERATOR awareness or response is required.

NOTE 1: An ALARM CONDITION can be invalid, i.e. a false positive ALARM CONDITION.

NOTE 2: An ALARM CONDITION can be missed, i.e. a false negative ALARM CONDITION.

©IEC. This material is reproduced from IEC 60601-1:2006+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.3 ALARM LIMIT— Threshold used by an ALARM SYSTEM to determine an ALARM CONDITION

4.4 ALARM SETTINGS — ALARM SYSTEM configuration, including but not limited to:

- a) ALARM LIMITS;
- b) The characteristics of any ALARM SIGNAL inactivation states; and
- c) The values of variables or parameters that determine the function of the ALARM SYSTEM

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM  Documents
Document Sharing Hub

NOTE: Some algorithmically-determined ALARM SETTINGS can require time to be determined or re-determined.

4.5 ALARM SIGNALING – Action taken by the ALARM SYSTEM to generate an ALARM SIGNAL at the OPERATOR'S position.

4.6 ALARM SIGNAL – Type of signal generated by the ALARM SYSTEM to indicate the presence (or occurrence) of an ALARM CONDITION.

©IEC. This material is reproduced from IEC 60601-1-8:2006 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.7 ALARM SYSTEM – Parts of ME EQUIPMENT or a ME SYSTEM that detect ALARM CONDITIONS and, as appropriate, generate ALARM SIGNALS.

©IEC. This material is reproduced from IEC 60601-1-8:2006+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.8 ALARM SUPPRESSION – Action taken by the ALARM SYSTEM to not generate an ALARM SIGNAL at the OPERATOR'S position when an ALARM CONDITION is detected.

4.9 ARCHITECTURE VIEW – Artifact within the INTEROPERABILITY ARCHITECTURE expressing the architecture from the perspective of specific set of concerns.

Adapted by UL from ISO/IEC/IEEE 42010-2011 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.10 ARCHITECTURE VIEWPOINT – Constraints establishing the conventions for the construction, interpretation, and use of an ARCHITECTURE VIEW to frame a specific set of concerns.

Adapted by UL from ISO/IEC/IEEE 42010-2011 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.11 ASSURANCE – Grounds for justified confidence that a claim has been or will be achieved.

NOTE: Assurance activities include verification and VALIDATION activities that provide OBJECTIVE EVIDENCE for claims reflected in INTEROPERABLE ITEM SSEPOs and INTEROPERABILITY SPECIFICATION.

©IEC. This material is reproduced from ISO/IEC 15026-1:2013 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.12 AUTHENTICATION/AUTHENTICATED/AUTHENTICITY – The process of verifying the IDENTITY of an entity.

4.13 AUTHENTICATION OF INFORMATION – Sensitive data is any critical SECURITY parameter that can compromise the use and SECURITY of the product such as passwords, keys, seeds for random number generators, AUTHENTICATION data., personally identifiable information and any data whose DISCLOSURE could jeopardize the SECURITY properties of the product.

4.14 AUTHORIZATION/AUTHORIZED – [Source: CNSSI-4009 via AAMI TIR57]

4.15 AVAILABILITY/AVAILABLE – [Source: SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542 via AAMI TIR57]

4.16 CLINICAL CARE – PATIENT contact and/or management, which corresponds to a block of activity (session) directly related to:

- a) Diagnosis of disease or other conditions,
- b) Cure, alleviation, mitigation, treatment/therapy, or prevention of disease,
- c) Compensation for an injury or handicap,
- d) Replacement or modification of the anatomy or of a physiological process, or
- e) Intended to affect the structure or any function of the body of the PATIENT.

4.17 COMPUTATIONAL VIEW – An aspect of the INTEROPERABILITY ARCHITECTURE that provides a decomposition in terms of logical functional as interactions between those functions.

NOTE 1: The Computational View is based on concepts from the ISO/IEC 10746 RM-ODP Computational View. However, this Standard does to require compliance to ISO/IEC 10746.

NOTE 2: The Computational View captures what is commonly referred to as a functional architecture, where interactions between functional elements are captured in terms of programmatic interfaces.

NOTE 3: For an overview of the notions of architectural view and viewpoint see ISO/IEC/IEEE 40210.

4.18 CONFIDENTIALITY – The property that data, information or software is not made AVAILABLE or disclosed to unauthorized individuals, entities, or processes.

4.19 CONSTITUENT INTEROPERABLE ITEM – A member of the collection of INTEROPERABLE ITEMS integrated to form the realization of an encompassing INTEROPERABLE ITEM (See definition of INTEROPERABLE ITEM (b)).

4.20 DEPLOYMENT CONTEXT OF USE – ACTORS, processes, and health-delivery objectives that may impact the safe and secure use of the INTEROPERABLE MEDICAL PRODUCT as part of deployment activities.

NOTE 1: DEPLOYMENT CONTEXT OF USE activities are summarized in Annex A.

NOTE 2: In typical cases, the DEPLOYMENT CONTEXT OF USE refers to the context of use in a Health Delivery Organization and addresses the use of the interoperability solution to support medical functions as well as the configuration, deployment, and maintenance of the interoperability solution.

4.21 DEVELOPMENT CONTEXT OF USE – Organizations, processes, technologies, INTEROPERABILITY FRAMEWORKS, and business relationships that may influence or use the INTEROPERABLE MEDICAL PRODUCT as part of development activities.

NOTE: DEVELOPMENT CONTEXT OF USE Activities are summarized in Annex A, and detailed in Annex E.

4.22 DISCLOSURE – Planned and managed release of information between the ORGANIZATION originating the INTEROPERABLE ITEM and stakeholder organizations to support the safe and secure use of the INTEROPERABLE ITEM in its DEVELOPMENT CONTEXT OF USE OR DEPLOYMENT CONTEXT OF USE.

NOTE 1: See Annex C and D for guidance on disclosures.

NOTE 2: ISO 14971 Information for Safety, IEC 80001 Responsibility Agreements and Information for Assurance are addressed by the disclosures of this Standard.

NOTE 3: Disclosures support “risk hand-offs” between organizations and are key element of supporting CROSS-ORGANIZATION risk management for INTEROPERABLE MEDICAL SYSTEMS.

4.23 EFFECTIVENESS – Ability to produce the intended result for the PATIENT and the RESPONSIBLE ORGANIZATION. Reasonable ASSURANCE that a device is successful in producing a desired or intended result when it can be determined, based upon valid scientific evidence, that in a significant portion of the target population, the use of the device for its intended uses and conditions of use, when accompanied by adequate directions for use and warnings against unsafe use, will provide clinically significant results.

©IEC. This material is reproduced from IEC 80001-1:2010 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.24 ERROR – Deviation from an ITEM INTEROPERABILITY SPECIFICATION that is observable on an interface of the INTEROPERABLE ITEM.

NOTE 1: An ERROR originating in an INTEROPERABLE ITEM's context may propagate into the INTEROPERABLE ITEM through its interface inputs.

NOTE 2: An ERROR may propagate out of an INTEROPERABLE ITEM over an interface due to either:

- a) A fault internal to the INTEROPERABLE ITEM; or
- b) An ERROR propagating into the INTEROPERABLE ITEM from its context that is passed through the INTEROPERABLE ITEM or transformed into an ERROR of different character.

4.25 ERROR PROPAGATION SPECIFICATION – Summary of inward and outward flowing interoperability-related ERRORS that may manifest on the INTEROPERABLE ITEM'S INTERFACES.

NOTE: See Annex H for the purpose of the ERROR PROPAGATION SPECIFICATION in the context of broader risk management activities. See Annex C for relationship of the ERROR PROPAGATION SPECIFICATION to other work products.

4.26 ESSENTIAL PERFORMANCE – The performance necessary to achieve freedom from unacceptable risk.

©IEC. This material is reproduced from IEC 60601-1:2005 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.27 EXTERNAL MEASURE – measure separate and distinct from the INTEROPERABLE ITEM that reduces or mitigates the risks resulting from the INTEROPERABLE ITEM or usage of the INTEROPERABLE ITEM within its DEVELOPMENT CONTEXT OF USE OR DEPLOYMENT CONTEXT OF USE.

NOTE 1: The means by which an external measure is to be achieved will typically be communicated through instructions for use and will typically coincide with ISO 14971 Information for Safety (Clause 6.2).

NOTE 2: INTEROPERABLE ITEM SSEOPs and EXTERNAL MEASURES are designed in concert with the intent that the

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM

Documents
Document Sharing Hub

INTEROPERABLE ITEM will be able to achieve its SSEPOs if the EXTERNAL MEASURES are achieved.

NOTE 3: EXTERNAL MEASURES represent obligations of the agents in the context of the INTEROPERABLE ITEM whereas SSEPOs represent obligations on INTEROPERABLE ITEM, given that EXTERNAL MEASURES are achieved. The organization producing the INTEROPERABLE ITEM also has the obligation of communicating the EXTERNAL MEASURES clearly.

Adapted by UL from ISO 26262-1:2011 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.28 EXTERNAL PRODUCT – An anticipated non-human ACTOR or specified INTEROPERABLE ITEM with which the INTEROPERABLE MEDICAL PRODUCT interacts but is not provided with the INTEROPERABLE MEDICAL PRODUCT.

NOTE – An EXTERNAL PRODUCT may be specified as an accessory to be provisioned by the user of the INTEROPERABLE MEDICAL PRODUCT (such as a sensor device) or be a part of the INTEROPERABLE ENVIRONMENT within which the INTEROPERABLE MEDICAL PRODUCT is used (such as an electronic medical record system).

4.29 EXTERNALLY SOURCED PRODUCT – Either a CONSTITUENT INTEROPERABLE ITEM in an INTEROPERABLE MEDICAL PRODUCT or an EXTERNAL PRODUCT that is specified as necessary to proper use of the INTEROPERABLE MEDICAL PRODUCT that is placed on the market by an external party that is not part of the ORGANIZATION.

4.30 FUNCTIONAL SAFETY CONCEPT – Design of functional and independence aspects of risk controls and associated requirements as necessary to achieve SSEPOs.

Adapted by UL from ISO 26262-1:2011 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.31 HAZARDOUS SITUATION – Circumstance in which people, property, or the environment are exposed to one or more hazard(s).

©IEC. This material is reproduced from ISO/IEC Guide 51:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.32 IDENTIFICATION/IDENTIFIED – See AUTHENTICATED.

4.33 IDENTIFIER – *[Source – Adapted from RFC 2828 (referring to DATA, but is generalized for this document)]*

4.34 IDENTITY – A particular presentation of an OPERATOR or INTEROPERABLE ITEM. An IDENTITY may be a unique reference to the OPERATOR or INTEROPERABLE ITEM, especially binding when proved through AUTHENTICATION.

4.35 IDENTITY CLAIM – Assertion or statement of the state or fact of being the same one as described.

4.36 INFORMATION VIEW – An aspect of the INTEROPERABILITY ARCHITECTURE that describes:

- a) The primary data elements exchanged between CONSTITUENT INTEROPERABLE ITEMS and between the INTEROPERABLE ITEM and its context; and
- b) Operations on those data elements.

NOTE 1: The INFORMATION VIEW is based on concepts from the ISO/IEC 10746 RM-ODP INFORMATION VIEW. However, this Standard requires compliance to ISO/IEC 10746

NOTE 2: The INFORMATION VIEW may also capture important internal state of an INTEROPERABLE ITEM that is necessary to specify constraints on the INTEROPERABLE ITEM's interoperability behavior.

NOTE 3: For an overview of the notions of architectural view and viewpoint see ISO/IEC/IEEE 40210.

4.37 INTEGRATOR – Natural or legal person carrying out the activity of INTEROPERABLE ITEM integration. See Annex A.

4.38 INTEGRITY – The ASSURANCE that data can only be altered by AUTHORIZED entities.

4.39 INTENDED USE [intended purpose] – Use for which a product, process or service is intended according to the specifications, instructions and information provided by the MANUFACTURER.

©ISO. This material is reproduced from ISO 14971-1:2007 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.40 INTERACTION – An action between an INTEROPERABLE ITEM and its context taking place over one of the INTEROPERABLE ITEM'S interfaces. See Annex O.

NOTE: An INTERACTION involves the participation of both the INTEROPERABLE ITEM and an ACTOR in its context. When the ACTOR in the context is an another INTEROPERABLE ITEM, the INTERACTION occurs over an INTEROPERABILITY INTERFACE.

4.41 INTERACTION BEHAVIORAL SPECIFICATION – Constraints on the interactions between an INTEROPERABLE ITEM and its context over its INTERFACES specified in terms of INTERFACE CONTRACTS.

NOTE: Specifications of interactions over the INTEROPERABILITY INTERFACES of an INTEROPERABLE ITEM are stated in terms of INTERFACE CONTRACTS.

4.42 INTERACTION PARAMETER SPECIFICATION – Part of an INTERACTION SPECIFICATION that specifies the parameters and accompanying characteristics of a particular INTERACTION. See Annex O.

4.43 INTERACTION POINT – INTEROPERABILITY ARCHITECTURE feature defined for the purpose of stating constraints and assumptions on data and control [information] that flow across an INTEROPERABLE ITEM'S BOUNDARY.

Each interaction point is specified as exactly one of the following types:

- a) Physiological – Supports machine-to-patient interactions associated with sensing or actuation capabilities related to the physiology of the patient;
- b) Operator – Supports machine-to-human interactions for commands or information exchange between the INTEROPERABLE ITEM and OPERATOR; or
- c) Interoperability – Supports machine-to-machine interactions.

An interoperability INTERACTION POINT consists of one or more related INTEROPERABILITY INTERFACES.

4.44 INTERACTION SPECIFICATION – Characteristics of an INTERACTION given at a level of precision that are sufficient to:

- a) Determine if INTEROPERABLE ITEMS participating in the INTERACTION comply with the specification; and
- b) Exclude undesirable behaviors leading to violations of SAFETY-related and SECURITY-related properties. See Annex O.

INTERACTION SPECIFICATIONS are accompanied by INTERFACE CONTRACTS that constrain the behavior of INTERACTIONS over INTERFACES.

4.45 INTERFACE CONTRACT – Behavioral constraints on the interactions between an INTEROPERABLE ITEM and its context over one of its INTEROPERABILITY INTERFACES.

NOTE 1: An INTERFACE CONTRACT imposes obligations on both the INTEROPERABLE ITEM and its clients. An INTERFACE CONTRACT will typically establish pre-conditions that clients of the INTEROPERABLE ITEM must achieve before or at the initiation of an interactions, and post-conditions that the INTEROPERABLE ITEM must achieve given that associated pre-conditions are satisfied.

NOTE 2: An INTERFACE CONTRACT may include constraints on data exchanged during an interaction, temporal ordering of interactions on the INTEROPERABILITY INTERFACE, timing constraints on the interaction or sequence of interactions, and exceptional behavior and error return codes.

Adapted by UL from ISO/IEC 10746-2:2010 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.46 INTERFACE SPECIFICATION— Collection of INTERACTION SPECIFICATIONS, associated INTERFACE CONTRACTS, and engineering and technology aspects of the interface realization.

4.47 INTEROPERABILITY ARCHITECTURE— Constraints and rules determining the ORGANIZATION of a set of INTEROPERABLE ITEMS, their designed interoperable interactions with each other, and their intended interactions with environment. The INTEROPERABILITY ARCHITECTURE provides a decomposition at the granularity at which INTEROPERABLE ITEMS may be exchanged and reused according to their designed interoperability.

NOTE 1: An INTEROPERABILITY ARCHITECTURE may be defined using a variety of methods including annotated graphical models or textual constraints as long as the precision is sufficient to determine compliance to this Standard. The INTEROPERABILITY ARCHITECTURE may be incorporated into a more comprehensive architecture description that addresses non-interoperability-related aspects.

NOTE 2: The rules and constraints of an INTEROPERABILITY ARCHITECTURE capture designed INTEROPERABILITY VARIABILITIES that allow multiple interoperability architecture instances to be compliant with an INTEROPERABILITY ARCHITECTURE. This concept enables a set of related interoperability architecture instances to be addressed determining compliance to this Standard.

4.48 INTEROPERABILITY ARCHITECTURE CONFIGURATION – Specific restriction of one or more INTEROPERABILITY VARIABILITIES of an INTEROPERABILITY ARCHITECTURE

NOTE: An INTEROPERABILITY ARCHITECTURE CONFIGURATION is a refinement of an INTEROPERABILITY ARCHITECTURE that restricts the set of conformant INTEROPERABILITY ARCHITECTURE INSTANCES for a particular purpose. Examples of common restrictions include bounding the number or types of medical devices that can connect with a platform, or restricting the applications that may be executed simultaneously with a high-criticality application. Such restrictions may be useful for scoping the use of an interoperability framework for a particular set of related applications whose ASSURANCE will be addressed collectively.

4.49 INTEROPERABILITY ARCHITECTURE INSTANCE— An INTEROPERABILITY ARCHITECTURE CONFIGURATION where no INTEROPERABILITY VARIABILITIES remain.

NOTE 1: An INTEROPERABILITY ARCHITECTURE INSTANCE represents a concrete realization whose behavior can be assessed via testing.

NOTE 2: An instance of an INTEROPERABILITY ARCHITECTURE for an INTEROPERABLE MEDICAL SYSTEM may be executed at the point-of-care to provide a particular clinical function.

NOTE 3: Compliance of an INTEROPERABLE ITEM to this Standard addresses the SAFETY and SECURITY properties of all INTEROPERABILITY ARCHITECTURE INSTANCES that conform to the INTEROPERABLE ITEM's INTEROPERABILITY ARCHITECTURE.

4.50 INTEROPERABILITY BINDINGS — Planned association of two or more INTEROPERABLE ITEMS over designated INTEROPERABILITY INTERFACES of the INTEROPERABLE ITEMS.

4.51 INTEROPERABILITY ECOSYSTEM — Stakeholders whose products and services enable interoperability.

4.52 INTEROPERABILITY FILE — One or more information repositories either containing or referencing records generated to demonstrate compliance to the requirements of this Standard.

4.53 INTEROPERABILITY FRAMEWORK — Consists of a managed collection of interoperability assets including:

- a) Items designed to be integrated in different configurations in conformance with a INTEROPERABILITY ARCHITECTURE;
- b) Processes conforming to life-cycle objectives of this Standard for coordinating life-cycle activities across the framework items to increase effective and trustworthy reuse of items and associated specification, RISK MANAGEMENT, and ASSURANCE results; and
- c) Assets, shared across the development of the framework items, for supporting interoperability-related aspects of development and ASSURANCE.

NOTE: The notion of an INTEROPERABILITY FRAMEWORK supports the notions of platform-based development, product lines and product families (e.g., as described in ISO/IEC 26550), and families of items developed around a common interoperability interfacing framework (e.g., IEEE 11073).

4.54 INTEROPERABILITY INTERFACE— An engineered mechanism for information exchange that provides all or part of a realization of an interoperability INTERACTION POINT.

NOTE 1: An interoperability INTERACTION POINT will often be realized in terms of multiple interfaces that address different levels of abstraction. For example, an interoperability INTERACTION POINT for reporting physiological data from a medical device may include network transport layer interfaces, middleware service interfaces, and data description interfaces.

NOTE 2: The granularity of an interface specified for the purposes of compliance with this Standard may be determined by following guidance in Annex N and Annex O.

4.55 INTEROPERABILITY SCENARIOS SPECIFICATIONS – Partial specification of an INTEROPERABLE MEDICAL SYSTEM or family of related INTEROPERABLE MEDICAL SYSTEMS describing an intended application of interoperability that may be evaluated under this Standard.

NOTE 1: An INTEROPERABILITY SCENARIO SPECIFICATION may serve to normalize use cases, requirements, and architectural approaches for the purpose of establishing community consensus for particular applications.

NOTE 2: An INTEROPERABILITY SCENARIO SPECIFICATION may be used as input to the later design and realization of an INTEROPERABLE MEDICAL SYSTEM which may benefit from reuse of the artifacts developed in and may claim compliance to the INTEROPERABILITY SCENARIO SPECIFICATION. See Annex B.

NOTE 3: An INTEROPERABILITY SCENARIO SPECIFICATION may include as aspects of use specification, INTEROPERABILITY ARCHITECTURE, INTEROPERABLE, and the like.

4.56 INTEROPERABILITY VARIABILITY— Designed feature within the INTEROPERABILITY ARCHITECTURE allowing variations in the set of conforming instances.

4.57 INTEROPERABLE APPLICATION SPECIFICATION – A summary of the important characteristics related to the use of the INTEROPERABLE MEDICAL PRODUCT within stated INTEROPERABILITY SCENARIO SPECIFICATIONS.

4.58 INTEROPERABLE ENVIRONMENT – The managed collection of interoperable products and associated services that can be integrated in one or more configurations to enable interoperable use of a specific INTEROPERABLE MEDICAL PRODUCT.

4.59 INTEROPERABLE ITEM— A realization of an ITEM INTEROPERABILITY SPECIFICATION for interoperable hardware, software or system to which the contents of this Standard are applied. This may take one of two forms:

- a) It may not be further decomposed with respect to interoperability and compliance with this Standard; or
- b) It may be a collection of INTEROPERABLE ITEMS integrated in accordance with integration life-cycle activities.

NOTE: A member of the collection of the integrated INTEROPERABLE ITEMS in (b) is referred to as a CONSTITUENT INTEROPERABLE ITEM.

4.60 INTEROPERABLE ITEM BOUNDARY – The division between the realization of the INTEROPERABLE ITEM and external ACTORS, as defined by the INTEROPERABLE ITEM'S INTERACTION POINTS.

NOTE: The boundary may help scope the ASSURANCE, risk management, and disclosure responsibilities of the INTEROPERABLE ITEM MANUFACTURER by indicating the engineering features under the INTEROPERABLE ITEM MANUFACTURER'S direct control.

4.61 INTEROPERABLE ENVIRONMENT – The managed collection of interoperable products and associated services that can be integrated in one or more configurations to enable interoperable use of a specific INTEROPERABLE MEDICAL PRODUCT.

4.62 INTEROPERABLE MEDICAL PRODUCT – Output that is intended for, or required by, a customer, for supporting the development and deployment of an INTEROPERABLE ITEM for medical purpose.

NOTE: Common examples of INTEROPERABLE MEDICAL PRODUCTS include:

- a) An INTEROPERABLE ITEM supporting a medical purpose;
- b) An INTEROPERABLE MEDICAL SYSTEM (as a special case of INTEROPERABLE ITEM);
- c) An INTEROPERABILITY FRAMEWORK; and
- d) Work products or services related to the stakeholder activities in Annex A.

4.63 INTEROPERABLE MEDICAL SYSTEM – An ITEM consisting of one or more integrated (sub)-items (and is therefore decomposable) with a clinical INTENDED USE.

4.64 INTEROPERABLE USE SPECIFICATION – A summary of the important characteristics related to the context of use of the INTEROPERABLE MEDICAL PRODUCT that serves as input for determining ITEM INTEROPERABILITY SPECIFICATIONS.

4.65 ITEM INTEROPERABILITY SPECIFICATION– Collection of artifacts which are necessary and sufficient to:

- a) Define the item's interoperability-related functionality and interfaces;
- b) Integrate the INTEROPERABLE ITEM with or as part of another INTEROPERABLE ITEM and to carry out associated SAFETY and SECURITY ASSURANCE activities, including those that determine that the item's conditions of acceptability have been satisfied; and
- c) Specify controls that are required to ensure SAFETY and SECURITY during the deployment, operation, and maintenance of the item.

NOTE: Specification artifacts may include requirements, INTERFACE SPECIFICATIONS including INTERFACE CONTRACTS that capture conditions of acceptability, technical instructions, risk management information, and operating instructions, and constraints on the technical, clinical, and operating environment needed to achieve safety.

4.66 IT-NETWORK [INFORMATION TECHNOLOGY NETWORK] – A system or systems composed of communicating nodes and transmission links to provide physically linked or wireless transmission between two or more specified communication nodes.

Adapted by UL from IEC 60907:2009 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

NOTE: The scope of the IT-NETWORK in this document is defined by the responsible organization based on where the health software in the IT-NETWORK is located and the defined use of the IT-NETWORK. It can contain IT infrastructure, home health, or general computing components or systems not intended by design to be used in a healthcare setting. See also 7.2.3.2.

4.67 **MANUFACTURER** – Natural or legal person with responsibility for the design, manufacture, packaging, or labeling of equipment or adapting equipment regardless of whether these operations are performed by that person or on that person's behalf by a third party.

Adapted by UL from IEC 60601-1:2005+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.68 **MEDICAL ELECTRICAL EQUIPMENT [ME EQUIPMENT]** – Electrical equipment having an applied part or transferring energy to or from the **PATIENT** or detecting such energy transfer to or from the **PATIENT** and which is:

- a) Provided with not more than one connection to a particular supply mains; and
- b) Intended by its **MANUFACTURER** to be used:
 - 1) In the diagnosis, treatment, or monitoring of a **PATIENT**; or
 - 2) For compensation or alleviation of disease, injury or disability, or other condition.

NOTE 1: In some jurisdictions, ME Equipment may meet the definition of a medical device as defined in a particular jurisdiction.

NOTE 2: Equipment, when mentioned in this Standard, should be taken to include ME EQUIPMENT.

Adapted by UL from IEC 60601-1:2005+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.69 **MEDICAL ELECTRICAL SYSTEM [ME SYSTEM]** – Combination, as specified by its **MANUFACTURER**, of items of equipment, at least one of which is ME EQUIPMENT to be inter-connected by functional connection or by use of a multiple socket-outlet.

Adapted by UL from IEC 60601-1:2005+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.70 **OBJECTIVE** – Something toward which work is to be directed, a strategic position to be attained, or a purpose to be achieved, a result to be obtained, a product to be produced, or a service to be performed.

©IEC. This material is reproduced from ISO/IEC/IEEE 24765:2017 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.71 **OBJECTIVE EVIDENCE** – Data supporting the existence or verity of something.

NOTE: **OBJECTIVE EVIDENCE** can be obtained through observation, measurement, testing, or other means.

©ISO. This material is reproduced from ISO 14971-1:2007 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.72 ORGANIZATION – An entity with responsibility for placing on the market an INTEROPERABLE MEDICAL PRODUCT intended to be used in accordance with an INTEROPERABLE APPLICATION SPECIFICATION.

4.73 OPERATIONAL CONTEXT OF USE – A sub-context of the DEPLOYMENT CONTEXT OF USE related specifically to the point-of-care. ACTORS, processes, and health-delivery objectives and use cases that may impact the safe and secure use of the interoperability solution [generic term encompassing both ITEM and INTEROPERABILITY FRAMEWORK] as part of delivery of care to the PATIENT in INTEROPERABLE ITEM operation activities.

4.74 OPERATOR – Someone who, under authority of the RESPONSIBLE ORGANIZATION, controls the function of a machine, process or system in a specified manner.

NOTE 1: Different categories of OPERATOR include:

- a) A medical professional;
- b) A PATIENT if appropriately AUTHORIZED; and
- c) Service personnel if appropriately AUTHORIZED.

NOTE 2: An OPERATOR may take control or receive information from the machine, process, or system in a venue outside of the RESPONSIBLE ORGANIZATION (i.e., in home care).

4.75 OPERATOR IDENTITY/IDENTIFICATION – person-specific information used to distinguish an individual OPERATOR. OPERATOR IDENTIFIERS include username, badge number, and/or other identifiers generated by ADT or EMPI.

4.76 PASSWORD – Sensitive data is any critical SECURITY parameter that can compromise the use and SECURITY of the product such as passwords, keys, seeds for random number generators, AUTHENTICATION data., personally identifiable information and any data whose DISCLOSURE could jeopardize the SECURITY properties of the product.

4.77 PATIENT – Living being (person or animal) undergoing a medical, surgical or dental procedure.

NOTE: A PATIENT can be an OPERATOR.

©IEC. This material is reproduced from IEC 60601-1:2005+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.78 PATIENT ASSOCIATION – The process of establishing a PATIENT IDENTITY within an INTEROPERABLE ITEM for the purpose of identifying the PATIENT UNDER CARE.

4.79 PATIENT DISASSOCIATION – THE process of dissolving the logical relationship between an INTEROPERABLE ITEM and the PATIENT UNDER CARE previously established by a PATIENT ASSOCIATION process.

NOTE: PATIENT DISASSOCIATION will likely involve clearing PATIENT IDENTITY information and medical information linked to the PATIENT IDENTITY.

4.80 PATIENT EPISODE – The period of time between and PATIENT ASSOCIATION and PATIENT DISASSOCIATION during which the medical functions of the INTEROPERABLE ITEM are dedicated to care-giving for the PATIENT UNDER CARE.

4.81 PATIENT ID – The IDENTITY CLAIM of a PATIENT.

4.82 PATIENT IDENTIFICATION – The process of matching the PATIENT with the PATIENT IDENTIFIER information (see also PATIENT IDENTITY VERIFICATION).

4.83 PATIENT IDENTIFIER – An item of person-specific information used to distinguish an individual PATIENT. PATIENT IDENTIFIERS include name (given name, family name, and/or middle name), DOB, MRN, location, other IDENTIFIERS generated by ADT or EMPI.

4.84 PATIENT IDENTITY – Selected data elements associated with a PATIENT to uniquely identify that PATIENT among other patients within a Health Delivery Organization. Selected data elements (PATIENT IDENTIFIERS) – usually the name (given name, family name, and/or middle name), birth date, SSN, MRN, and sometimes the gender for a single PATIENT. PATIENT IDENTITY can be either verified or un-verified. (See PATIENT IDENTITY VERIFICATION)

4.85 PATIENT IDENTITY VERIFICATION – The process of matching PATIENT IDENTIFIERS that were input to the ME SYSTEM with a trusted source of PATIENT information (ADT/EMPI) to ensure the PATIENT is accurately IDENTIFIED.

4.86 PATIENT UNDER CARE – The particular PATIENT whose care is being addressed by the INTEROPERABLE ITEM while it is performing its clinical function.

4.87 PHYSIOLOGICAL ALARM CONDITIONS – ALARM CONDITION arising from a monitored PATIENT-related variable.

©IEC. This material is reproduced from IEC 60601-1-8:2006+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.88 POTENTIALLY HAZARD CONDITION – Conditions on the state of an INTEROPERABLE ITEM that may lead to a violation of the INTEROPERABLE ITEMS INTEROPERABILITY SPECIFICATION and/or indirectly to PATIENT harm.

NOTE 1: The term POTENTIALLY HAZARD CONDITION generalizes the notion of fault or root cause to address the fact that an INTEROPERABLE ITEM may not know the potential PATIENT harms associated with INTEROPERABLE MEDICAL SYSTEMs into which it is integrated. In such cases, the objectives of INTEROPERABLE ITEM development center around (a) developing technical specifications (captured in the INTEROPERABLE ITEM INTEROPERABILITY SPECIFICATION) that are appropriate for the INTENDED USE of the INTEROPERABLE ITEM and (b) mitigating POTENTIALLY HAZARD CONDITIONS that could lead to violations of the technical specification.

NOTE 2: A POTENTIALLY HAZARD CONDITION may represent a precondition for a RISK CONCERN.

4.89 PROTECTED HEALTH INFORMATION (PHI) – Protected health information (PHI), also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and any information about health status, provision of health care, or payment for health care that is created or collected by an entity, or their representative, and can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Source: <https://www.hhs.gov/hipaa/for-professionals/faq/2042/what-personal-health-information-do-individuals/index.html>

4.90 PROVENANCE – A record of the original source and chain of possession of data – combination of AUTHENTICITY, INTEGRITY, and no-repudiation for every entity that has processed the data – a chain of AUTHENTICATION OF INFORMATION.

4.91 REFERENCE ARCHITECTURE – An INTEROPERABILITY ARCHITECTURE for an INTEROPERABILITY FRAMEWORK that serves a schema and establishes constraints on INTEROPERABLE ITEM and INTEROPERABLE MEDICAL SYSTEM instances that are compliant with the INTEROPERABILITY FRAMEWORK.

4.92 RELEASE CRITERIA – Conditions and traceability relationships on the INTEROPERABLE ITEM INTEROPERABILITY SPECIFICATION, INTEROPERABLE ITEM realization and associated work products and DISCLOSURES that are to be achieved and substantiated with OBJECTIVE EVIDENCE before the INTEROPERABLE ITEM is released.

NOTE 1: RELEASE CRITERIA include primary conditions and relationships to be assessed when determining compliance to this Standard. RELEASE CRITERIA for the primary development activities of the Standard are presented in Annex F.

NOTE 2: Though not required by this Standard, release criteria may be used to inform the contents of a risk management file or the design of an ASSURANCE case for the INTEROPERABLE ITEM.

4.93 RESPONSIBILITY AGREEMENT – One or more documents that together fully define the responsibilities of all relevant stakeholders.

NOTE: This agreement can be a legal document, e.g. a contract.

©IEC. This material is reproduced from IEC 80001-1:2010 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.94 RESPONSIBLE ORGANIZATION – Entity accountable for the use and maintenance of an ME EQUIPMENT or an ME SYSTEM

NOTE 1: The accountable entity can be, for example, a hospital, an individual clinician or a layperson. In home use applications, the PATIENT, OPERATOR and RESPONSIBLE ORGANIZATION can be one and the same person.

NOTE 2: Education and training is included in “use.”

©IEC. This material is reproduced from IEC 60601-1:2005+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.95 RISK CONCERN – Potential adverse consequences and their occurrence as well as preconditions for them.

NOTE 1: See Annex H for a discussion of RISK CONCERN and the use of this term in this Standard.

NOTE 2: RISK CONCERNS are a generalization of ISO 14971 HAZARDOUS SITUATIONS that serve as drivers for the risk management process of this Standard in a manner analogous to the way that HAZARDOUS SITUATIONS serve as drivers for the ISO 14971 RISK MANAGEMENT PROCESS.

NOTE 3: A POTENTIALLY HAZARD CONDITION may represent a precondition for a RISK CONCERN.

©IEC. This material is reproduced from ISO/IEC 15026-3:2015 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.96 RISK CONTROL – Process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels.

©ISO. This material is reproduced from ISO 14971-1:2007 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.97 RISK MANAGEMENT – Systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk.

©ISO. This material is reproduced from ISO 14971-1:2007 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

4.98 SAFETY – Freedom from risk which is not tolerable.

©IEC. This material is reproduced from ISO/IEE Guide 51:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.99 SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVE [SSEPO] – An OBJECTIVE for the INTEROPERABLE ITEMS design, functionality, performance, and RISK CONTROLS that characterizes the INTEROPERABLE ITEM's intentions and obligations for achieving a SAFETY-, SECURITY-, AND ESSENTIAL PERFORMANCE – related property.

NOTE 1: INTEROPERABLE ITEM SSEOPs and EXTERNAL MEASURES are designed in concert with the intent that the INTEROPERABLE ITEM will be able to achieve its SSEPOs if the EXTERNAL MEASURES are achieved.

NOTE 2: EXTERNAL MEASURES represent obligations of the agents in the context of the INTEROPERABLE ITEM whereas SSEPOs represent obligations on INTEROPERABLE ITEM, given that EXTERNAL MEASURES are achieved.

NOTE 3: Section 8.3 provides candidate system-level SSEPOs to consider when forming INTEROPERABLE ITEM SSEPOs.

NOTE 4: SSEPOs are refined into requirements on the INTEROPERABLE ITEM, which are in turn refined to INTERFACE CONTRACTs that constrain the interactions of the INTEROPERABLE ITEM with its context over its INTEROPERABILITY INTERFACES.

4.100 SECURITY – The process of having acceptable levels of CONFIDENTIALITY, INTEGRITY, AUTHENTICITY and/or AVAILABILITY of product data and/or functionality through risk analysis.

4.101 TECHNICAL ALARM CONDITIONS – ALARM CONDITION arising from a monitored equipment-related or ALARM SYSTEM-related variable.

©IEC. This material is reproduced from IEC 60601-1-8:2006+A1:2012 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved

4.102 TECHNICAL SAFETY CONCEPT – Design and requirements for the realization of the FUNCTIONAL SAFETY CONCEPT in terms of the INTEROPERABILITY ARCHITECTURE and specific technologies used in the realization of the INTEROPERABLE ITEM.

Adapted by UL from ISO 26262-1:2011 with permission of the American National Standards Institute (ANSI) on behalf of the International Electrotechnical Commission. All rights reserved.

4.103 VALIDATION – Confirmation, through the provision of OBJECTIVE EVIDENCE, that the INTEROPERABLE ITEM is fit for purpose as expressed in the INTEROPERABLE USE SPECIFICATION and INTEROPERABLE APPLICATION SPECIFICATION.

4.104 VERIFICATION – Confirmation, through the provision of OBJECTIVE EVIDENCE, that specified requirements have been fulfilled.

©ISO. This material is reproduced from ISO 14971-1:2007 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

5 (Leadership) Management Responsibility

5.1 Top management shall provide evidence (see the NOTE in 5.2) of its commitment to assuring safe and secure interoperability by:

- a) Establishing policy for determining criteria for safe and secure interoperability;
- b) Ensuring that objectives (see 8.3) specific to the interoperability of its products with respect to SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE are established and met;
- c) Ensuring that processes required by this Standard are established and maintained; and
- d) Ensuring the AVAILABILITY of resources to effectively implement the processes.

5.2 Top management shall provide evidence (see NOTE) of its commitment to collaboration within the INTEROPERABILITY ECOSYSTEM, by ensuring that:

- a) Roles and needs of stakeholders in the INTEROPERABILITY ECOSYSTEM are determined and understood;
- b) Risks and opportunities that can affect the ability of stakeholders in the INTEROPERABILITY ECOSYSTEM to assure safe and secure interoperability are determined and addressed;
- c) Ongoing communication, including provision of timely DISCLOSURES (see 6.3) and focus on enhancing stakeholder collaboration is maintained.

NOTE: Evidence of management commitment may be maintained separately or relevant parts incorporated into a Risk Management or Quality Management System documentation.

6 Interoperability Information

6.1 Controlled information

6.1.1 The ORGANIZATION shall maintain controlled information (see NOTE 1) to:

- a) Provide evidence that the required processes are being established and carried out; and
- b) Provide evidence of compliance to this Standard.

Controlled information shall be maintained in a manner so as to be unambiguously referenced and accessed in a timely fashion when required.

NOTE 1: Controlled information may be maintained in documents or in electronic information management systems. Information can be maintained in distributed repositories, including information contained within the INTEROPERABLE MEDICAL PRODUCT (e.g., machine readable information).

NOTE 2: Controlled information required by this Standard can be maintained as part of other documentation required, for example, by a MANUFACTURER'S quality management system.

6.2 INTEROPERABILITY FILE

6.2.1 One or more files shall be established and maintained, either containing or referencing information for demonstrating compliance with the requirements of this Standard, including required processes as applicable.

6.2.2 For each type or family of INTEROPERABLE MEDICAL PRODUCTS the content of the file(s) shall include, but is not limited to:

- a) Description of the interoperability of the INTEROPERABLE MEDICAL PRODUCT;
- b) Scope of the INTEROPERABLE ENVIRONMENT and anticipated EXTERNAL PRODUCTS;
- c) INTEROPERABLE USE SPECIFICATIONS for the INTEROPERABLE MEDICAL PRODUCT (see 9.1.4);
- d) INTEROPERABILITY SPECIFICATIONS for the INTEROPERABLE MEDICAL PRODUCT;
- e) Description of the interoperability of anticipated and specified EXTERNAL PRODUCTS;
- f) INTEROPERABLE APPLICATION SPECIFICATION for the INTEROPERABLE MEDICAL PRODUCT (see 13.2); and
- g) Information necessary for demonstrating traceability and adequacy of SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE evidence with respect to interoperability-related RELEASE CRITERIA for specified application.

NOTE: See Annex C for more information.

6.3 DISCLOSURE and communication

6.3.1 General

6.3.1.1 Information required for assuring safe and secure interoperability for any specified application of the INTEROPERABLE MEDICAL PRODUCT shall be disclosed as appropriate to relevant stakeholders in the INTEROPERABILITY ECOSYSTEM.

6.3.1.2 Disclosed information shall be communicated through appropriate means.

NOTE: Appropriate means of communicating disclosed information can include:

- a) Accompanying documents containing information on basic SAFETY and ESSENTIAL PERFORMANCE (see the Standard for Medical Electrical Equipment – Part 1: General Requirements for Basic Safety and Essential Performance, IEC 60601-1);
- b) Autonomous machine-to-machine communication;
- c) Human readable disclosures conveyed through software; and

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents
Document Sharing Hub

d) Business interfaces.

6.3.2 Information to be disclosed

6.3.2.1 Information disclosed to stakeholders in the INTEROPERABILITY ECOSYSTEM shall include, as appropriate, information about the PRODUCT required by the stakeholder for:

- a) Correct use of the INTEROPERABLE MEDICAL PRODUCT for a specified application within the INTEROPERABILITY ECOSYSTEM (see 13.2.1);
- b) Technical integration of the INTEROPERABLE MEDICAL PRODUCT into other products or systems within the INTEROPERABILITY ECOSYSTEM;
- c) Performance of integration testing of the INTEROPERABLE MEDICAL PRODUCT when integrated into other products or systems within the INTEROPERABILITY ECOSYSTEM;
- d) Performance of provisioning and installation of the INTEROPERABLE MEDICAL PRODUCT when integrated into other products or systems within the INTEROPERABILITY ECOSYSTEM;
- e) Operating and maintenance activities related to the INTEROPERABLE MEDICAL PRODUCT when integrated into other products or systems within the INTEROPERABILITY ECOSYSTEM; and
- f) Decommissioning and disposal activities related to the INTEROPERABLE MEDICAL PRODUCT within the INTEROPERABILITY ECOSYSTEM.

6.3.2.2 Information disclosed to a provider of EXTERNALLY SOURCED PRODUCT (see Section 10, Interoperability of Externally Sourced Products) shall include applicable information required by the ORGANIZATION for:

- a) Determining INTEROPERABLE USE SPECIFICATIONS (see 9.2) relevant to the correct use of the EXTERNALLY SOURCED PRODUCT when integrated into the INTEROPERABLE MEDICAL PRODUCT or used with the INTEROPERABLE MEDICAL PRODUCT;
- b) Technical integration of the EXTERNALLY SOURCED PRODUCT into the INTEROPERABLE MEDICAL PRODUCT;
- c) Integration testing of the EXTERNALLY SOURCED PRODUCT when integrated into the INTEROPERABLE MEDICAL PRODUCT;
- d) Provisioning and installation of the EXTERNALLY SOURCED PRODUCT when integrated into the INTEROPERABLE MEDICAL PRODUCT;
- e) Operating and maintenance activities related to the EXTERNALLY SOURCED PRODUCT when integrated into the INTEROPERABLE MEDICAL PRODUCT or used with the INTEROPERABLE MEDICAL PRODUCT; and
- f) Decommissioning and disposal activities related to the EXTERNALLY SOURCED PRODUCT when integrated into the INTEROPERABLE MEDICAL PRODUCT or used with the INTEROPERABLE MEDICAL PRODUCT.

NOTE: See Annex D for more information.

6.3.3 Required DISCLOSURE

6.3.3.1 The INTEROPERABLE MEDICAL PRODUCT'S INTEROPERABLE APPLICATION SPECIFICATION (see 13.2) shall be disclosed as part of market release of the INTEROPERABLE MEDICAL PRODUCT or provision of the INTEROPERABLE MEDICAL PRODUCT for specified application.

6.3.3.2 DISCLOSURES for purchasing or acquisition of EXTERNALLY SOURCED PRODUCT, shall include as appropriate:

- a) Specifications for EXTERNALLY SOURCED PRODUCT; and
- b) RESPONSIBILITY AGREEMENT (See Section 10).

7 Interoperability Management

7.1 Scope of interoperability management

7.1.1 The ORGANIZATION shall determine the scope of interoperability of its INTEROPERABLE MEDICAL PRODUCTS and potential application by the INTEROPERABILITY ECOSYSTEM that affect the ability to assure safe and secure interoperability. (See NOTE 1 of 7.1.2.)

7.1.2 The ORGANIZATION shall monitor information relevant to the scope, including any emergent aspects, after deployment and during operation of the INTEROPERABLE MEDICAL PRODUCT by the INTEROPERABILITY ECOSYSTEM that incorporates its INTEROPERABLE MEDICAL PRODUCTS.

NOTE 1: The scope of interoperability management should include consideration of the roles played by the organization in an INTEROPERABILITY ECOSYSTEM, as well as the manner in which its INTEROPERABLE MEDICAL PRODUCTS are used in the INTEROPERABLE ENVIRONMENT.

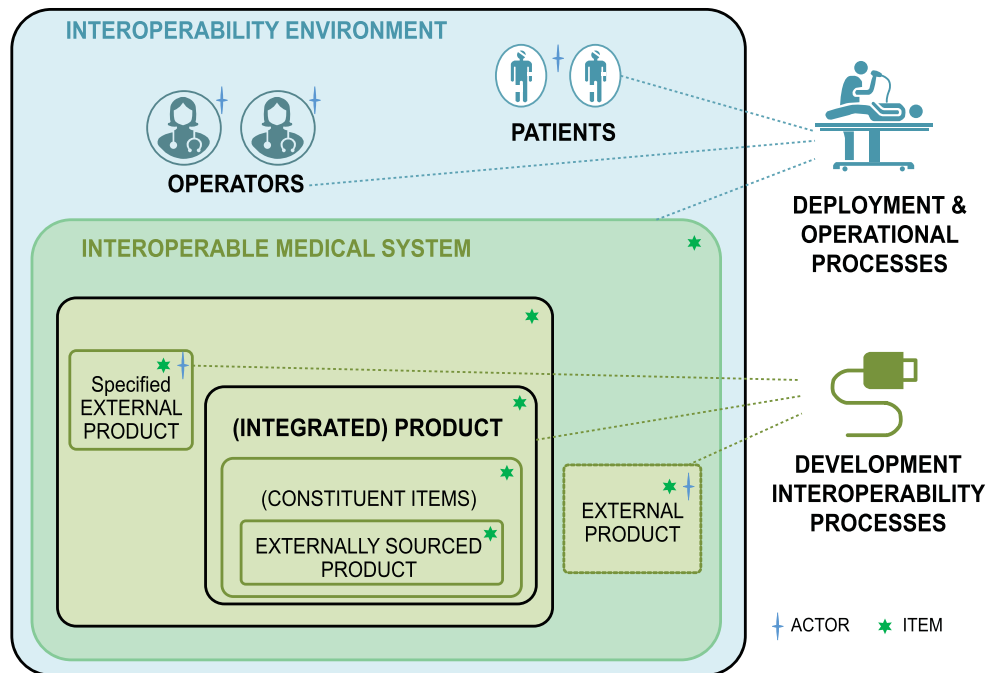
NOTE 2: See Annex A for more information on the various potential stakeholders and their roles in an INTEROPERABILITY ECOSYSTEM.

7.2 The INTEROPERABLE ENVIRONMENT

7.2.1 The ORGANIZATION shall determine the scope of the INTEROPERABLE ENVIRONMENT for its INTEROPERABLE MEDICAL PRODUCTS. See Figure 7.1 for a schematic representation of the INTEROPERABLE ENVIRONMENT.

NOTE: The INTEROPERABLE MEDICAL PRODUCT may be in the form of a single contained INTEROPERABLE ITEM, or a platform comprising a collection of reusable INTEROPERABLE ITEMS, or specific configurations of items or instantiations of platforms for specified clinical applications.

Figure 7.1
INTEROPERABLE ENVIRONMENT ontology



su3403

7.2.2 In determining the INTEROPERABLE ENVIRONMENT, the following shall be considered:

- Other INTEROPERABLE MEDICAL PRODUCTS that incorporate or interact with the ORGANIZATION'S INTEROPERABLE MEDICAL PRODUCTS and their interoperability needs;
- EXTERNAL PRODUCTS, including anticipated and specified EXTERNAL PRODUCTS, needed for application of the INTEROPERABLE MEDICAL PRODUCT;
- EXTERNALLY SOURCED PRODUCTS that are incorporated into the ORGANIZATION'S INTEROPERABLE MEDICAL PRODUCTS and information, including disclosed information about them; and
- Any other products or services, including emergent aspects, in the INTEROPERABILITY ECOSYSTEM relevant to the ability to assure safe and secure interoperability.

7.2.3 Based on the above, the INTEROPERABLE ENVIRONMENT shall be determined, including the external infrastructure and resources that are relevant to the ORGANIZATION'S ability to assure safe and secure interoperability.

7.3 Processes for assuring safe and secure interoperability

7.3.1 The ORGANIZATION shall determine the processes that assure safe and secure interoperability.

7.3.2 When determining the processes, the following shall be considered:

- The scope of interoperability management referred to in 7.1;
- The INTEROPERABLE ENVIRONMENT referred to in 7.2;
- The INTEROPERABLE MEDICAL PRODUCTS of the ORGANIZATION; and
- Risk management process for assuring safe and secure interoperability (see 8.2).

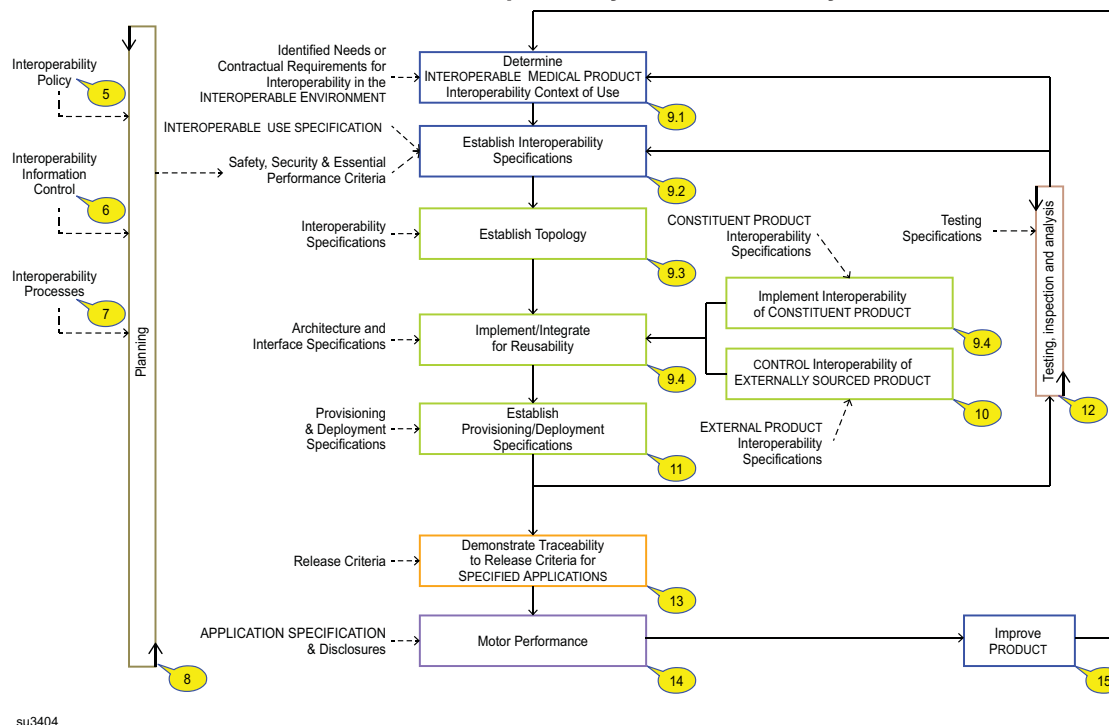
7.3.3 All of the requirements of this Standard shall apply when they are applicable within the determined scope. Justification shall be provided for any requirement that is determined as not applicable.

NOTE: See Annex B for more information.

7.3.4 The methods used shall be suitable to the type and scope of the INTEROPERABLE MEDICAL PRODUCT.

A schematic representation of interoperability realization processes (along with corresponding section numbers of this Standard) is shown in Figure 7.2. Depending on the type of INTEROPERABLE MEDICAL PRODUCT, individual elements of realization can have varying emphasis. Realization activities can be performed iteratively or in multiple steps as appropriate to the INTEROPERABLE MEDICAL PRODUCT.

Figure 7.2
Schematic of interoperability realization lifecycle



su3404

7.3.5 Information on the ORGANIZATION'S interoperability realization processes shall be controlled and maintained. (See 6.1)

NOTE: Controlled information on processes for assuring safe and secure interoperability may be maintained separately or relevant parts incorporated into the ORGANIZATION'S Risk Management or Quality Management System documentation.

7.3.6 Compliance with this Standard may only be claimed if the requirements determined as not being applicable do not affect the ORGANIZATION'S ability to assure safe and secure interoperability.

8 Interoperability Realization Processes

8.1 Interoperability realization planning

8.1.1 The ORGANIZATION shall plan the realization of interoperability for the INTEROPERABLE MEDICAL PRODUCT, including:

- a) Design, development, and implementation of interoperability for the INTEROPERABLE MEDICAL PRODUCT (see Section 9, Design, Development and Implementation of Interoperability);
- b) Control of EXTERNALLY SOURCED PRODUCTS (see Section 10, Interoperability of Externally Sourced Products);
- c) Provisioning and deployment of the INTEROPERABLE MEDICAL PRODUCT within the INTEROPERABLE ENVIRONMENT (see Section 11, Provisioning, Deployment, and Operation);
- d) Testing for interoperability (see Section 12, Testing and Review);
- e) Release of interoperability for specified application (see Section 13, Traceability and Release);
- f) Monitoring and incident response during use of its INTEROPERABLE MEDICAL PRODUCT within the INTEROPERABLE ENVIRONMENT (see Section 14, Interoperability Performance Monitoring and Control of Changes);
- g) Improvement of INTEROPERABLE MEDICAL PRODUCT (see Section 15, Improvement of Processes);
- h) RISK MANAGEMENT (see 8.2); and
- i) Communication with stakeholders in the INTEROPERABILITY ECOSYSTEM, including DISCLOSURE (see 6.3).

NOTE: Annex E contains a more detailed description of the steps in the interoperability realization process.

8.1.2 Realization activities shall ensure that:

- a) Interoperability objectives (see 8.3) are met by:
 - 1) Identifying applicable interoperability properties (see 8.3) relating to interoperability objectives;
 - 2) Establishing SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE criteria with respect to the interoperability properties; and

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM  Documents
Document Sharing Hub

- 3) Ensuring that the INTEROPERABLE MEDICAL PRODUCT meets the SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE criteria.
- b) Ensuring that the INTEROPERABLE MEDICAL PRODUCT meets RELEASE CRITERIA (see Section 13, Traceability and Release); including criteria for risk acceptance;
- c) Usability of INTEROPERABLE MEDICAL PRODUCT interoperability is acceptable, including ensuring that:
 - 1) Unsafe control actions are avoided, such as when settings and configurations are changed;
 - 2) Communications to and from the INTEROPERABLE ENVIRONMENT occur in a timely and correct fashion; and
 - 3) Appropriate information on the current state of the INTEROPERABLE MEDICAL PRODUCT is provided to OPERATORS and EXTERNAL PRODUCTS, as appropriate.
- d) SECURITY of INTEROPERABLE MEDICAL PRODUCT interoperability is acceptable, including ensuring that:
 - 1) Cyber and physical threats are IDENTIFIED;
 - 2) Vulnerabilities are IDENTIFIED; and
 - 3) Mitigations are IDENTIFIED, implemented and tested.

NOTE 1: See Annex J for more information.

NOTE 2: See Annex K for more information.

8.2 RISK MANAGEMENT

8.2.1 RISK MANAGEMENT shall be incorporated throughout interoperability realization and ensure that:

- a) Potential HAZARDOUS SITUATIONS associated with the use or reuse of the INTEROPERABLE MEDICAL PRODUCT in the INTEROPERABLE ENVIRONMENT and related POTENTIALLY HAZARDOUS CONDITIONS of the INTEROPERABLE MEDICAL PRODUCT are IDENTIFIED (See NOTE 1);
- b) The level of risk associated with each HAZARDOUS SITUATION or the POTENTIALLY HAZARDOUS CONDITIONS is estimated based on the probability of occurrence and the severity of harm that may result;
- c) The level of risk is evaluated using risk acceptance criteria;
- d) RISK CONTROL requirements that reduce risk sufficiently to meet risk acceptance criteria are IDENTIFIED, implemented, and are effective;
- e) Controls required for specified application are included in DISCLOSURES (see 6.3), as appropriate include information on POTENTIALLY HAZARDOUS CONDITIONS; and
- f) Information from integration and application of the INTEROPERABLE MEDICAL PRODUCT in the INTEROPERABLE ENVIRONMENT that is relevant to RISK MANAGEMENT is monitored and reviewed for impact on previously conducted RISK MANAGEMENT activities.

NOTE 1: In order to identify HAZARDOUS SITUATIONS, the organization needs to have a good understanding of the clinical context of use (see 9.1.2). For general purpose INTEROPERABLE MEDICAL PRODUCTS, specific information on clinical use may not be AVAILABLE. In such cases, the technical context of use (see 9.1.3) should be analyzed and POTENTIALLY HAZARDOUS CONDITIONS of the product IDENTIFIED. These may include operating states in which the product fails to perform or goes outside specified performance limits. Risk management activities may then be performed with respect to POTENTIALLY HAZARDOUS CONDITIONS. Both HAZARDOUS SITUATIONS and POTENTIALLY HAZARDOUS CONDITIONS can be addressed as part of RISK CONCERNS (see Annex E).

NOTE 2: See Annex H for more information.

8.3 Candidate SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVES

8.3.1 General

8.3.1.1 In order to support interoperability, the candidate risk concerns and candidate SSEPOS shall be considered in the RISK MANAGEMENT and development life-cycle for the item.

8.3.2 Clinical properties

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

8.3.2.1 Semantic interoperability

8.3.2.1.1 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 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.

8.3.2.1.2 The following INTEROPERABLE MEDICAL SYSTEM-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- 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.

8.3.2.2 PATIENT IDENTITY

8.3.2.2.1 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.

8.3.2.2.2 The following interoperable system-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- a) While an INTEROPERABLE MEDICAL SYSTEM is supporting care-giving for a PATIENT, all constituents of INTEROPERABLE MEDICAL SYSTEM that have a PATIENT IDENTITY storage capability, hold an IDENTIFIER corresponding to 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 constituents 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.

8.3.2.3 OPERATOR ID, AUTHENTICATION, and AUTHORIZATION

8.3.2.3.1 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.

8.3.2.3.2 The following INTEROPERABLE MEDICAL SYSTEM-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- 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:

a) Is traceable to the OPERATOR; and

b) 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.

8.3.2.4 Item Id, AUTHENTICATION, and AUTHORIZATION

8.3.2.4.1 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.

8.3.2.4.2 The following INTEROPERABLE MEDICAL SYSTEM-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- 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.

8.3.3 Engineering properties

NOTE: See Annex P for guidance that supports these objectives.

8.3.3.1 INTEROPERABILITY ITEM Connectivity

8.3.3.1.1 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 SSEPOs.
- 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.

8.3.3.1.2 The following INTEROPERABLE MEDICAL SYSTEM-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- 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.

8.3.3.2 Safe States

8.3.3.2.1 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.

8.3.3.2.2 The following INTEROPERABLE MEDICAL SYSTEM-level objectives shall be considered in the formulation of the T SSEPOs:

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.

8.3.3.3 Time Synchronization

8.3.3.3.1 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.

8.3.3.3.2 The following interoperable system-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOs:

- 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.

8.3.3.4 Shared Resources, and Data/Time Partitioning

8.3.3.4.1 The following INTEROPERABLE MEDICAL SYSTEM-level risk concerns shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- a) Execution of interoperability-related functions realizing ESSENTIAL PERFORMANCE or 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 ESSENTIAL PERFORMANCE or 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.

8.3.3.4.2 The following interoperable system-level objectives shall be considered in the formation of the INTEROPERABLE ITEM SSEPOS:

- 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 SSEPOS, 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 SSEPOS.
- d) The INTEROPERABLE MEDICAL SYSTEM and its CONSTITUENT INTEROPERABLE ITEMS signal current or impending failure or degradation of its medical function or violation of SSEPOS due to lack of access or scarcity of shared resources.

8.3.4 Service properties

8.3.4.1 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 Q for detailed requirements.

8.3.5 SECURITY properties

8.3.5.1 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.

9 Design, Development and Implementation of Interoperability

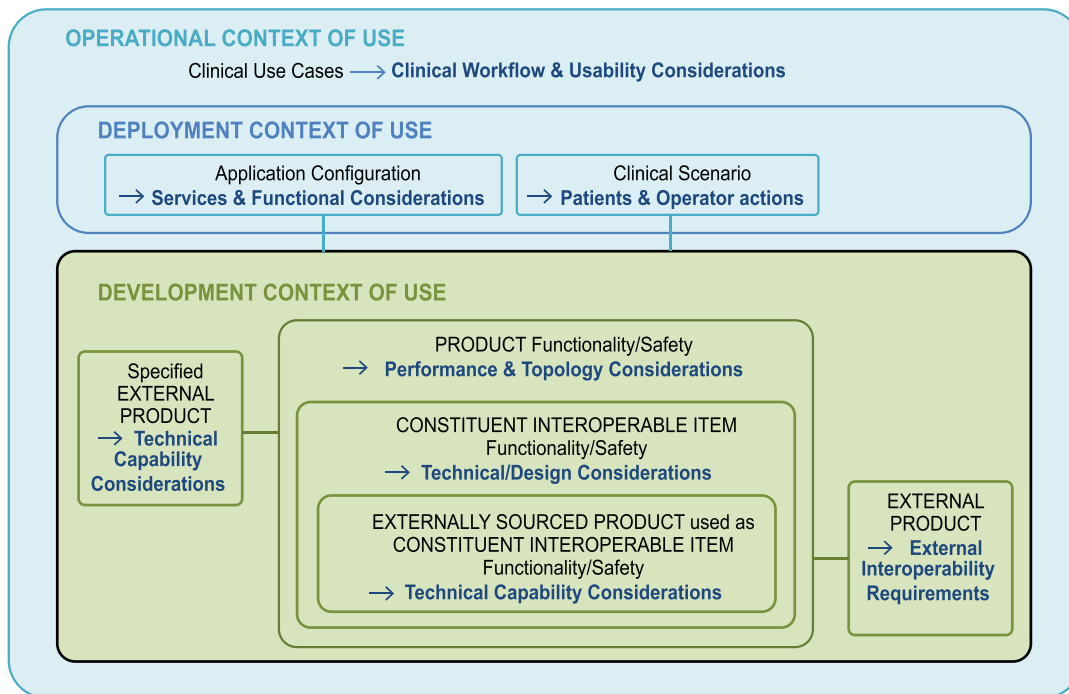
9.1 Interoperability context of use

9.1.1 General

9.1.1.1 The ORGANIZATION shall determine the interoperability context of use and reuse for the INTEROPERABLE MEDICAL PRODUCT. Figure 9.1 schematically shows the potential contexts of use and their relationships.

NOTE: Depending on the nature of the INTEROPERABLE MEDICAL PRODUCT, the context of use or reuse may include deployment or development aspects or both.

Figure 9.1
Interoperability contexts of use



su3405

9.1.2 Deployment aspects in context of use

9.1.2.1 When applicable, interoperability aspects relevant to deployment shall include:

- Intended clinical or medical uses and situations for which the INTEROPERABLE MEDICAL PRODUCT is intended to be deployed, including anticipated activities for the clinical workflows within which the INTEROPERABLE MEDICAL PRODUCT is intended to be used. (See NOTE 1.)
- Relevant clinical indications and scenarios and the associated application configurations of the INTEROPERABLE MEDICAL PRODUCT required for them.

c) Operations aspects such as services and functionality required for the INTEROPERABLE MEDICAL PRODUCT for set up, preparation or integration, and deployment prior, during, after clinical use including:

- 1) The type or category of clinical staff (See NOTE 2);
- 2) Potential changes or new/novel equipment or workflow that could improve the clinical workflow in the future; and
- 3) Benefits of the proposed clinical workflow.

d) Impact of the INTEROPERABLE MEDICAL PRODUCT on the clinical workflow when used as intended, including usability considerations.

e) Interoperability aspects for assuring that any patients associated with the INTEROPERABLE MEDICAL PRODUCT are correctly IDENTIFIED and are consistent with care-giving intent (i.e., care is being provided to the "right PATIENT").

f) Interoperability aspects for assuring that any OPERATORS associated with the INTEROPERABLE MEDICAL PRODUCT are correctly IDENTIFIED and trusted to control the INTEROPERABLE MEDICAL PRODUCT.

g) Interoperability aspects for providing and controlling access based on OPERATOR roles.

h) HAZARDOUS SITUATIONS, breach of SECURITY, or use ERROR (including foreseeable misuse) related to interoperability (see NOTE 3), that could potentially be introduced during APPLICATION of the INTEROPERABLE MEDICAL PRODUCT and potential resulting harm.

i) Potential risk controls, such as OPERATOR actions AVAILABLE in the DEPLOYMENT CONTEXT OF USE.

j) Any other aspects of interactions with the INTEROPERABLE MEDICAL PRODUCT in the deployment context relevant to assuring safe and secure interoperability.

NOTE 1: It might be helpful to consider the current state standard of clinical practice, the clinical challenge/function intended to be addressed by the INTEROPERABLE MEDICAL PRODUCT, as well as the instructions for operation and management of the components according to clinical lifecycle phases.

NOTE 2: Examples of clinical staff include surgeons, intensivists, anesthesia providers, chief nurse, nursing assistant, respiratory therapists, etc.

NOTE 3: A fault tree or similar analysis may be used to provide a more detailed representation of potential HAZARDOUS SITUATIONS arising at various points in the clinical workflow or through combinations of conditions from multiple points in the workflow.

NOTE 4: See Annex L for more information.

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents
Document Sharing Hub

9.1.3 Development aspects in context of use

9.1.3.1 When applicable, aspects relevant to development shall include:

- a) Product boundaries at the granularity at which product interoperability will occur;
- b) EXTERNAL PRODUCTS and technical processes in the INTEROPERABLE ENVIRONMENT for the product (see NOTE 1);
- c) Semantic interoperability aspects, including data elements, nomenclature and frameworks for IDENTIFICATION of EXTERNAL PRODUCTS;
- d) Interoperability needs of the INTEROPERABLE ENVIRONMENT, including EXTERNAL PRODUCTS, including:
 - 1) Known or contractually provided requirements for interoperable functions of the product, and
 - 2) Known or contractually provided requirements for interoperability performance levels and interface characteristics of the product.
- e) Product interfaces with the INTEROPERABLE ENVIRONMENT, including with EXTERNAL PRODUCTS, patients, and, operators with which the product interfaces, and their characteristics;
- f) Functional and performance constraints of the INTEROPERABLE ENVIRONMENT (see NOTE 2);
- g) POTENTIALLY HAZARDOUS CONDITIONS of the product that could result in potential HAZARDOUS SITUATIONS in the INTEROPERABLE ENVIRONMENT, including those resulting from:
 - 1) Control actions of the product;
 - 2) Data or operational instructions communicated to operators by the product; and
 - 3) Data and commands communicated to EXTERNAL PRODUCTS by the product.
- h) Usability and SECURITY considerations in the INTEROPERABLE ENVIRONMENT;
- i) Potential risk controls, such as actions by EXTERNAL PRODUCTS AVAILABLE in the DEVELOPMENT CONTEXT OF USE; and
- j) Any other aspects of interactions with the product in the technical context relevant to assuring safe and secure interoperability.

NOTE 1: EXTERNAL PRODUCTS may include existing technology platforms, electronic medical records systems, pharmacy management systems, and other interoperable products used in the clinical environment.

NOTE 2: Interoperability constraints may include data constraints, temporal ordering constraints, input/output relationships, exceptional behaviors, fault propagations, mitigations, and appropriate IDENTIFICATION of attributes relevant to interoperability of the INTEROPERABLE MEDICAL PRODUCT within the INTEROPERABLE ENVIRONMENT.

Also see E1.1.2 and E1.1.3.

9.1.4 INTEROPERABLE USE SPECIFICATION

9.1.4.1 Information on the interoperability context of use and reuse shall be controlled and maintained as INTEROPERABLE USE SPECIFICATIONS and include:

- a) A summary description of the scope of interoperability of the INTEROPERABLE MEDICAL PRODUCT;
- b) A summary description of the INTEROPERABLE ENVIRONMENT (including EXTERNAL PRODUCTS) within which the INTEROPERABLE MEDICAL PRODUCT is intended to be used; and
- c) Important constraints of the interoperability of the INTEROPERABLE MEDICAL PRODUCT (see 9.1.2 and 9.1.3), including constraints related to SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVES (see 8.3) and RELEASE CRITERIA with respect to them (see 13.1.2 (a)).

NOTE 1: INTEROPERABLE USE SPECIFICATION may include statements of user needs or specific market requirements for the product. In some cases this information may be captured in a Market Requirements Document.

NOTE 2: The INTEROPERABLE USE SPECIFICATION is an input to interoperability realization activities and in determining the INTEROPERABLE APPLICATION SPECIFICATION (see Section 13). Statements related to INTENDED USE may be included in the INTEROPERABLE APPLICATION SPECIFICATION.

9.2 INTEROPERABILITY SPECIFICATION

9.2.1 The ORGANIZATION shall establish specifications for INTEROPERABLE ITEMS that comprise the INTEROPERABLE MEDICAL PRODUCT related to the scope and purpose of the interoperability of the INTEROPERABLE MEDICAL PRODUCT.

NOTE: Interoperability specifications may be developed and refined as realization activities for the INTEROPERABLE MEDICAL PRODUCT proceed (see Sections 9 – 11).

9.2.2 INTEROPERABLE ITEM INTEROPERABILITY SPECIFICATIONS shall include specifications related to the context of use and reuse determined in 9.1, including:

- a) Interoperability functional and performance specifications required to meet the INTEROPERABLE USE SPECIFICATIONS (see 9.1.4) of the INTEROPERABLE MEDICAL PRODUCT, including:
 - 1) Specifications derived from the clinical interoperability aspects determined for the INTEROPERABLE MEDICAL PRODUCT (see 9.1.2), including the clinical purpose and function and actual conditions under which the product is intended to be used; and
 - 2) Specifications derived from technical interoperability aspects determined for the INTEROPERABLE MEDICAL PRODUCT (see 9.1.3), including application, function, and performance of the INTEROPERABLE MEDICAL PRODUCT and situations in which the INTEROPERABLE MEDICAL PRODUCT is intended to be integrated into operational contexts.
- b) Specifications or criteria for meeting interoperability SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVES (see 8.3) and the role of the INTEROPERABLE MEDICAL PRODUCT in supporting interoperability in INTEROPERABLE MEDICAL SYSTEMS;
- c) Specifications to meet statutory and regulatory requirements applicable to the INTEROPERABLE MEDICAL PRODUCT;
- d) Specifications to meet external references (See NOTE);

- e) Specifications arising from RELEASE CRITERIA;
- f) Specifications arising from risk controls or risk acceptance criteria; and
- g) Any other specifications related to meeting SAFETY, SECURITY, AND ESSENTIAL PERFORMANCE OBJECTIVES of the INTEROPERABLE MEDICAL PRODUCT in the INTEROPERABLE ENVIRONMENT.

NOTE: External references may include external reference architectures, nomenclature frameworks, design standards or codes of practice.

9.2.3 INTEROPERABLE ITEM INTEROPERABILITY SPECIFICATIONS shall include contractual or other requirements of the INTEROPERABLE ENVIRONMENT; including those related to:

- a) Design, development, and integration of interoperability function and performance; and technical characteristics of the INTEROPERABLE MEDICAL PRODUCT required by the INTEROPERABLE ENVIRONMENT;
- b) Provisioning and deployment of the INTEROPERABLE MEDICAL PRODUCT required for application in the INTEROPERABLE ENVIRONMENT;
- c) Installation, maintenance, monitoring and incident response during operation of the INTEROPERABLE MEDICAL PRODUCT in the INTEROPERABLE ENVIRONMENT;
- d) Testing, including qualification and acceptance testing for the INTEROPERABLE MEDICAL PRODUCT; and
- e) Traceability to RELEASE CRITERIA specifically required by the INTEROPERABLE ENVIRONMENT.

9.2.4 INTEROPERABILITY SPECIFICATIONS shall be adequate for realization purposes, complete, and unambiguous, and include as applicable:

- a) INTEROPERABLE USE SPECIFICATION (see 9.1.4);
- b) Architecture, interface, and INTERACTION SPECIFICATIONS (see 9.3);
- c) Sourcing specifications (see Section 10, Interoperability of Externally Sourced Products);
- d) Provisioning and deployment specifications (see Section 11, Provisioning, Deployment, and Operation); and
- e) INTEROPERABLE APPLICATION SPECIFICATION (see Section 12).

9.2.5 Conflicting specifications shall be resolved.