IEEE SA
STANDARDS ASSOCIATION

IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety, Security

STANDARDS

ULNORM.COM : Click to view the full PDF of UL 2933 2024

IEEE Engineering in Medicine and Biology Society

Developed by the
IEEE Engineering in Medicine and
Biology Standards Committee

IEEE Std 2933™-2024/UL 2933:2024

IEEE

IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety, and Security

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Developed by the

IEEE Engineering in Medicine and Biology Standards Committee
of the
IEEE Engineering in Medicine and Biology Society

Approved 6 June 2024

IEEE SA Standards Board

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
Three Park Avenue
New York, New York 10016-5997, USA

All rights reserved.

Abstract: A framework with TIPPSS principles (trust, identity, privacy, protection, safety, and security) for Clinical Internet of Things (IoT) data and device interoperability is established in this standard. This includes wearable clinical IoT and interoperability with healthcare systems including electronic health records (EHR), electronic medical records (EMR), other Clinical IoT devices, in-hospital devices, and future devices and connected healthcare systems.

Keywords: 2933, CIoT, clinical, clinical IoT, data, device, identity, information, patient, privacy, protection, safety, security, software, system, TIPPSS, trust

This word cloud was created from the content in this standards document, showing the emphasis on significant topics:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

ULSE Inc.
1603 Orrington Ave., Suite 2000, Evanston, IL 60201

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

Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc. and ULSE, Inc.
All rights reserved. Published 30 September 2024. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-1257-5 STD27324
Print: ISBN 979-8-8557-1258-2 STDPD27324

IEEE prohibits discrimination, harassment, and bullying.
For more information, visit https://www.ieee.org/about/corporate/governance/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright © 2024 IEEE and ULSE. All rights reserved.

Commitments for amendments

This Standard is issued jointly by the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and ULSE Inc. (ULSE) Comments or proposals for revisions or any part of the standard may be submitted to IEEE and/or ULSE at any time. Revisions to this Standard will be made only after processing according to the Standards development procedures of IEEE and ULSE.

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

Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on IEEE standards should be submitted using the Contact Us form.[2]

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

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

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

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic,

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Copyright © 2024 IEEE and ULSE. All rights reserved.

and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Copyright © 2024 IEEE and ULSE. All rights reserved.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system.[3] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[4]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual,

[3] Available at: https://development.standards.ieee.org/myproject-web/public/view.html.
[4] Available at: https://standards.ieee.org/thank-you/contact/.

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[5] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[6] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the IEEE SA Patent Policy.[7]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with the submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that

[5] Available at: https://standards.ieee.org/about/contact.
[6] Available at: https://standards.ieee.org/standard/
[7] Available at: https://standards.ieee.org/about/sasb/patcom/materials.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Participants

At the time this draft standard was completed, the P2933 Working Group had the following membership:

Florence D. Hudson, *Chair*
Mitchell Parker, *Vice Chair*
William Harding, *Vice Chair*
Kenneth Fuchs, *Secretary*

Michael Shea, *Trust and Identity Subgroup Co-Chair*
Sherri Douville, *Trust and Identity Subgroup Co-Chair*
Nada Philip, *Privacy Subgroup Chair*
Axel Wirth, *Protection, Safety and Security Subgroup Chair*
Konstantinos Katzis, *Use Cases and Human Factors Co-Chair*
Dane Stout, *Use Cases and Human Factors Co-Chair*
Neil Petroff, *Integrated Systems Design Subgroup Co-Chair*
Kim Reisinger, *Integrated Systems Design Subgroup Co-Chair*
Orlando Lopez, *Data & Device Validation and Interoperability Subgroup Chair*

Femi (Olufemi) Adeluyi
Brian Ahier
Bob Aiello
Karen Alexander
Wesley Allen
Prashanth Areddy
Justin Armstrong
Katherine August
Moussa Ayyash
Mohammad Bajwa
Pradeep Balachandran
Viesturs Bambans
Judy L. Barkal
Alan Barnes
John Bishop
Bernd Blobel
Douglas Bogia
Nyteisha Bookert
Jeffrey Boyd
Mollie Breen
Robert Bussey
Braulio Cabral
Zulema Caldwell
Colin Cantlie
Carole C. Carey
Brian Carlsen
Jennifer Cawthra
Cheng Chang
Shane (Hsun-Hsien) Chang
Stephen Chavez
Jia Chen
Olivia Choudhury
Malcolm Clarke
Robert Clint
Bernie Cohen
Deniz Coskun
Michael Cowan
Michael Curley
Maria Grazia D'Elia
Doug DeShazo
Jonathan Desmond
Emily Dillon
Danielle Doyen
Pedro Duque
Kurt Elliason
Anura Fernando
Barbara Filkins
Rodolfo Fiorini
Stefanie Freitag
Marcus Garbe
Lina Garces
Lukas Geissmann
Maeva Ghonda
Amos Gichamba
Ben Goodman
John Griffith
Peter Gunter
Vicky Hailey
Sujoy Ghosh Hajra
George Harper
Paul Harris
Tyrone Heggins
Marco Hernandez
Karen Herrington
Justin Heyl
Pamella Howell
Craig Hyps
Mike Jaffe
Amit Jain
Ganesh Jayaramakrishnan
Miro Käch
Erwin Karincic
Emerson Keenan
Colin Kennedy
Dan Kernan
Edmund Kienast
Irene Kilanioti
Michael J. Kirwan
Jeff Klaben
Jennifer Kleinhans
David Knox
Sergey Krivenko
Stanislav Kryvenko
Antonios Lalas
Cliff Lee
Duckki Lee
Chii-Wann Lin
Ashley Luft
Ashish Mahajan
Biswajit Maharathi
Mufti Mahmud
Subhamoy Mandal
Cynthia Mares
Johnny Marques
Alexandre Matov
Koichiro Matsumoto
Hande McGinty
Zach McKinney
Matt McMahon
Joerg-Uwe Meyer
Ann Mongoven
Muhammad Mujeeb-U-Rahman
Paul Murdock
Rajesh Murthy
Ayman Nassar
Emily Nichols
Norliza Mohd Noor
Henry Ogoe
Andrew O'Hare
Chokha Palayamkottai
Anupam Kumar Pandey
Ketan Paranjape
Tanja Pavleska
Paul Petronelli
Cristian Pimentel
Hugo Plácido da Silva
Jodyn Platt

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Daniel Pletea
Eleftheria Polychronidou
Michal Ptaszynski
Beth Pumo
Bina Ramamurthy
Scott Rich
Chris Riha
Scott M. Robertson
Marina Romanchikova
Joseph Ronzio
Martin Rosner
David Rotenberg
Jason Royes
Kobi Rubin
Chandrasekaran Sakthivel
Jason Salstrom
Brian Scogland
Oshani Seneviratne
Terseer Taysay Shaguy
Parthiv Shah
Ren Shan
Rajveer Shekhawat
Ian Sherlock
Jorge Silva
Lisa Simone
Dharm Singh
Lakeidra Smith
David Snyder
Lisa Spellman
Emily Spratt
Ernesto Staroswiecki
Robert Stemp
Nicholas Sturgeon
Eric Svetcov
Haluk Tekbulut
Grace Trinidad
Michaela Vanderveen
Rohith Yanambaka Venkata
Konstantinos Votis
Ray Walshe
Jerry Wang
Linling Wang
Yong Wang
Paul Warner
Jason Waterman
Scott Whitmire
Jim Whitmore
Jason Winkler
Phil Wolff
Carol Woody
Marcus Young
Yu Yuan
George Zaki
Ali Zalzala

The following members of the individual Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Bjoern Andersen
Boon Chong Ang
Justin Armstrong
Katherine August
Pradeep Balachandran
Judy Barkal
Lyle Bullock
Colin Cantlie
Carole Carey
Simona Carini
Pin Chang
Steven Dain
Sherri Douville
Kurt Elliason
Javier Espina
Kenneth Fuchs
David Fuschi
Pershing Gervais
Rohit Goswami
Charles Gropper
Louis Gullo
Jon Hagar
William Harding
Marco Hernandez
Werner Hoelzl
Florence Hudson
Craig Hyps
Erwin Karincic
Piotr Karocki
Martin Kasparick
Konstantinos Katzis
Stuart Kerry
Quist-Aphetsi Kester
Edmund Kienast
Yongbum Kim
Roberto Moreno
Rajesh Murthy
Mitchell Parker
Bansi Patel
Nada Philip
Esteban Pino
Kim Reisinger
Stefan Schlichting
Mathini Sellathurai
Jhony Sembiring
Sarah Shafqat
Michael Shea
Harry Solomon
Thomas Starai
Eugene Stoudenmire
Dane Stout
Mark Sturza
John Vergis
Axel Wirth
Oren Yuen
Janusz Zalewski

When the IEEE SA Standards Board approved this standard on 6 June 2024, it had the following membership:

David J. Law, *Chair*
Jon W. Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara R. Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss
Hao Hu
Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano
Paul Nikolich
Robby Robson
Mark Siira
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Introduction

This introduction is not part of IEEE Std 2933/UL 2933:2024, IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety, and Security.

This standard for Clinical Internet of Things (CIoT) data and device interoperability with Trust, Identity, Privacy, Protection, Safety, and Security (TIPPSS), addresses the need for specific technical considerations to be incorporated in the design, development, deployment, and decommissioning/disposal stages of connected healthcare and clinical IoT devices and systems to help reduce risk to the data, device, patient, and provider. The purpose of TIPPSS is to help protect humans, devices, and data from harm. Stakeholders expect an implicit level of assurance at all levels of TIPPSS. It is expected that TIPPSS principles are considered as part of the device lifecycle. Connected healthcare systems, including CIoT devices, span multiple boundaries and can utilize technology from many areas to assemble solutions to allow stakeholders such as medical providers to better care for their patients.

This standard applies to CIoT objects, from apps to sensors and glucometers to MRI machines and stationary devices, that are used to inform clinical decisions or are used for clinical purposes. TIPPSS applies to all classes of cleared or investigational medical devices. Any clinical IoT device that can be compromised from a trust, identity, privacy, protection, safety, or security perspective is in scope.

This standard enables solution providers to follow a structured process and guidelines for device and systems development, engineering, deployment, operations, and decommissioning that incorporates TIPPSS principles at all device lifecycle stages. These solutions can include hardware, firmware, software, services, and/or a combination of any of those four types of solution elements. These solutions can also include multiple means of communication, including cellular, Ethernet, IEEE 802.11-based, or IEEE 802.15-based (Bluetooth®), among others. These can also include the inclusion of the reference to existing standards.

Multiple existing standards exist for safety, security, and medical devices. This standard provides a meta-framework for device manufacturers, deployment organizations, and other interested parties to design TIPPSS elements into their products, architectures, and systems.

TIPPSS has been designed to provide a framework and practices to address the various interrelated aspects of factors that can help achieve safe and effective interoperability (see Figure 1) in connected healthcare systems leveraging CIoT devices. For example:

— A CIoT device needs to have a unique identity and be secure for it to be trusted.

— Privacy laws and use cases define the requirements for the level of security required, e.g., cryptographic strength.

— A device needs to be secure in order to be safe and provide protection to users and patients.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Figure 1—TIPPSS

Copyright © 2024 IEEE and ULSE. All rights reserved.

The practices set forth in this standard aim to enable the improved protection of the human subjects of these CIoT solutions, the critical and sensitive data being stored and exchanged via multiple means, and the CIoT solutions themselves. These practices aim to make CIoT solutions more resistant to cyber threats, reduce the impacts of any potential cyber incident(s), and enable quick and accurate recovery. Due to their exploitation of weaknesses in individual solution components that can damage entire infrastructures, ransomware attacks signal the need for TIPPSS principles that take a comprehensive, multi-faceted approach to develop trusted, safe, and secure CIoT systems.

This standard applies to legacy and traditional devices, as well as the evolving ecosystem of CIoT solutions being developed now and in the future. This standard will complement, integrate with, and enhance existing standards already used for individual connected healthcare solution components. TIPPSS is designed to augment and promote existing safety and risk management frameworks and techniques to apply them to the CIoT world at scale. This standard is designed to meet today's needs while being extensible for the future.

This standard provides the frameworks, guiding principles, processes, and related standards for incorporating all these principles into end-to-end systems engineering processes. It enables solution providers to proactively identify these capabilities and gaps within their own systems and processes. The goals are to facilitate better and more efficient communications of these expectations and requirements early enough in the development process to protect human subjects better, increase end-user satisfaction, increase system resilience, reduce overall compliance costs, and reduce overall support costs.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Contents

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety, and Security

ULNORM.COM : Click to view the full PDF of UL 2933 2024

1. Overview

1.1 Scope

This standard establishes a framework based on TIPPSS principles (trust, identity, privacy, protection, safety, and security) for Clinical Internet of Things (CIoT) data and device interoperability. This includes CIoT such as in-hospital devices, wearable devices, investigational devices, etc. that communicate with each other and with healthcare systems including electronic health records (EHRs), electronic medical records (EMRs), and other connected healthcare systems.

NOTE 1—This standard is limited to devices both physical and virtual that are used in a clinical application, not necessarily a clinical setting. As such use cases where devices are currently considered for personal health and wellness are not covered by the standard.

NOTE 2—This standard is not a protocol for communications. It is the decision of the vendor and/or solutions provider to provide interoperability using protocols or standards such as ISO/IEEE 11073 (Health informatics—Medical/health device communication standards), HL7 v2,[8] Fast Healthcare Interoperability Resources (FHIR), etc.

NOTE 3—This standard incorporates numerous existing safety standards by reference. It is redundant to attempt to build another standard for safety when many tested and respected ones exist.

1.2 Purpose

The purpose of this standard is to help enable secured data sharing in connected healthcare solutions for improved healthcare outcomes, help protect patient and data privacy and security, and assist in protecting the subjects and humans who are the ultimate users of these solutions.

[8] Published by HL7 International.

Copyright © 2024 IEEE and ULSE. All rights reserved.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[9, 10]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO/IEC 27001:2022, Information security management systems—Requirements.[11]

ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection—Information security controls.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[12]

Subclauses 3.1.1 through 3.1.3 are groupings of definitions organized as a taxonomy. The subclauses build on each other and are not necessarily in alphabetical order but in order of complexity.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

[9] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[10] The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.
[11] ISO publications are available from the International Organization for Standardization (https://www.iso.org/home.html) and the American National Standards Institute (https://www.ansi.org/).
[12] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

Copyright © 2024 IEEE and ULSE. All rights reserved.

3.1.1 IoT definitions

actuator: Component of a device that changes one or more physical (electrical, chemical, optical, etc.) properties. (ISO/IEC 20924:2021, 3.2.1)[13]

NOTE—The change can be nonmechanical in nature.[14]

Internet of Things (IoT): Infrastructure of interconnected people, devices, systems, and information resources together with services that process and react to information from the physical world and virtual world. (ISO/IEC 20924:2021, 3.2.4)[11]

IoT device: Either an IoT physical and/or IoT virtual device.

IoT gateway: Entity of an IoT system that connects one or more proximity networks and the IoT devices on those networks to each other and to one or more access networks. (ISO/IEC 20924:2021, 3.2.8)[11]

IoT physical device: An instrument, apparatus, implement, machine, appliance, implant, in vitro reagent, or material that interacts and communicates over a network with the physical world through sensing and/or actuating. (ISO/IEC 20924:2021, 3.2.6)[11]

IoT system: System providing functionalities of IoT.

NOTE—An IoT system can include, but may not be limited to, IoT devices, IoT gateways, IoT sensors, and IoT actuators. (ISO/IEC 20924:2021, 3.2.9)[11]

IoT virtual device: Software running on a mobile device (app) or computing platform (application) that communicates over a network.

sensor: Component of a device that measures one or more physical (physiological, electrical, chemical, optical, etc.) properties. (Adapted from ISO/IEC 20924:2021, 3.2.12)[11]

3.1.2 Clinical-related definitions

clinical: Relating to a healthcare setting or healthcare application with professional healthcare oversight.

clinical actuator: A physical device or component thereof that changes one or more physical properties in response to an input intended for clinical contexts of use. (Adapted from ISO/IEC 20924:2021 3.2.1)[11]

clinical context: A clinical setting, environment, or application.

clinical device: A clinical virtual device and/or clinical physical device.

clinical physical device: An instrument, apparatus, implement, machine, appliance, implant, in vitro reagent, or material intended for clinical contexts of use.

clinical sensor: A physical device or component thereof that measures one or more physical (includes physiological, chemical, optical, etc.) properties intended for clinical contexts of use. (Adapted from ISO/IEC 20924:2021 3.2.12)[11]

ULNORM.COM : Click to view the full PDF of UL 2933 2024

[13] ©ISO. This material is reproduced from ISO/IEC 20924:2021 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
[14] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

Copyright © 2024 IEEE and ULSE. All rights reserved.

clinical virtual device: Software running on a mobile device (app) or computing platform (application) intended for clinical contexts of use.

3.1.3 Clinical IoT (CIoT) related definitions

Clinical Internet of Things (CIoT): IoT used in a clinical context.

Clinical IoT (CIoT) actuator: A networked clinical actuator.

Clinical IoT (CIoT) application: Clinical IoT (CIoT) software typically running on a non-mobile computing platform.

Clinical IoT (CIoT) component/element: A single entity that performs a single function and combines with additional components/elements to comprise a CIoT device.

Clinical IoT (CIoT) device: A networked clinical device.

Clinical IoT (CIoT) ecosystem: The set of systems that make up the environment in which a CIoT device and other system entities, including humans, operate.

Clinical IoT (CIoT) mobile app: Clinical IoT software running on a mobile device.

Clinical IoT (CIoT) physical device: A networked clinical physical device.

NOTE—A Clinical IoT physical device may perform one or more functions and comprise one or more components/elements such as a sensor, an actuator, data storage, communication capabilities, etc.

Clinical IoT (CIoT) sensor: A networked clinical sensor.

NOTE—A clinical sensor connected to a network via a gateway (such as a smartphone) is considered a CIoT sensor.

Clinical IoT (CIoT) system: An IoT system used in a clinical context.

NOTE—A Clinical IoT system is a network of IoT (cyber-physical system) components, consisting of a mixture of cyber-physical devices, web-server components, or software system components that can connect to other system components in a network for a clinical use case.

Clinical IoT (CIoT) virtual device: A networked clinical virtual device.

3.1.4 General definitions

abnormal use: A conscious, intentional act or intentional omission of an act that is counter to or violates NORMAL USE and is also beyond any further reasonable means of USER INTERFACE-related RISK CONTROL by the MANUFACTURER. (IEC 62366-1:2015) [15]

NOTE—Reckless use, sabotage, or intentional disregard of information for SAFETY are such acts.

[15] Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

access control: Protection of system resources against unauthorized access; a process by which the use of system resources is regulated according to security policy, and usage is permitted only to authorized entities (users, programs, processes, or other systems) according to that policy. (ISO/IEC 27000:2014, 2.1)[16]

accompanying documentation: Materials accompanying a medical device and containing information for the user or those accountable for the installation, use, and maintenance of the medical device, particularly regarding safe use. (IEC 62366-1:2015)[12]

adaptive (system): A system capable of changing its behavior in response to changes in its environment.

NOTE—In CIoT systems, environmental changes might include expanded numbers of patients, patients with new/different medical conditions, new physical environments, different geographic locations, etc. An adaptive system is one that can be personalized for a patient or group of patients, including those with special needs. Adaptation is a requirement for the development of reference architecture.

aggregator: A device that collects data from multiple data streams and aggregates the data into customized data stream/s. It supplies the aggregated data to one or more data consumers. It does not translate the data, which would be the function of a gateway.

NOTE—Aggregators and gateways can be combined.

alert signal: Any audible, visual, and/or other signal that draws attention to a condition (event, issue, etc.).

architecture: The fundamental structure or framework underlying a system and the discipline of creating such structures and systems.

asset: Anything that has value to a person or organization. (NIST SP 800-160v1r1)

attack: Assault on a system that comes from an intelligent threat—an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. (IEC 62443-1-1:2009, 3.2.9)[17]

NOTE—There are different commonly recognized classes of attack as follows:

- An “active attack” attempts to alter system resources or affect their operation.
- A “passive attack” attempts to learn or make use of information from the system but does not affect system resources.
- An “inside attack” is an attack initiated by an entity inside the security perimeter (an “insider”)—i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- An “outside attack” is initiated from outside the perimeter by an unauthorized or illegitimate system user (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

attribute: A quality or feature regarded as a characteristic or inherent part of someone or something; a trait, element, aspect, affordance, or property of the person or thing.

authenticate: Verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission. (IEC 62443-1-1:2009, 3.2.12)[14]

[16] ©ISO. This material is reproduced from ISO/IEC 27000:2014 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.
[17] Copyright © 2009 IEC Geneva, Switzerland. www.iec.ch.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources. (NIST SP 800-63-3)

authenticator: Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. (NIST SP 800-63-3)

authorization: Right or permission that is granted to a system entity to access a system resource. (IEC 62443-1-1:2009, 3.2.14)[14]

authorize: To grant access, typically automated by evaluating a subject's attributes. (Adapted from NIST SP 800-63-3)

availability: Property of being accessible and usable upon demand by an authorized entity. (ISO/IEC 27000:2014, 2.9)[13]

availability manager: An entity that assesses all system devices and component/elements to verify that all are online, fully functioning, and ready to perform a process or function.

NOTE—A manager in the services quality and integration/reconciliation of TIPPSS (SQIRT) Layer of CIoT reference architecture. All system devices and components are either available or unavailable, and fully functional or compromised in some way at any point in time.

best practice(s): Adopting the latest technologies or techniques for the design and implementation of interoperable CIoT systems with TIPPSS.

NOTE—This includes, for example, generally applicable and discipline specific premarket design and assessment protocols, postmarket surveillance, operating procedures, guidelines, regulations, etc. that are commonly accepted and utilized by the CIoT medical device community, especially those that pertain to any of the TIPPSS attributes.

Bill of Materials (BOM): The list of all physical and digital materials and their characteristics that are required to manufacture a device.

NOTE—A BOM may be made up of a Hardware Bill of Materials (HBOM) and a Software Bill of Materials (SBOM).

bootstrapping: Providing just enough introduction and information exchange between a device and the network onboarding component to establish a secure channel over which provisioning of the device's onboarding credentials can occur.

NOTE—Bootstrapping consists of the following:

— Initial establishment of trust/introduction between device and the network onboarding component.

— Subsequent provisioning of keys or other credentials and configuration information to the device.

caregiver: A human who provides clinical care, including basic device-related services.

NOTE—The human could be a licensed or allied health professional or a family member.

certificate authority (CA): A company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individual persons) and bind them to cryptographic keys through the issuance of electronic documents known as digital certificates.

cloud computing: The on-demand availability, over the internet, of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

comprised identity: A device identity that represents components that each have their own identities, for things within things.

confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO/IEC 27000:2014, 2.12)[13]

controller: The component of a system that sends program messages to and receives response messages from devices. (IEEE Std 488.2-1992)

controller (identity): In the context of identity, a controller may refer to an entity that can demonstrate control of a private/public key pair and therefore prove ownership of an identifier.

correct use: Normal use without error. (IEC 62366-1:2015)[12]

Cyber-Physical System (CPS): A system that integrates computation with physical processes, in a network manner, whose behavior is defined by both cyber and physical parts of the system. (IEEE Std 2660.1-2020)

decommissioning: The point in the device lifecycle where it will no longer be utilized for its intended purpose.

deploying organization: Any group or individual that installs, configures, administers and/or maintains Clinical IoT with TIPPSS solutions.

deprovisioning: The removal of access to provisioned services.

device: An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory. (Adapted from the FDA Federal Food, Drug and Cosmetic Act)

NOTE—The term device used in its most general form in this standard refers to cyber devices that include both physical (sensors, actuators, machines, etc.) and virtual devices (software app and applications). A subset of these could be considered medical devices (see definition) based on their intended use, which is a regulatory concept that varies with geography.

Device Identifier Composition Engine (DICE): The hardware requirements and process for creating an identity value that is derived from a unique device secret and the identity (a condensed cryptographic representation) of the first mutable code.

device information declaration: An artifact that asserts proof of ownership or authorized networks for an IoT device during the onboarding process.

device lifecycle: The series of stages a device goes through from conception, design, development, etc. to end-of-life (EOL).

discovery: A mechanism that will enable an application to access the IoT data without the need to know the actual source of data, sensor description, or location.

discrete component: An electronic device constructed as a single unit and affixed to a printed circuit board.

NOTE—A component can include but is not limited to resistors, capacitors, packaged ICs (integrated circuits), MCUs, memory chips, etc.

ecosystem: The set of systems that make up the environment in which a device operates.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

edge device: An edge device is a device that provides an entry point into enterprise, carrier, or service provider networks.

NOTE—An edge device is any piece of hardware that controls data flow at the boundary between two networks. Examples include gateways, routers, switches, multiplexers, IoT Gateways, and a variety of other devices. Edge devices also provide connections into carrier and service provider networks.

effectiveness: Accuracy and completeness with which users achieve specified goals. (IEC 62366-1:2015)[12]

electronic health record (EHR or iEHR for integrated HER): A digital version of a patient's paper chart.

NOTE—An EHR/iEHR is a real-time, patient-centered record that makes information available instantly and securely to authorized users. While an EHR/iEHR does contain the medical and treatment history of a patient, an EHR/iEHR system is built to go beyond standard clinical data collected in a provider's office (see EMR) and can be inclusive of a broader view of a patient's care.

electronic medical record (EMR): Electronic/digital versions of the paper charts in clinician offices, clinics, and hospitals.

NOTE—EMRs contain notes and information collected by and for the clinicians in that office, clinic, or hospital and are mostly used by providers for diagnosis and treatment.

entity: A resource of any kind that can be uniquely and independently identified. [IETF RFC 3986, Uniform Resource Identifier (URL)]

Fast Healthcare Interoperability Resources (FHIR): A standard describing data formats and elements and an application programming interface for exchanging electronic health records.

NOTE—The FHIR standard was created by the Health Level Seven (HL7) International health-care standards organization.

firmware: Computer programs and data stored in hardware, typically in read-only memory (ROM) or programmable read-only memory (PROM), such that the programs and data cannot be dynamically written or modified during execution of the programs. (NIST SP 800-53 Rev. 5)

formative evaluation: User interface evaluation conducted with the intent to explore user interface design strengths, weaknesses, and unanticipated use errors. (IEC 62366-1:2015)[12]

gateway: A relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other. Also described as an intermediate system that is the translation interface between two computer networks. (IEC 62443-1-1:2009, 3.2.53)[13]

happy path: A situation in a use case where everything happens as it is supposed to.

hardware: A physical element, component, or device.

Hospital @Home: A clinical workflow where the patient is cared for at home, using connected healthcare devices and Clinical IoT connected digitally to a hospital or clinical care team for remote support.

identifier: A pattern to uniquely identify a single entity (instance identifier) or a class of entities (i.e., type identifier) within a specific context.

identity: An attribute or set of attributes that uniquely describes a subject within a given context. (NIST SP 800-63-3)

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

individually identifiable health information: Information, including demographic data, which relates to the following:

— An individual's past, present or future physical or mental health or condition;

— The delivery of healthcare to the individual; or

— The past, present, or future payment for the delivery of healthcare to the individual.

and that identifies the individual or for which there is a reasonable basis to believe an individual can be identified using it. Individually identifiable health information includes common identifiers including name, address, birth date, and, depending on the local authority, Social Security Number, Social Insurance Number, or Medical Record Number.

integrated systems design (ISD): A comprehensive approach to design that brings together specializations, usually considered separately, to develop an integrated holistic system of systems approach. It attempts to consider all the factors and modulations necessary for a holistic integrated systems decision-making, design, development, and maintenance process.

integrity: A quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information. (IEC 62443-1-1:2009, 3.2.60)[13]

intelligent system: A system that involves some elements of learning and/or adaptation, so the output is not always the same given the same inputs (not like a deterministic, closed-loop system).

NOTE—An integrated system may or may not be an intelligent system; however, most devices and systems in the CIoT ecosystem for which this standard will apply are likely to have some level of intelligence.

interface: Logical entry or exit point that provides access to the module for logical information flows. (IEC 62443-1-1:2009, 3.2.62)[13]

interoperability: The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged. (ISO/IEC 17788:2014, 3.1.5)[18]

local area network (LAN): A medium-range network that can typically support communication in areas ranging from a home to an enterprise such as a hospital.

Manufacturer Authorized Signing Authority (MASA): The entity that, for the purpose of this document, signs the vouchers for a manufacturer's pledges.

microcontroller unit (MCU): A compact integrated circuit designed to govern a specific operation in an embedded system.

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

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

[18] Copyright © 2014 IEC Geneva, Switzerland. www.iec.ch

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

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

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

— Supporting or sustaining life, controlling conception, disinfection of medical devices;

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

and does not achieve its primary intended action by pharmacological, immunological, or metabolic means in or on the human body but that may be assisted in its intended function by such means. (GHTF/SG1/N71:2012)

Medical Device Registry: A database containing information relating to medical devices and related metadata depending on the purpose of the registry.

NOTE—Usage of these registries includes various objectives, including short- and long-term surveillance, fulfillment of postmarket observational study commitments for regulatory bodies, and comparative safety and effectiveness assessments, including those in under-studied subpopulations.

monitoring: The act of surveillance, specifically patient surveillance in this standard.

NOTE—Monitoring of an individual's status can occur in different locations (remote, vehicle, clinic, etc.), at different times (episodic, periodic, continuous); results can be communicated synchronously or asynchronously or processed for interoperability or further use, and stored on the device, on a remote server, in the cloud, or other secure location.

OpenID Connect (OIDC): A simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner.

onboarding: All steps required to provide a device with the network credentials and other required information and data needed to connect securely to the network to be operational.

organizational interoperability: Coordination of well-understood distributed workflows and activities by systems, organizations, or people interacting in business processes, such as how the business services and the consumer services will interact, understanding the information, and sharing the information, using the correct format, and using it for the correct business processes.

patient: One or more of the following:

— A person who requires medical or dental care.

— A person receiving medical or dental care or treatment.

— A person waiting for medical care, receiving it, or who has already received it.

— A person under a physician's care for a particular disease or condition.

— An individual who is receiving needed professional services directed by a licensed medical practitioner toward maintenance, improvement or protection of health or lessening of illness, disability, or pain.

personal/patient area network (PAN): A short range network that can typically support communication across devices immediately in the vicinity of a person/patient.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

personal health record (PHR): A health record where health data and other information related to the care of a patient is maintained by the patient.

personally identifiable information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (NIST SP 800-63-3)

principle of least privilege (PoLP): The principle that users and programs should only have the necessary privileges to complete their tasks.

printed circuit board (PCB): A non-conductive substrate on which a pattern of traces of conductive material (such as copper) has been etched or deposited, which mechanically supports and electrically connects components (e.g., capacitors, resistors) that are soldered to the substrate, but not including the components attached to it. (IEEE Std 1680.1-2018)

privacy: Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. (NIST SP 800-188)

NOTE—The definition of privacy may change based on local regulations.

protected health information (PHI): All "individually identifiable health information" held or transmitted by a covered entity or its business associate in any form or media, whether electronic, paper, or oral. (Privacy Rule - U.S. Family Educational Rights and Privacy Act, 20 U.S.C. §1232g)

protection: A capability that prevents someone or something from suffering damage, harm, or injury, as well as providing for increased safety, efficacy, and security for medical devices and data in connected healthcare systems and in the use of Clinical IoT devices.

provider: An individual or organization providing healthcare.

provisioning: All steps required to provide a device with the network credentials and other information needed to connect securely to a network and to be recognized and operational in the context of the network.

NOTE—It includes the subprocess of bootstrapping and then, after the device and the network onboarding component have established a secure channel through bootstrapping, the remainder of the onboarding process consists of using this secure channel to configure the device with its onboarding credentials.

recycling/repurposing: The removal of a device from service from the owning organization and transfer to another organization.

reference architecture (RA): An authoritative source of information about a specific subject area that provides conceptual, functional, and architectural guidance. (ISO/IEC 20547-3:2020)[19]

NOTE 1—Reference architectures generally serve as a foundation for solution architectures and can also be used for comparison and alignment of instantiations of architectures and solutions.

NOTE 2—Specifically, regarding CIoT systems with TIPPSS, the RA incorporates aspects of RAs within business, healthcare, and services sectors.

regulatory interoperability: Whether and to what extent integrated CIoT systems can effectively operate under different authorities (nation, country, state, or regions) by adhering to the governing laws, authorizations, regulations, and policies driven by statutes and enforced by government or agencies tasked with setting such requirements. In addition, regulatory interoperability can refer to other requirements as

[19] Copyright © 2015 IEC Geneva, Switzerland. www.iec.ch

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

specified in guidelines, consensus documents, and strategies, and adopted as best practices or certified through accrediting bodies.

reprovisioning: The act of taking a device that was previously provisioned and provisioning for a different network context.

Responsible Organization (RO): The organizational entity accountable for the use and maintenance of a medical device or combination of medical devices. (IEC 62366-1:2015)[12]

REST (REpresentational State Transfer): An architectural style for providing standards between computer systems on the web, making it easier for systems to communicate with each other.

risk: The combination of the probability of occurrence of harm and the severity of that harm. (ISO 14971:2019, 3.18) [20]

role-based access control (RBAC): Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role).

NOTE—Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single person or several individuals.

roots of trust: Reliable hardware, firmware, and software components that perform specific, critical security functions.

NOTE—Because roots of trust are inherently trusted, those roots shall be secure by design. As such, the implementations of roots of trust start with a known hardware base so that malware cannot tamper with the functions that the roots provide. Roots of trust provide a firm foundation from which to build security and trust.

router: A device that converts data from one physical communication medium to another, for example, from serial RS232 to Ethernet. A router also aggregates data from numerous communicating entities for the purpose of communicating along a defined path.

safety: Freedom from unacceptable risk of harm, specifically the prevention of injury or damage to the health of people or damage to property or the environment related to a CIoT device or solution.

security: State where information and systems are protected from unauthorized activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to violation of confidentiality, integrity, and availability are maintained and operated at a safe and effective level throughout the lifecycle. (Adapted from ISO 81001-1:2021, 3.2.13)

semantic interoperability: The ability of two or more systems or applications to exchange data with unambiguous, shared meaning. (Adapted from Wikipedia)

NOTE—Semantic interoperability is a requirement to enable machine computable logic, inferencing, knowledge discovery, and data federation between information systems. Defines and standardizes information to be shared, processed, and well-understood (without ambiguity) by systems. Examples of strategies for semantic interoperability are unambiguous codes and identifiers for health information, e.g., clinical terminologies, taxonomies, or ontologies, such as LOINC, SNOMED-CT, ICD-10, etc.

session: A discrete connection that starts with trust establishment with a unique peer, either through one-way or mutual authentication, and all successive communications with the peer until deliberate termination is accomplished through explicit action from either peer or timed event.

[20] ©ISO. This material is reproduced from ISO 14971:2019 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

single fault condition: A condition in which a single means for reducing risk is defective, or a single abnormal condition is present (IEC 60601-1:2020)

Software as a Medical Device (SaMD): Software whose intended use is for one or more medical purposes that performs these purposes without being part of a hardware medical device. (FDA https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd)

Software Bill of Materials (SBOM): A nested inventory, a list of ingredients that make up software components. (CISA https://www.cisa.gov/sbom)

Software Identification (SWID) Tag: A structured set of data elements that identify the software product, characterize the product's version, the organizations and individuals that had a role in the production and distribution of the product, information about the artifacts that comprise a software product, relationships between software products, and other descriptive metadata.

solution provider: Any group or individual that designs, develops, manufactures, tests, integrates, deploys, or in other ways provides Clinical IoT with TIPPSS solutions, including hardware, firmware, software, and/or services.

stakeholders: Entities with an interest in adhering to or applying the standard, and individuals affected by the implementation of the system(s) designed via application of the standard.

status: The state of a system, device, component, or element at any point in time that determines its ability to perform a process or function. The state may be at rest or in motion, available or unavailable, fully functional or compromised, etc.

subassembly (SA): A functionally complete part of a Clinical IoT device. The subassembly includes a printed circuit board (PCB) as well as all components required and listed on its bill of materials (BOM).

summative evaluation: User interface evaluation conducted at the end of the user interface development with the intent to obtain objective evidence that the user interface can be used safely. (IEC 62366-1:2015)[12]

syntactic interoperability: The data structure and data formats that enable data exchange.

NOTE—This includes data communication and exchange rules, how to arrange/order data, and how to convert the data into similar formats. Examples of syntactic approaches are the definition of data formats, well-defined syntax and encoding (e.g., message content structure, size of headers, size of message body, fields contained in a message), such as different versions of HL7 or DICOM.

system of systems (SoS): A set of components (e.g., mechanical, electrical, software) and/or subsystems integrated to perform a function or functions based on stakeholders' needs. This may include subsystems that may interact with other subsystems to the benefit of the overall system. In addition, the SoS, or any system within the SoS, may interact with external systems as well.

system service/process: A series of steps usually driven by a software application to control and implement a function or an operation.

systems engineering: An interdisciplinary approach to the realization of complex systems that aims to satisfy stakeholders' needs. It considers system performance in the context of intended use and device lifecycle. (IEEE/ISO/IEC 15288)

task: One or more user interactions with a medical device to achieve a desired result. (IEC 62366-1:2015)[12]

technical interoperability: The communication links, protocols, and infrastructure, represented in the lower layers of the ISO/OSI communications model, for data exchange.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

threat: Potential cause of unacceptable asset loss and the undesirable consequences or impact of such a loss. (NIST FIPS 200)

trust: The belief that a person, service, or thing will not cause harm to any other person, device, or thing when allowed to operate with a specific CIoT device or ecosystem. An outcome of trust is to allow only designated people, devices, applications, or services to have device or data access with each other.

trust anchor: An authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative.

trust framework: A pre-negotiated set of business, legal, and technical agreements that bind all stakeholders with mutual assurance of the reliability and repeatability of online transactions.

Universal Device Identifier (UDI) System: A system established by the U.S. Food and Drug Administration (FDA) to identify medical devices sold in the United States.

Universal Serial Bus (USB): USB is an industry standard that establishes specifications for cables, connectors, and protocols for connection, communication, and power supply interfacing between computers and peripherals, and other computers.

usability engineering/human factors engineering: Application of knowledge about human behavior, abilities, limitations, and other characteristics to the design of medical devices (including hardware and software), systems, and tasks to achieve adequate usability. (IEC 62366-1:2015)[12]

usability engineering file: The set of records and other documents that are produced by the usability engineering process. (IEC 62366-1:2015)[12]

usability test: Method for exploring or evaluating a user interface, with intended users, within a specified intended use environment. (IEC 62366-1:2015)[12]

usability: Characteristic of the user interface that facilitates use and thereby establishes effectiveness, efficiency, and user satisfaction in the intended use environment. (IEC 62366-1:2015)[12]

use environment: Actual conditions and settings in which users interact with a medical device. (IEC 62366-1:2015)[12]

use error: User action or lack of user action while using the medical device that leads to a different result than that intended by the manufacturer or expected by the user. (IEC 62366-1:2015)[12]

use scenario: Specific sequence of tasks performed by a specific user in a specific use environment and any resulting response of a medical device. (IEC 62366-1:2015)[12]

use specification: Application specification summary of the important characteristics related to the context of use of a medical device. (IEC 62366-1:2015)[12]

user: Person interacting with (i.e., operating or handling) the medical device. (IEC 62366-1:2015)[12]

NOTE 1—The user can be at the device or operating it remotely.

NOTE 2—The user can be a patient, caregiver, clinician, operator, etc.

user group: Subset of intended users who are differentiated from other intended users by factors that are likely to influence usability, such as age, culture, expertise, or type of interaction with a medical device. (IEC 62366-1:2015)[12]

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

user interface: Means by which the user and the medical device interact. (IEC 62366-1:2015)[12]

user interface evaluation process: Process by which the manufacturer explores or assesses the user interactions with the user interface. (IEC 62366-1:2015)[12]

user interface specification: Collection of specifications that comprehensively and prospectively describe the user interface of a medical device. (IEC 62366-1:2015)[12]

user-managed software: Computer programs stored in and executed by computer hardware, and associated data that also is stored in the hardware, which may be dynamically written or modified during execution. The user of the software can operate the software in the cloud, on-prem, on the device, or on a server, and designate when to apply updates.

user profile: Summary of the mental, physical, and demographic traits of an intended user group, as well as any special characteristics, such as occupational skills, job requirements, and working conditions, which can have a bearing on design decisions. (IEC 62366-1:2015)[12]

NOTE—The user profile needs to consider the fact that, in many cases, the users will also be patients who may have challenges due to their health conditions.

vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST FIPS 200)

wellbeing (or well-being): A state of human equilibrium or balance that is affected by life events or challenges.

NOTE—Wellbeing is stable when one has the resources needed to meet life's challenges at distinct levels such as biophysical, psychological, and social.

wellness: A subset of wellbeing, usually focused only on biophysical and psychological aspects.

wide area network (WAN): A long-range network that can cover the earth.

3.2 Acronyms and abbreviations

A/D	analog to digital
AI	artificial intelligence
AICD	automated implantable cardioverter defibrillator
AID	automated insulin delivery
AI/ML	artificial intelligence and machine learning
ALOF	automatic logoff
APEC	Asia-Pacific Economic Cooperation
API	application programming interface
app	application

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

AUDT	audit controls
BIOS	basic input/output system
BIT	built-in test
BLE	Bluetooth Low Energy
BMC	baseboard management controller
BRSKI	Bootstrapping Remote Secure Key Infrastructure
CA	certificate authority
CBOR	Concise Binary Object Representation
CCPA	California Consumer Privacy Act
CDI	Compound Device Identifier
CGM	continuous glucose monitor
CIoT	Clinical Internet of Things
CMDB	configuration management database
COPD	chronic obstructive pulmonary disease
CoSWID	Concise Software Identification
CPS	Cyber-Physical System
CPU	central processing unit
CRL	certificate revocation list
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DBS	deep brain stimulator
DICE	Device Identifier Composition Engine
DICOM	Digital Imaging and Communications in Medicine
DPIA	Data Protection Impact Assessment
ECG	electrocardiogram
EHR	electronic health record
EMC	electromagnetic compatibility

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

EMR	electronic medical record
ePHI	electronic protected health information
EPROM	erasable programmable read-only memory
FDA	Food and Drug Administration (United States)
FHIR	Fast Healthcare Interoperability Resources
FIPs	Fair Information Practices
FMEA	Failure Modes and Effects Analysis
FW	firmware
GDPR	General Data Protection Regulation
GPIO	general purpose input/output
GPU	graphics processing unit
GUDID	Global Unique Device Identification Database
HDO	Health Delivery Organization
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level Seven
HTA	health technology assessment
HW	hardware
IAM	identity and access management
ICD	International Classification of Diseases
IFU	instructions for use
IGAU	health data integrity and authenticity
IoC	indicator of compromise
IoT	Internet of Things
IPG	implanted pulse generators
IRB	Institutional Review Board
ISAC	Information Sharing and Analysis Center
ISD	integrated systems design

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

LAN	local area network
LPC	Low Pin Count
MAB	MAC Authentication Bypass
MASA	Manufacturer Authorized Signing Authority
MCU	microcontroller unit
MD	medical device
MES	manufacturing execution system
MFA	multi-factor authentication
MIoT	Medical Internet of Things
MLDP	malware detection/protection
MUD	manufacturer usage description
MVRA	Minimum Viable Reference Architecture
NFC	near-field communication
NITRD	Networking and Information Technology Research and Development Program (U.S.)
NIST CSF	NIST Cybersecurity Framework
OAuth	Open Authorization
OIDC	OpenID Connect
OSI	Open Systems Interconnection
OTA	over-the-air
PA	production associate
PACS	picture archiving and communications system
PAN	personal/patient area network
PCB	printed circuit board
PCI	Peripheral Component Interconnect
PHI	protected health information
PHIPAA	Personal Health Information Privacy and Access Act (Canada)
PHR	personal health record

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

PIA	Privacy Impact Assessment
PII	personally identifiable information
PIPEDA	Personal Information Protection and Electronic Documents Act
PKI	public key infrastructure
PM	Privacy Manager
POD	people, organizations, and devices
PoLP	principle of least privilege
PROM	programmable read-only memory
PSK	pre-shared key
PURL	persistent uniform resource locator
PWB	printed wiring board
RA	reference architecture
RAM	random-access memory
RBAC	role-based access control
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFID	Radio Frequency Identification
ROM	read-only memory
SA	subassembly
SaMD	Software as a Medical Device
SBOM	Software Bill of Materials
SAST	Static Application Security Testing
SD	secure digital
SDK	software development kit
SIEM	Security Information and Event Management
SiMD	Software in a Medical Device
SMBus	System Management Bus

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

SNMP	Simple Network Management Protocol
SOA	service-oriented architecture
SOC	Security Operations Center
SoS	system of systems
SPDX	Software Package Data Exchange
SQIRT	services quality and integration/reconciliation of TIPPSS
SSDLC	Secure Software Development Lifecycle
SSO	Single Sign-On
SW	software
SWID	Software Identification
TIPPSS	Trust, Identity, Privacy, Protection, Safety, and Security
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDI	unique device identifier
UDS	unique device secret
UI	user interface
USB	Universal Serial Bus
V&V	verification and validation
WAN	wide area network
WPA	Wi-Fi Protected Access
ZTA	Zero Trust Architecture

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4. Trust and identity

4.1 Introduction

The world faces an ever-growing population of devices that connect our homes, our environments, and ourselves. Some even deliver life-saving information and treatments. Globally, Clinical IoT (CIoT) has the potential to improve health outcomes, facilitate recovery, lower healthcare costs, and increase the availability and accessibility of data-driven medicine.

Copyright © 2024 IEEE and ULSE. All rights reserved.

TIPPSS begins with *trust* and *identity* as that is the core capability to enable privacy, protection, safety, and security. The identity of CIoT devices is critical to help verify a level of trust that the people, services, and things connecting are, in fact, the correct ones and are the reliable, correct, and indisputable assertion of their identity. In this standard, trust in CIoT means that only trusted services and devices can access and/or control a device and/or generated data. This is after verified identification and authentication and is based on assigned roles and rights. After authentication, and based on assigned roles and rights, the CIoT devices and trusted services and/or devices can access and/or control the device and/or the generated data. Failures of identity or trust can compromise privacy as well as the delivery of health services, resulting in potential harm or adverse events.

The COVID-19 crisis has been a catalyst for the global healthcare system to look beyond the traditional silos of the clinical setting into decentralized and home-based care delivery models. The decentralization of populations, even within highly populated environments, characterizes a need to create solutions that enable patients, their care providers, other healthcare professionals, and patient advocates to securely exchange data across platform-agnostic technologies and systems. This standard applies to both centralized and decentralized healthcare environments.

This clause considers the set of clinical use cases as analyzed in Annex B to derive and frame a generic methodology that can help enable a wide range of business requirements and technical specifications for establishing trust and identity in CIoT. This clause considers the current landscape (people, organizations, devices, and software) in which users and organizations deploy CIoT, the existing and emerging identity protocols and trust frameworks, and the gaps and opportunities for high-functioning CIoT. This provides the context for specific technical and governance definitions, requirements, needs, and best practices for the trust and identity aspects of this standard.

In the past, trust and identity expectations and practices for people, organizations, and devices (POD) have been inconsistent and often incompatible. In this standard, this deficit is addressed, while easing the technical and procedural interoperability of CIoT.

4.2 Overview

Trust and identity in TIPPSS are critical dimensions in the correct and safe operation of a CIoT device. Two perspectives are used in defining the requirements for trust and identity—the macro and micro views (see Figure 2). The macro perspective is the device and its interactions with the outside “world.” That is, communication and interaction between the device and systems connected over a network (hardwire or wireless). The micro perspective is the looking “inward” view. The scope includes the trust and identity of all the hardware and software components used to build a device.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

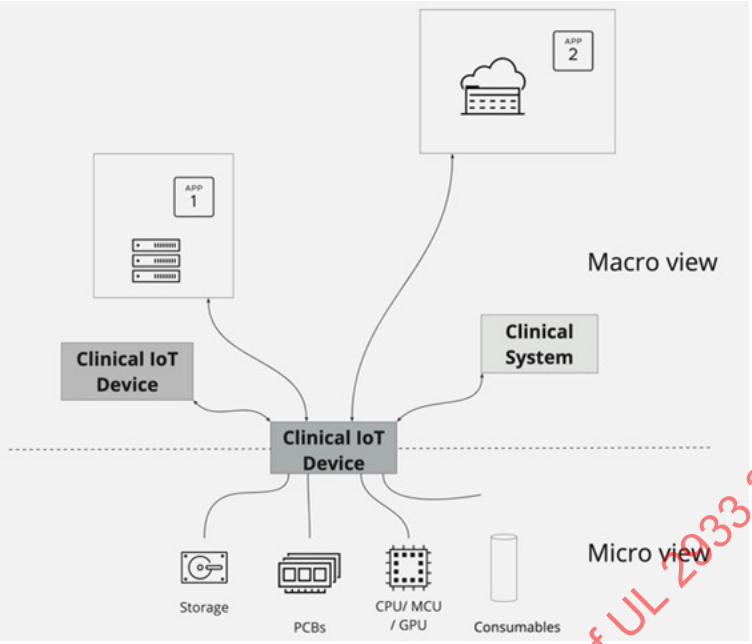

Figure 2—CIoT device in context

Similar to how entry and access are granted to people requesting to enter our home (e.g., the repair person versus a family member), the objective is to translate these concepts to a device context in connected healthcare. In CIoT data and device interoperability with TIPPSS, trust and identity are used to help ensure the privacy, protection, safety, and security of the CIoT device ecosystem, which also affects the patient and the connected healthcare system.

Trust and identity in TIPPSS include an elemental view of the complex and discrete components in a device, including transistors, multipurpose computer chips, storage, incoming software updates, data, incoming digital services, interaction with the physical world via sensors and actuators, human intervention, and connections.

Device trust and identity include multiple levels outlined in the following:

— Device development and manufacturing
— Device lifecycle design and management
— Inter-device and systems trust
— Interactions between environments
— Decentralized environments
— Device-to-human interaction (e.g., support technician, clinical operator, or patient)

The micro perspective is covered in 4.3. This includes requirements for designing, developing, and manufacturing CIoT devices. Manufacturers shall include trust and identity considerations right from the conceptualization of the device, and build them into the device and the entire manufacturing process. In this subclause, working through the layers listed in Figure 3, the primary areas of concern for TIPPSS in CIoT are covered.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

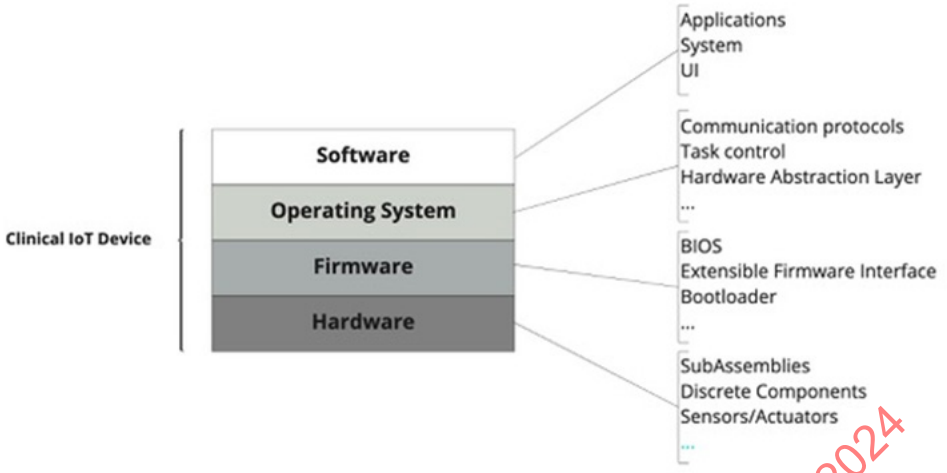

Figure 3—Logical CIoT device layers

The macro perspective is covered in 4.4, moving from manufacturing to use. This subclause outlines the requirements for trust and identity as a device moves into healthcare delivery organization(s), and increasingly as healthcare delivery moves out of the clinical environment to decentralized delivery in non-hospital environments (e.g., home, temporary facilities, or battlefield).

One of the outcomes of the COVID-19 pandemic is a momentous change in healthcare delivery models. These changes now require the ability to support centralized, decentralized, and hybrid models of delivery with no loss of trust.

Human trust and identity management mechanisms, also referred to as identity and access management (IAM), have evolved with the increase of the Internet of Things (IoT) and include standards, protocols, and enablers such as Security Assertion Markup Language (SAML), Open Authorization (OAuth), OpenID Connect (OIDC), and emerging decentralized identifiers and verifiable credentials standards. This TIPPSS standard will not delve into the various human IAM tools available in the CIoT space of connected healthcare but will primarily focus on machine-to-machine CIoT device communication. In this space, the use of public key infrastructure (PKI) digital certificates to provide both a root of trust with a certificate authority (CA), and identity assertions via the certificates themselves, are common. Additionally, new models of decentralized trust assurance and governance are emerging, extending the identity and trust zone in decentralized healthcare delivery.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4.3 Micro view

When regarding a CIoT device, one should recognize that the processes and practices that produced that device are an entire world unto themselves. Trust and identity in the micro view take on a different context from the macro view. Identity is correlated with traceability and trust is related to compliance with specifications and standards. Tens to thousands of physical, software, and potentially consumable elements can make up the composition of a device. There are documented challenges of counterfeit and non-compliant components, particularly concerning CIoT devices. It is through the traceability of the elements that a device is composed, and the ability to verify that these elements meet the specifications and standards that create the trust that the manufacturer has correctly built the device. Manufacturers shall plan for trust and identity, starting with the inception of device design, to help provide for the correct embedding of trust and identity capabilities into device development and manufacturing processes.

Copyright © 2024 IEEE and ULSE. All rights reserved.

In the creation of a medical device, there may be single or multiple printed circuit boards (PCBs). PCBs contain multiple components with various functions, such as a central processing unit (CPU), graphics processing unit (GPU), wireless transceiver, memory, resistor, capacitor, analog to digital (A/D) converter, general-purpose input/output (GPIO) device, rectifier, and more. In between those components, there are elements that enable communications and control, such as a System Management Bus (SMBus), a low bandwidth bus such as a Low Pin Count (LPC) interface, or a baseboard management controller (BMC), as examples.

Component-to-component communication on a PCB may also include off-the-shelf Bluetooth, near-field communication (NFC), CPU, and/or GPU components. Medical device manufacturers consume these components when creating advanced medical devices such as deep brain stimulators (DBS), implanted pulse generators (IPG), neurostimulators, cardiac-stimulators, insulin pumps, and more. Accordingly, there is a need to prevent third-party manufactured and sourced components from causing issues that could put the device, device manufacturer, user, or patient at risk. For example, a lack of signal filtering, power management, shielding, and even trust between components might compromise the entire system, impact the quality of data, and permit the device to be hacked and compromised. A PCB can be hacked at the subassembly or chip level, prior to being fully assembled as a final device or through backdoors and vulnerabilities within a system. The devices are also susceptible to compromise during field updating, refurbishment, or retooling for reuse, through the physical replacement of components, or the introduction of PCBs/PWBs with compromised components. The previously mentioned communications conduits of an SMBus, LPC, and BMC are often targeted either through unchecked basic input/output system (BIOS) patches or the inclusion of surreptitious components that can enable system attacks.

NOTE—While hardware-based attacks are real, the predominant attack surfaces for any device (medical or otherwise), are through the introduction of exploits in the firmware, software, and service updates and connections. Accordingly, this standard details the TIPPSS recommendations to avert these potential compromises and enable a more trusted, private, protected, safe, and secure connected medical device from manufacturing throughout the device lifecycle.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4.3.1 Discrete components

Within a CIoT device, identity starts with the components used in device construction. The definition of discrete components is extended to include all elements that the manufacturer can affix to a PCB (including the circuit board itself).

Trust that the manufacturer has correctly manufactured the device is based upon a combination of high confidence that they built validated and approved components into the device, and that all manufacturing processes have been complied with during the manufacturing stage. Thus, by using valid and compliant components, manufacturers can help avoid the following issues:

- Counterfeit, misbranded, uprated, or reprocessed components.
- Low-quality product (e.g., sub-standard material).
- Complete component failure (explodes, overheats, shorts, etc.)
- Does not meet lifecycle expectations (i.e., does not last as long as expected, or reduces the component's ability to provide reliable performance).
- Intermittent failure or performance reduction due to lack of environmental control [e.g., heat, electromagnetic interference (EMI)].
- Lack of available products (shortages could force users to integrate sub-standard components).
- Incorrect use of a component (i.e., not connected correctly or following quality requirements).
- Lack of recursive testing (even when in production use). Enabling test modes to continuously check the component functionality.

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.3.1.1 Practices and processes

The manufacturer shall reflect the requirements listed in 4.3.1.1.1 through 4.3.1.1.4 in their internal practices and processes. The manufacturer shall assign owners, typically in the form of roles, to each of the required activities.

4.3.1.1.1 Component inspection

During all steps of manufacturing, manufacturers shall visually inspect discrete components for obvious defects.

NOTE—Modern manufacturing inspection processes use vision sensors to inspect both the outside and inside of a component (for the purpose of this discussion, the concept of visual inspection includes the grouping of Xd-rays, ultrasound, and thermal imaging).

Further, the manufacturer shall use visual inspection to examine manufactured components against the "gold unit." The gold unit is the representation of the "perfect" unit. In other words, manufacturers shall compare new components to a component deemed "perfect" specific to length, width, height, color, angle, reflection, etc.

4.3.1.1.2 Component testing

The testing of discrete components can be in the form of electrical, thermal, pressure/force, reliability, quality, and/or chemical tests as appropriate by the manufacturer. Manufacturers may use a subset of those tests to determine the life expectancy of a component or the component's ability to operate in harsh environments. Thorough testing shall be performed by the manufacturer to help verify the quality and reliability of a discrete component.

4.3.1.1.3 Component certification

There may be grades or levels of use, based on system criticality or regulatory requirements, with which some components are associated to certify the components for usage. For example, a component that passes testing with an "A+" grade might be acceptable in medical devices. However, a component that receives a "D" grade might still pass inspection but with a target for usage in non-critical systems (e.g., a child's inexpensive toy).

4.3.1.1.4 Component traceability

Manufacturers shall identify every discrete component either individually or as a member of a subassembly for traceability. Manufacturers shall also mark each component with a manufacturer's symbol as well as with inspection grading. Additionally, manufacturers may identify other components based on the material composition. Further, manufacturers or subcontractors can direct part mark (DPM) some components with detailed information, using lasers that etch microscopic information.

Counterfeiting components is a serious and growing problem in the supply chains of all CIoT device manufacturers. Manufacturers shall have documented processes for validating the identity of the suppliers of components used in their CIoT devices. Manufacturers should meet component identification, track, and traceability requirements as defined in SEMI T20 [B51], SEMI T22 [B52], and their associated subordinate standards when manufacturing their own components.[21] Similarly, manufacturers should require their

[21]Numbers in brackets correspond with the sources listed in Annex A.

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

component vendors to meet component identification, track, and traceability requirements as defined in SEMI T20 [B51], SEMI T22 [B52], and their associated subordinate standards. Those standards address authentication methods via labeling, authentication methods via communication, and qualifications of authentication services.

In the case that a manufacturer is unable to meet the requirements of SEMI T20 [B51], the manufacturer shall document all decisions and factors that prevented compliance with SEMI T20 [B51].

4.3.2 Subassembly

CIoT devices may be constructed using from one-to-many subassemblies (SAs). SAs are made up of discrete components and are functionally complete parts of a final product. This standard focuses on SAs that are comprised of PCBs and the components mounted on the PCBs. The components mounted on the PCBs may or may not have the ability to communicate their identity through electronic means. This standard focuses on the components that can communicate their identity.

Trust in the manufacturing of a device is additive in nature. To achieve a baseline of trust, each step of the manufacturing process shall be known, documented, and demonstrably followed by the manufacturer. Each SA assembled with expected and identified components increases the trust level. When the final assembly is complete and it is possible to validate all SAs against a primary bill of materials (BOM), including both hardware and software, this establishes a level of trust that the device has been manufactured and assembled correctly and in a trustworthy manner.

For CIoT devices, PCBs should meet a high-reliability electronics standard, and every component of an SA shall have a unique identifier that can be traced back to its source, including the materials used in its manufacturing.

Starting with the incoming inspection of individual components, manufacturers shall inspect all incoming components and verify the Certificate of Origin of the components. The manufacturing execution system (MES) should record the certificate and retain it for the life of the product.

Traceability of components to their manufacturer and source allows for the provisioning of identity for components that do not have the ability to electronically communicate their identity autonomously. The manufacturer's MES/traceability system should record the identity of these components.

In preparation for the manufacturing of subassemblies, an MES shall use the device bill of materials (BOM) to create "kitting" lists, including all the necessary components for the device. In the creation of the kitting list, the MES shall link back to the Certificate of Origin for each of the individual components. Each component added to the assembly shall have a unique identifier assigned. Trust requires a known, approved, and verifiable identity for the traceability of all components of the SA. Further, during the creation of the SAs, the manufacturer shall add the certificates of origin of each component added to the SA to the BOM of the SA created.

For electronic components, the manufacturer shall include its assurance identifier in the component. Each electronic component [e.g., CPU, GPU, application-specific integrated circuit (ASIC), microcontroller unit (MCU)] shall provide its identity attributes to the SA or final assembly, and its attributes shall be linked to a verifiable attestation from the original component manufacturer.

For non-electronic components, manufacturers shall track identifiers during the manufacturing process and record them in the manufacturing execution system (MES). Manufacturers shall validate identifiers against a certified supplier list. The SA shall have a hash of all identifiers identified in the SA BOM associated with the SA. The manufacturer shall certify the hash and BOM of the SA. For high-reliability electronics, the manufacturer shall provide a cryptographically verifiable hash(es) of the SAs encompassing the final assembly.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.3.2.1 Practices and processes

4.3.2.1.1 Component traceability

Due to the nature of a CIoT device, the manufacturer shall document, retain, and be able to prove the following:

- Who manufactured specific components, and the creation and location of manufacture.
- What SA utilized it and when (including time, date, serial number, lot number, assembly equipment, and, if applicable, the operator/assembler).
- The identifier of the SA.
- Expiration date, if applicable.

The device manufacturer shall meet the minimum requirements for component traceability based on perceived risk as defined in IPC-1782 [B19].

4.3.2.1.2 Component identifiers

Every component and nonquantifiable material (e.g., cleaning material, epoxy, silicon rubber) used in a SA shall have an identifier, such as a serial number or batch/lot number. Where possible, the use of unique component level identifiers should be implemented. Where this is not feasible, manufacturers shall use batch and lot level identifiers. The manufacturer shall document and retain this information. Additionally, a manufacturer shall create a hardware bill of materials (HBOM), which is a comprehensive list of all the components, parts, and materials required to build a hardware product or system. Further, a HBOM serves as a reference document for manufacturers, engineers, and procurement teams to help ensure the correct and complete acquisition of all necessary items. The recommended use of a HBOM includes the following:

- Component identification
- Documentation and organization
- Manufacturing and assembly guidance
- Supplier management
- Cost estimation and budgeting
- Version control and revisions
- Compliance and regulatory requirements
- Service and maintenance

4.3.2.1.3 Process traceability

The manufacturing of an SA requires that a recipe list of processes be followed to verify that the SA has been correctly assembled, tested, and packaged. The manufacturer shall document, retain, and be able to prove that every process has been correctly executed.

Manufacturers shall meet the minimum requirements for process traceability based on perceived risk as defined in IPC-1782 [B19].

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.3.3 Device software

Device software is the computer program(s) and data stored in hardware or persistent storage to prevent dynamic writing or modification during the execution of programs. Management and updating of the device software is the responsibility of the CIoT manufacturer. Device software includes firmware, operating system, and all additional libraries or drivers required to operate the CIoT device.

In the past, applying updates to IoT devices required physical access to occur. A technician would have to either physically connect via a cable to the device or may need to open a device physically to change programmable read-only memory (PROM) to apply updates. As the number of devices continues to increase exponentially, the management and updating of devices have become a significant issue. This issue restricts manual or physical updating of devices to a very narrow range of life-critical devices; all other devices should support “over-the-air” (OTA) updates.

Prior to applying any firmware update to a receiving CIoT device:

— The CIoT device shall authenticate the source (the trust anchor) of the command/instruction to update the firmware.

— The CIoT device shall validate that the trust anchor is authorized to command the update.

— The CIoT device shall authenticate the source (server) of the firmware update using approved cryptographic algorithms.

— The CIoT device shall authenticate the integrity of any firmware update file using approved cryptographic algorithms.

Supporting an OTA update requires that the device be designed to support this. Design considerations include full or partial firmware updates, single or multiple bootloaders, and support for a Software Bill of Materials (SBOM). There are engineering and architecture design considerations to allow the updating of firmware. Manufacturers shall refer to guidelines such as NIST SP 800-193 [B45] (or jurisdictionally similar regulations) for regulatory requirements for the design and implementation of roots of trust and chains of trust in the firmware update process.

In device software updates, there are two design patterns—full updates and partial updates for specific components or defined issues. The full update process is simpler than that of a partial update; manufacturers shall include design considerations to allow for partial updates to occur.

The trust and identity processes for device software center on the authorized trust anchor(s) that provide device software updates, supply updated device software documentation, e.g., SBOM, and provide instructions on how to validate and update the SBOM.

The security baseline for firmware updates shall follow the guidance in Clause 8 for both full and partial firmware updates.

Full device software updates simplify both the update and code management process. Full device software updates shall be adopted unless extraordinary circumstances exist that prevent their use.

4.3.3.1 Practices and processes

The manufacturer shall reflect the following requirements in their internal practices and processes. The manufacturer shall assign owners, typically in the form of roles, to each of the required activities.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.3.3.1.1 Designing for security

Like quality and manufacturability, the security of a CIoT device cannot be addressed after the fact; it needs to be part of the system design from the initial conceptualization of the device. In designing for security, manufacturers should adopt a Secure Software Development Lifecycle (SSDLC) approach covering people, processes, and technologies. Jurisdictional regulators [e.g., NIST, The European Union Agency for Cybersecurity (ENISA)] have publications outlining the elements that manufacturers should consider.

4.3.3.1.2 Ability to update device software

The ability to support remote or OTA device software updates requires specific hardware design decisions, for example, the capability to support multiple bootloaders. Where OTA updates can be applied, the device shall be able to fail back to a previous device software version.

4.3.3.1.3 Software Bill of Materials (SBOM)

Manufacturers of CIoT devices should include the creation, maintenance, and distribution of SBOMs for device software. The use of SBOMs in CIoT devices is key in building confidence and assuring the integrity of the CIoT ecosystems. In many CIoT devices, real resource constraints may exist. The use of other data formats for the SBOM may be appropriate. In these considerations, manufacturers should consider the use of Concise Binary Object Representation (CBOR) based Software Identification (SWID), CycloneDX, or Concise Software Identification (CoSWID) Tags.

For further requirements for SBOMs, see Clause 8, Security.

4.3.4 Final product

In terms of healthcare technology, the concept of a final product might vary based on its position within the larger supply chain. For example, for a company that makes subassemblies utilized by companies that are building more complex technology, the concept of a final product might be that subassembly. Additionally, companies that make components at multiple locations and ship to a final assembly facility might consider each of the elements at each facility as a “final product.” That said, manufacturers of final products shall uniquely identify them to establish clear traceability within a company and across companies and users.

When considering unique device identifiers (UDIs) specific to the final product, there are two classes—identifiers used internally within only a single company, and identifiers used between multiple companies. In the first class, manufacturers shall establish methods of identification that confirm full traceability from the moment a component enters the company to the point where the component leaves the company.

For the second class of identifiers, manufacturers of technologies to be distributed outside of the company shall use externally recognized unique identification such that full traceability of the technologies can be established all the way back to the discrete component level. For both classes, identifier formats shall support version numbering for every revision or change of device components.

At the completion of manufacturing, the device shall have a UDI assigned (provisioned) that is known to the manufacturer. This ID shall be in addition to the regulatory UDI and shall be valid for the life of the device. The identifier should be stored in secure hardware (for example, Secure Enclave, TrustZone, etc.).

If the device uses cryptographic data protection, the device identifier shall be bound to any certificate(s) (e.g., X.509, MUD, W3C Verifiable Credential) installed on the device.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Ideally, the device should use asymmetric cryptography and a public/private key pair. If the device uses symmetric encryption with a single key, the manufacturer shall assess the associated security risks and shall document the justification for not using asymmetric cryptography.

A certificate:

a) Is for a specific purpose, and therefore, a device can have multiple certificates supporting multiple distinct functions.

b) Has a shorter life than the device ID and shall have the capability of being revoked or reissued.

c) Can contain the device ID as reference (e.g., in a custom field or extension), but the device ID is not part of the separately managed cryptographic function managed by the device cryptographic key (as embedded in the certificate).

The device shall only share the public key. The private key shall remain protected and ideally never exposed outside the device's secure memory.

Prior to shipping the completed product, the manufacturer shall record the device identifier (ID), UDI, and/or public certificates in the Manufacturer Device Registry.

Device manufacturers shall implement technologies that enable the generation and secure storage of cryptographic material, including keys, passphrases, and certificates, and other services that help protect the interactions between subassembly components. Example implementations of these include Trusted Platform Module (TPM), TrustZone, and Secure Enclave.

Prior to field deployment of those devices, device manufacturers shall perform the following:

— In-circuit testing

— Burn-in testing

— Functional testing

— Software-specific security testing (e.g., fuzz or pen testing)

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4.3.5 Manufacturer device registry

Manufacturers of CIoT devices shall have a registry that is accessible by their devices for the purpose of registration, authentication, and authorization of the identity of CIoT devices.

Once the deploying entity installs and configures the device(s), the expectation is that software updates will occur over its lifetime. The entity deploying the updates shall have the means to verify the device's identity, and the device shall have the means to validate the authenticity of the update.

4.3.5.1 Practices and processes

The manufacturer shall reflect the following requirements (4.3.5.1.1 through 4.3.5.1.5) in their internal practices and processes. The manufacturer shall assign owners, typically in the form of roles, to each of the required activities.

4.3.5.1.1 Device identifiers (device ID)

The requirements for device IDs are as follows:

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Shall uniquely identify the device.

— Shall be valid for the life of the device.

— The device software shall have the following:

1) The ability to use cryptographic certificates as device identifiers

NOTE—Digital Certificates can either be obtained through a trusted vendor, generated through the use of certificate management software such as OpenSSL or LibreSSL, or generated by a purpose-built Certificate Management System that abstracts away the complexities. Systems and processes that provide cryptographic keys or certificates should comply with NIST SP 800-57 [B40], Recommendation for Key Management.

2) The capability of binding device identifiers [proprietary ID, S/N, MAC address(es), UDI, DID, etc.] to certificates.

3) Any binding of cryptographic keys shall be to the public key.

4) If the device uses symmetric encryption, the binding may result in a higher security risk due to shared keys.

NOTE—IDs and certificates have differing functions and lifetimes and, therefore, cannot be the same.

4.3.5.1.2 Properties of the device

Properties of the device are as follows:

— The manufacturer shall securely generate the device ID during manufacturing (provisioning).

— The device shall securely store its device ID (e.g., in hardware-protected memory).

— The manufacturer shall securely store the device ID in the Medical Device Registry and/or Device History Record (DHR).

4.3.5.1.3 Generalized requirements for a medical device registry

The generalized requirements for a medical device registry are as follows:

— Identifiers stored in the registry are sufficiently secure (content and function of registry).

— The manufacturer shall enter the device ID into the registry prior to shipment of the final completed product.

— Device IDs shall be issued utilizing recognized trust anchor processes and practices.

— Medical Device Registry shall store, at a minimum, the following attributes: device ID, OS versions, manufacturer, make, model, S/N, asset tag ID, and PHI attributes.

— If third-party manufacturers are used, device ID shall be technically and legally protected, consistent with applicable requirements.

4.3.5.1.4 Functions of the device ID

The function requirements of the device ID are as follows:

— Shall be used for tracking device attributes by the deploying organization.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Shall be used for identification of devices for service and support purposes by the deploying organization or manufacturer.

— Shall be used for management of device lifecycle (e.g., shelf life) by the deploying organization or manufacturer.

4.3.5.1.5 Functions not suitable for device ID

The functions that are unsuitable for the device ID are as follows:

— Although device IDs should be unique to each device manufactured, manufacturers shall not use them to support security and cryptographic functions.

NOTE—Device IDs follow a set pattern and are predictable; therefore, using them as the basis for strong cryptographic functions nullifies the benefits of strong cryptography.

— Security and lifetime requirements for device IDs and cryptographic certificates are fundamentally different. The requirements may utilize related technologies and implementations; however, they shall be distinct from each other.

— Manufacturers may embed device IDs in a certificate as supplemental information. For example, when using X.509 certificates, custom fields or extensions can be used to store the ID.

— Certificates need to fulfill a set of requirements that device IDs cannot fulfill:

1) Devices shall secure certificates and keep them secret [ideally generated as a public/private key pair with the private key generated and remaining on the device (i.e., the key is never exposed) and the public key is shared].

2) Devices shall have a limited life and support revocation and re-issuance.

3) Devices shall allow multiple certificates per device to support differing functions (secure boot, code signing, encrypted communication, authentication, authorization, etc.).

4.3.6 Decommissioning

At a defined point in the CIoT device lifecycle, the current operator of the device may determine that the device has reached the end of its useful life within the organization. It is widespread practice for CIoT devices to be removed from service from one organization and resold (through third-party organizations) to other organizations. The decommissioning process is the sequence of events that shall occur to help verify that the operator removes all identifying material (e.g., certificates, public keys, W3C decentralized identifiers) from the CIoT device that was created and issued in the processes of onboarding and using the device prior to it being redeployed or resold.

Since there are many varieties of major operating systems, and each requires significant manual work to arrange the material in accordance with HIPAA and HITECH requirements or to the standards of GDPR for demonstrable proof to a Supervisory Authority under Article 36 [B8], the manufacturer shall have the device itself perform the erasure of operator-installed or configured identifiers and certificates.

Subclause 6.12 provides greater detail on decommissioning processes.

4.3.6.1 Practices and processes

The manufacturer shall reflect the following requirements (4.3.6.1.1) in their internal practices and processes. The manufacturer shall assign owners, typically in the form of roles, to each of the required activities.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.3.6.1.1 Recycling/repurposing

When recycling or repurposing technology, technology companies such as parts recyclers, qualified disposal organizations, resellers, or remanufacturers, shall establish full traceability forward and backward as it relates to being able to determine initial use, new use, and end-of-life. It is critical that technology that has reached end-of-life, shall be disposed of or decommissioned such that the technology cannot be consumed by another technology, where that recent technology functions in the same or near-same way as previously defined.

Further, if end-of-life technology is deemed viable for repurposing, then all previous data that might be linked with a patient, or configurations, certificates, or identities linking to a specific care provider and/or EHR system, shall be destroyed by the recycling/repurposing organization, where destruction of that data can be confirmed through testing and validation practices. Lastly, the organization responsible for the recycling/repurposing of the device shall maintain data associated with the appropriate decommissioning or destruction of a device.

The recycler or reseller organizations shall perform a full erasure and rebuild of the device to factory "new" standards as part of the refurbishment process before selling or deploying the device to a new customer. This shall include the following:

a) Replacement of persistent storage.

b) Wiping of all non-replaceable storage to NIST SP 800-88 Rev. 1 [B42] (or equivalent) standards.

c) Reinstallation or resetting of the operating environment to factory parameters.

d) Updating the device to the most current firmware version.

e) Testing the device to verify that it meets operational parameters set by the manufacturer.

f) Creating and maintaining documentation around all actions performed on the device.

g) Removal of organization electronic identifiers, certificates, and asset tags.

4.4 Macro view—Inter-device and systems

Whereas traditional identity management has been concerned primarily with people interacting with online services, the trust and identity ecosystem of CIoT includes people, organizations, and devices (POD), referred to in this standard as TriPOD. Thus, the environment that is in scope for this standard encompasses all three types of entities and the trust and identity interactions that take place among them. Figure 4 uses one scenario referred to as "Hospital @Home" in Annex B of this standard to illustrate the CIoT environment and the components that are in-scope for compliance. In this scenario, a manufacturer produces a portable clinical device and markets that device for patient use outside of a clinical setting. A clinician prescribes a patient of a healthcare clinic a care plan that includes this type of portable device, and the patient acquires the device and uses it in their home setting.

Figure 5, Figure 6, and Figure 7 address each of the three entities separately and provide examples of their trust and identity interactions within the context of the "Hospital @Home" use case (UC).

ULNORM.COM: Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

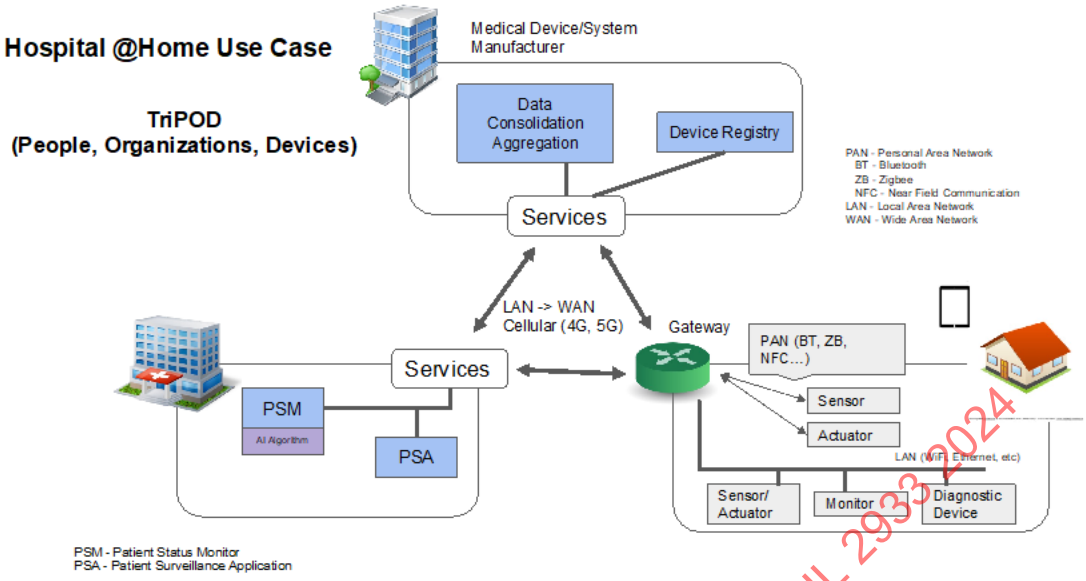

Figure 4—Trust and identity interactions of people, organizations, and devices in the CIoT Hospital @Home use case

Figure 5 addresses the "people" component of the Hospital @Home use case for trust and identity events and interactions. As indicated above, the Hospital @Home scenario centers around a clinician prescribing a patient of a clinic a portable clinical device for use in a home setting. The first identity event takes place when the clinic's electronic systems establish the patient's identity. An application on a remote controller may control the portable device that the patient takes home. In this case, the patient and a clinician/caregiver begin by establishing their identities in the application and performing a pairing of the remote controller and the portable clinical device. Identity establishment involves the creation of credentials, and the patient and clinician/caregiver will use these credentials to authenticate to the remote controller in subsequent interactions.

Solution providers of applications that enable patient credential creation and device pairing shall incorporate industry-standard security mechanisms such as multi-factor authentication (MFA) and token-based access into the applications. The clinical device may upload its data to the cloud storage of the device manufacturer. Thus, the patient, clinician/caregiver, and a Healthcare Practitioner from the patient's clinic will need to have their identities established in the device manufacturer's electronic systems so they may later authenticate and view data from the device. The Healthcare Practitioner will also need to establish their identity to the patient's home network—which may be through a Gateway—to communicate directly with the portable clinical device. Once the Healthcare Practitioner's identity is established, the practitioner can authenticate to the Gateway for subsequent interactions. Solution Providers of applications that enable people to have trust and identity interactions within the CIoT environment shall incorporate industry-standard security mechanisms such as MFA and token-based access into the applications.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

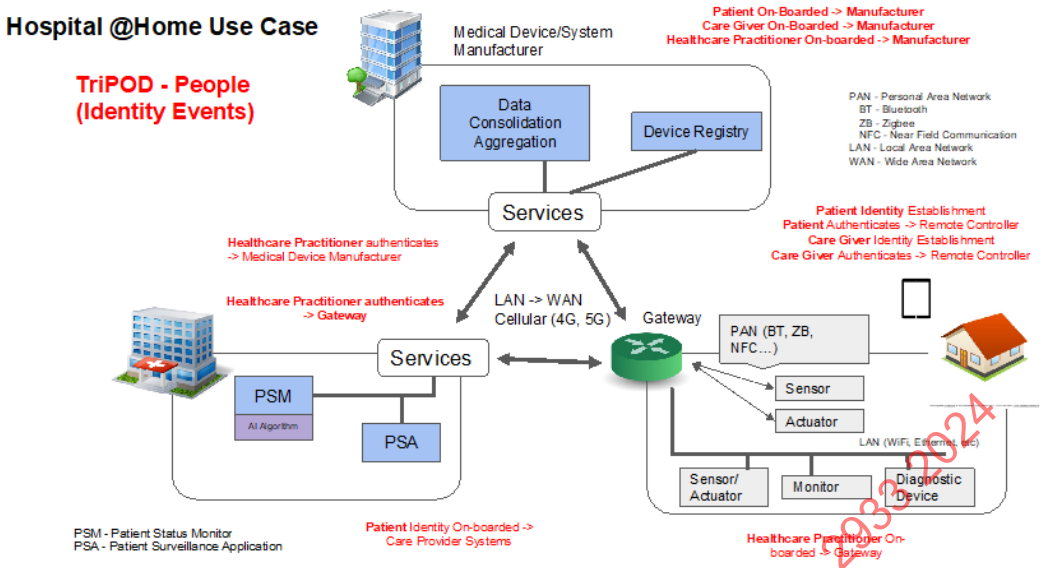

Figure 5—Trust and identity events of people in the "Hospital @Home" use case

Figure 6 depicts the trust and identity events and interactions that involve "organizations." The device manufacturer will need to communicate with the device for a variety of reasons such as to install updates or troubleshoot problems. Thus, the device manufacturer will need to design and/or implement a process to on-board their identity to both the patient's home network and the network of the patient's clinic/care provider to enable communication with a device in either of these locations. Once the manufacturer establishes their identity to these networks, the manufacturer shall use their credentials to authenticate in subsequent interactions. The device manufacturer shall adhere to the trust and identity requirements enumerated in 4.3 of this document to be TIPPSS compliant.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

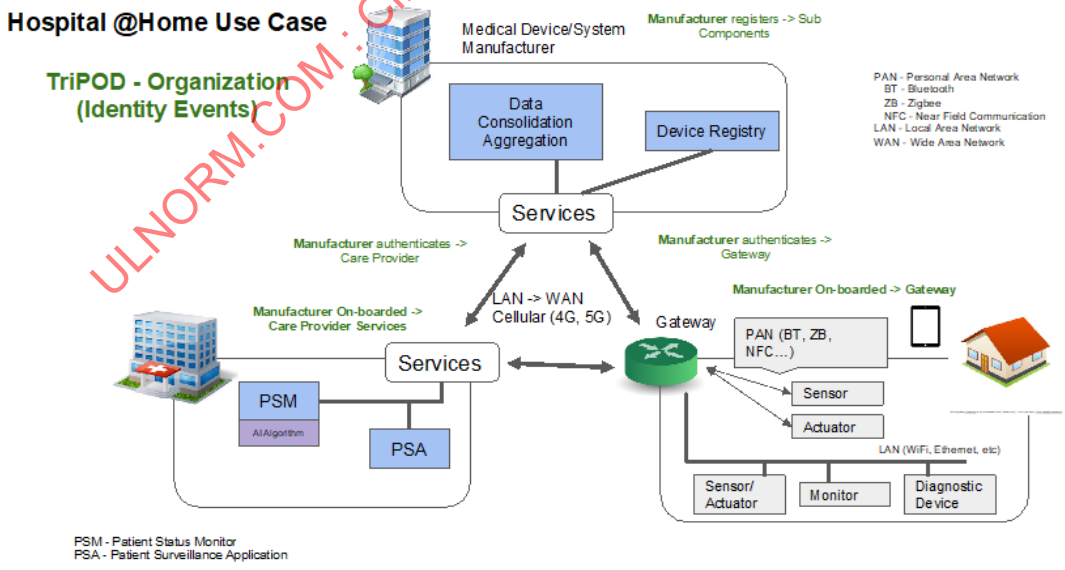

Figure 6—Trust and identity events of organizations in the "Hospital @Home" use case

Copyright © 2024 IEEE and ULSE. All rights reserved.

Figure 7 illustrates the trust and identity events and interactions that involve "devices." In the context of Figure 6, devices/things include both hardware and software and represent the largest number of identity interactions of the three TriPOD entities. The clinical device begins its "life" by having its identity established/registered in the manufacturer's systems. Within the home setting, the CIoT device shall be on-boarded to the patient's local area network (LAN) and Gateway, and the device shall be paired with the Remote Controller. Gateways establish their identity to systems and services that exist at both the manufacturer and the clinic/care provider. In addition, the manufacturer shall register the clinic/care provider's identity to enable bilateral, authenticated communication. CIoT devices/things shall adhere to the requirements enumerated in 4.3 and 4.4 of this document to be TIPPSS compliant within the CIoT environment.

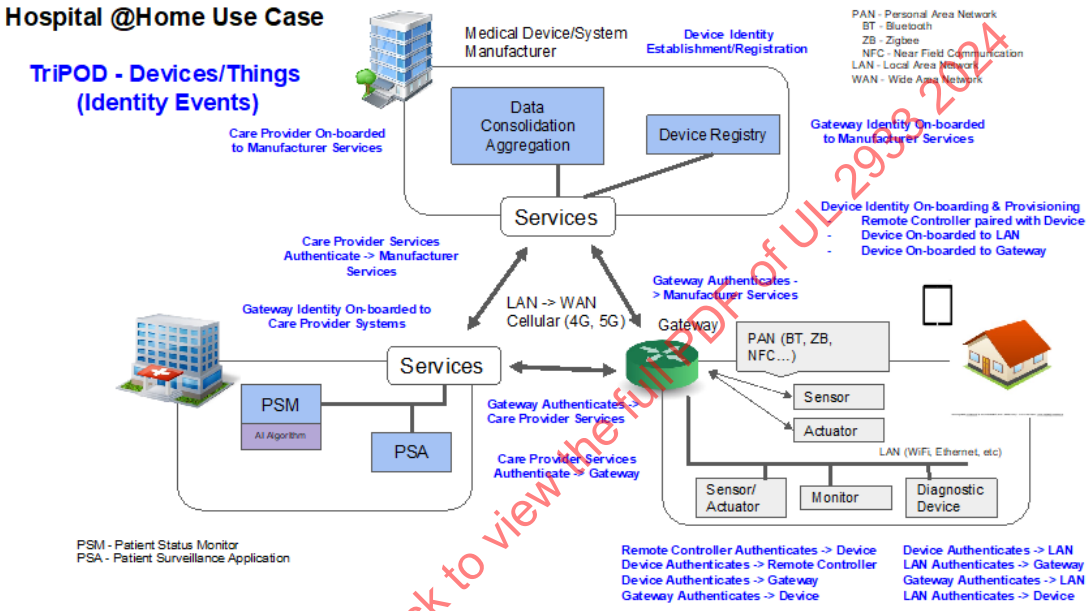

Figure 7—Trust and identity events of devices in the "Hospital @Home" use case

4.4.1 User-managed software

User-managed software is software that connects to or interacts with a CIoT device. The device may store the software on local disk storage or in the cloud. The location where the software executes is determined and managed by the user (operator).

Manufacturers of user-managed software shall supply, or link to, an SBOM that provides a qualified list of all software components [including programs, libraries, and software development kits (SDKs)] on which the software is dependent.

Since software and vulnerability naming and versioning can be inconsistent between platforms, tools, and reference databases, manufacturers shall use commonly used conventions for naming and versioning, and standardized data formats to exchange SBOM data.

4.4.1.1 Practices and processes

The manufacturer shall reflect the following requirements in their internal practices and processes. The manufacturer shall assign owners, typically in the form of roles, to each of the required activities.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.4.1.1.1 Software updates

Before applying any software updates on a device, the update process shall authenticate the following:

a) *The source of the update command*—If an automated interface triggers a software update process, it should validate the origin of the update command/instruction. The device shall log and retain all software update commands.

b) *The source of the software update image*—The device shall validate the source of any software update image prior to downloading it to the device.

c) *The integrity of the software update image*—Software update processes shall have a mechanism to validate the integrity of the received update image file. The software update process shall validate the image prior to applying any updated image to the device.

The update processes for application and operating system software shall be kept as separate and distinct operations.

4.4.1.1.2 Software as a Medical Device (SaMD)

Healthcare experiences provided through traditional and novel infrastructure, platforms, virtual reality, and services involve an array of technology, including but not limited to hardware, devices, and software. The healthcare ecosystem is also rapidly evolving and growing in the utilization of SaMD. SaMD is software intended for use in one or more medical purposes that performs these purposes without being part of a hardware medical device. SaMD is not software integral to a medical device, or software used in the manufacturing or maintenance of a medical device. Novel trust and identity issues are emerging in association with SaMD that do not exist in non-medical systems, and that do not exist in medical devices, and therefore shall be addressed by the manufacturer for the benefit of the protection and safety of humans.

Examples of SaMD include software with a medical purpose that operates on a general-purpose computing platform, or software connected to a hardware medical device, but the device does not need it to function, or it is not an accessory to the device.

Establishing trust

Each entity (see definition for an entity in 3.1.4) in the IoT model shall establish a trust relationship before exchanging data, which may include confidential and privacy-restricted information. A CIoT device often requires communication and, therefore, the establishment of trust with many different entities to fulfill its intended function throughout its device lifecycle. These entities could include those used to securely onboard and provision the device and connect to networking devices, gateways, controllers, servers, and applications. In addition to trust relationships established with hardware and software components, various users, such as caregivers, technicians, and vendors, may need to interact with the IoT device. Figure 8 illustrates various trust relationships that PODs may establish in an IoT architecture, and Figure 9 illustrates the CIoT device lifecycle roles.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

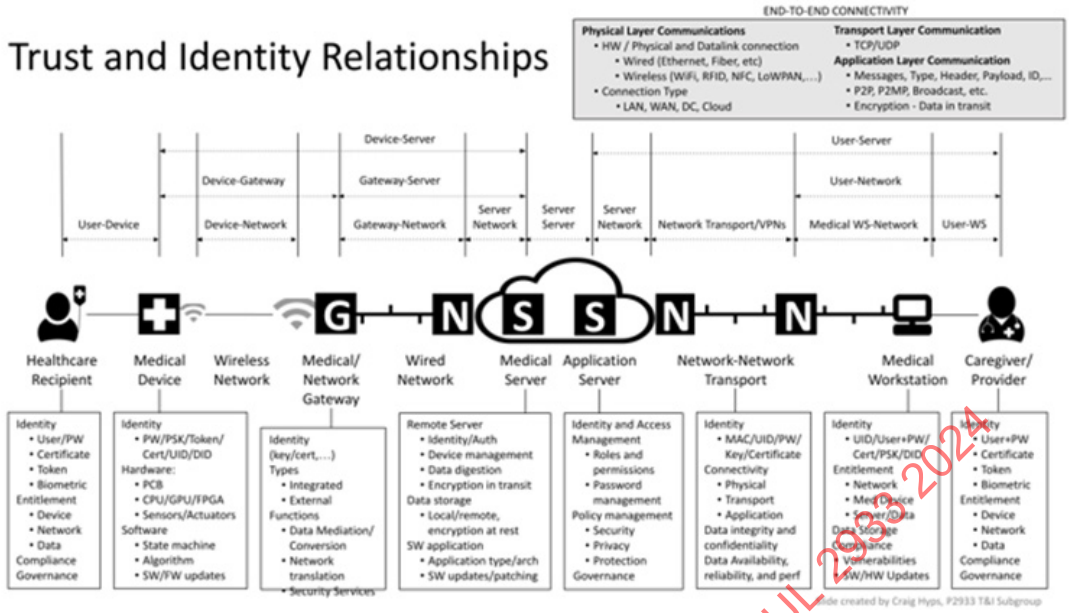

Figure 8—Trust and identity relationships

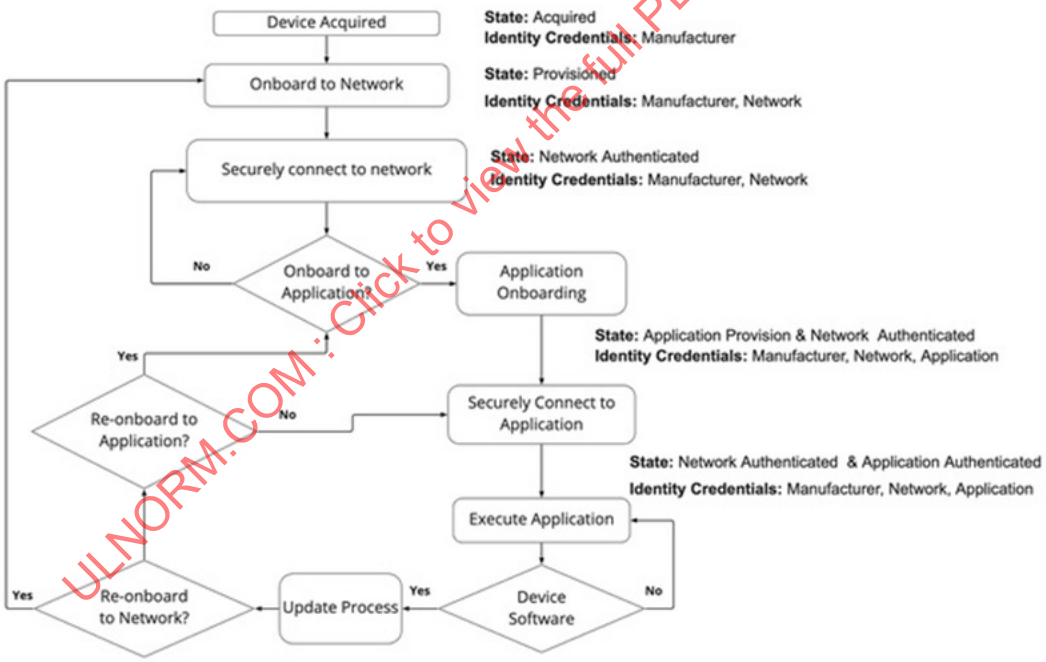

Figure 9—CIoT device lifecycle roles

This standard does not dictate the specific implementation of Zero Trust principles but does embrace the intent and goals of a Zero Trust approach. Zero Trust is not a standard, but an approach to protecting devices and establishing secure communications between entities in a Zero Trust Architecture (ZTA). ZTA advocates that no component of the system should implicitly trust another; rather it should challenge any access to any secured entity or its data, continuously verify access, and grant only the access required per its role or function.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Each trust relationship is unique and may, therefore, employ the same or different methods, including identity credentials. Each trust relationship shall include the following core elements: authentication, identity, context, authorization, and audit/accounting.

4.4.2 Authentication

Authentication provides evidence that the entity is what or who it has declared itself to be. There are multiple forms of identity and different methods to convey and verify those credentials by peer or hierarchical entities, which may interact with the primary entity and establish a trust relationship. Authenticity is the basis for establishing trust in the data coming from a device.

Specific use cases determine which forms of identity and conveyance methods are appropriate based on the entity and use case.

4.4.3 Identity

Identity is an essential component of authentication. While some authenticating systems may leverage device identifiers, not all identifiers express a true and verifiable identity of the device. An example is MAC-based "authentication" or MAC Authentication Bypass (MAB) methods, which use the network address of the device to distinguish the device. Manufacturers shall not use this as a unique identifier since other devices can easily spoof or duplicate the value. Similarly, the use of shared keys such as pre-shared key (PSK) mechanisms cannot uniquely identify an individual entity unless the key is unique to that entity. Consequently, these mechanisms do not represent true authentication.

To properly authenticate a CIoT entity, the CIoT device or user shall have a unique verifiable identity. An identity may include one or more unique identifiers such as a PKI certificate, key, username/password credentials, and biometrics. The CIoT device shall maintain its identity over its device lifecycle to improve resilience and help prevent misuse due to compromise. Identity maintenance operations should include password complexity and periodic updates, certificate expiry, renewal, and revocation. Identity assertions, as provided by Single Sign-On (SSO), such as OAuth or tokenized mechanisms like Kerberos, shall undergo continuous verification after successful session establishment by the device.

The deploying organization shall consider the sensitivity and impact of compromise in determining the inherent strength of the identity. Strength can be measured based on cipher strength, key lengths for certificates, key/credential length, and complexity.

The authentication framework includes the components and systems used to communicate and verify identities, such as identity management systems, including identity stores, PKI infrastructure, and decentralized identifier (DID) systems.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4.4.4 Context

In addition to identity, context is a critical factor in establishing trust. Context includes variable factors and attributes such as the following:

a) Location—Where are the device, peer, or hierarchy located? Is the originating location of the device or user expected or in a trusted domain?

b) Date/Time—When is a trust established? Is the communication occurring during expected hours of operation?

c) Communication method—Is the device or user connecting from an expected or approved method or medium?

Copyright © 2024 IEEE and ULSE. All rights reserved.

d) Compliance—Is the device compliant as determined through direct communication or reference to a trusted third-party system?

e) Risk—Is the device known to be vulnerable due to hardware/software versions, lack of patching, or lack of other protective agents or methods?

f) Behavior—Is the device communicating as expected?

For existing devices that lack identity or authentication ability, the use of context becomes a critical factor in establishing trust. While this standard is based on the use of an explicit identity to establish trust and secure communications, it does recognize the potential need to elevate trust and increase security for legacy devices. To the extent that legacy devices do not implement the requirements listed in this standard, trust and security may be compromised. Stronger trust relationships can be established by incorporating both explicit and durable identity combined with multiple contextual factors as listed in a) through f) above.

4.4.5 Authorization

Authorization is the process of establishing permissions to the device, user, server, application/service, or other entity in the CIoT architecture based on its role. each CIoT device has a specific role and shall require specific permissions to accomplish its core function in healthcare delivery. Likewise, different systems and personas interact with the device, and each for a different reason. To reduce the risk to or from any device, user, other entity, or to the data held or communicated, the CIoT system shall only grant permissions necessary for the IoT entity to perform its essential functions. This is the principle of least privilege (PoLP) concept. Furthermore, access permissions to any other entity, including its configurations or data, shall be commensurate with the role of the entity as determined by the deploying organization. This concept is the basis of role-based access control (RBAC).

Authorization is a function of identity as well as context.

4.4.6 Accounting/Audit

Accounting is the process of auditing access to the device, remote server, or entity in the IoT system. This includes the servers or applications that manage and contain the data from the device. Key accounting processes include the following:

a) Devices and users shall authenticate to devices or the servers that manage the device or hold and communicate the data from the device.

b) Deploying organizations shall grant each recipient or user of the device only the privileges required to perform the required function, and those in conformance with regulations.

c) Devices and/or supporting systems, such as servers, shall record all access to the CIoT device, whether to receive data from the device, add data to the device, or manipulate the configuration or functioning of the device.

The device manufacturer shall design the discrete CIoT device network connection such that it is continuously monitored, and the session automatically terminated based on the explicit completion of the data exchange, by the direct intervention of the communicating peers, or by a timer based on the risk of exposure of an untrusted entity from making an unauthorized connection to one of the peers through the exploitation of a previously authenticated session.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.4.7 Device onboarding

The manufacturer may provision device bootstrapping information to the device during the manufacturing process. The manufacturer shall provide the information to the device before it initiates the onboarding process. This information pertains only to the device and, once installed, should not change over the lifetime of the device unless it is reprogrammed by the manufacturer.

Device bootstrapping information should include identifiers, keying material, and additional data required to establish mutual trust between the device and the onboarding network, such as the following:

a) Device identifier (e.g., X.509 certificate–DevID, X.509 iDevID per IEEE Std 802.1AR [B17], Device Identifier Composition Engine [DICE] Compound Device Identifier [CDI])

b) Secret (e.g., private key, public/private key pair, pre-shared key). Secrets shall be unique. As such, a PSK shall implement a unique key per device, such as Identity PSK (iPSK), Private PSK (PPSK), or dynamic PSK.

c) Serial number—the unique serial number assigned to the device.

d) Device information declaration or similar mechanism such as a voucher request.

e) Manufacturer Authorized Signing Authority (MASA) URI.

NOTE—The device information declaration is the responsibility of the manufacturer, and the manufacturer may include it with the device. The manufacturer may also sign it and provide it to the network onboarding component for the owner for use during onboarding. This is to allow the IoT device to establish trust with the network as a precursor to the acquisition of onboarding credentials. Device information declaration is optional if the trust relationship is one-way and the IoT device does not require verification of the onboarding owner or network. Mutual trust between the IoT device and the network onboarding component requires device information declaration.

Various standards, such as Bootstrapping Remote Secure Key Infrastructure (BRSKI) and Device Identifier Composition Engine (DICE), detail methods to establish identity and securely bootstrap CIoT devices to the network. Key tenets of these architectures include the establishment of identity and trust between a device and its owner, to enable at scale the secure transfer of ownership, and to provide an audit of ownership. The BRSKI and DICE standards are not mutually exclusive, and one or more elements of each may be implemented simultaneously. While this standard does not mandate a specific identity and onboarding standard, it does mandate the implementation of identity assertion and trust establishment as outlined in these standards to include the following:

— The manufacturer shall assign a unique identity or secret to the device that is uncorrelated and statistically unique.

— The unique manufacturer device identity or secret should be at least 256 bits and have the same security strength used in derived identities.

— The unique manufacturer device identity shall not change over the lifetime of the device unless reprogrammed by the manufacturer.

— Manufacturers shall store the identity or secret in a manner that prevents tampering, such as non-volatile write-once storage or electronic fuse (eFuse) memory.

— Manufacturers shall safeguard secrets in a secure storage element that prevents them from being extracted, tampered with, or modified without detection. Since device bootstrapping credentials should not change over the lifetime of the device, and if the credential is a certificate, the certificate should not expire for the expected and documented life of the product.

— The unique manufacturer-assigned identity should be used to bootstrap the device and provision new identities for trust establishment for higher layer services, but not directly for trust establishment. This process enables multiple unique derived identities to be generated and reprovisioned for

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

different trust relationships, including network authentication, device attestation, firmware and software updates, and secure communications with services, applications, and users.

NOTE—DICE enables even the smallest and least computationally equipped devices to implement strong identity and secure device updates. DICE works by organizing the boot process into layers and creating secrets unique to each layer and configuration based on a unique device secret (UDS). DICE produces a Compound Device Identifier (CDI) using a simple cryptographic one-way key derivation based on the UDS and the identity of the boot code. Successive boot and application layers implement a similar process by which the next layer's identity is derived based on the previous layer's identity and software. Additional security is provided by implementing power-on latch functions such that lower layer identities are only available temporarily after the device reset, and identities for a prior layer are deleted from memory before passing control to the next layer.

The bootstrapping process shall provide mechanisms to support the establishment of mutual trust between the device and the onboarding network (device owner) that include the following elements:

- The onboarding component or registrar ascertains the identity of the candidate device.
- The onboarding component or registrar ascertains whether the onboarding domain owns the candidate device and can authorize it to enroll or onboard to the owner's network.
- The device ascertains the identity of the onboarding component or registrar.
- The device ascertains whether the currently connected network is a valid and authorized network to join.

To support security capabilities such as proof of ownership and to onboard only to authorized networks, a device shall include a device information declaration or similar mechanism such as a voucher request as specified in IETF RFC 8995 [B11]. A device information declaration or similar mechanism allows the IoT device to consult the device ownership information to determine whether the network that is trying to onboard the device also owns it. If so, this provides assurance that the acquired device can be onboarded and used on this network. If the owner of the device does not own the network that is trying to onboard the device, the IoT device should consult the list of authorized onboarders in the device information declaration to verify that the onboarding network is owned by one of the entities authorized to onboard it.

Among the information asserted in the device information declaration may be the following:

- Certificate of the device owner.
- Certificates of all entities (if any) that the device owner has authorized to onboard the device (in addition to the device owner).

Creation and maintenance of the device information declaration shall be the responsibility of the device manufacturer (which is the first owner of the device), and as the owner of the device is transferred from one entity to another during the device lifecycle, any ownership information that is present in the device information declaration shall be kept up to date, with each change of ownership clearly recorded by the deploying organization.

During the bootstrapping process, the device communicates with the network onboarding component of the network. After both the device and the network onboarding component authenticate, then the device and the network onboarding component establish a secure channel. The network onboarding component then uses the secure channel to provision the device's onboarding credentials to the device. The new credential establishes the identity and ownership of the onboarded device. This credential (e.g., X.509 iDevId as referenced in IEEE Std 802.1AR [B17] or a certificate signed by the device owner domain CA) establishes the device's identity on the owner network. The credentials shall be renewable by the deploying organization to help prevent compromise. In the case of a certificate credential, the certificate shall have an expiry and be renewable by the current owner. Additionally, the owner authenticating identity store or domain CA shall have the ability to revoke the credential or certificate as required based on retirement or transfer of the device or due to potential compromise of the device.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

When onboarding is complete, the device has been provided the information it needs to connect to the local network, such as a network SSID and Extended Authentication Profile (EAP) profile and device certificate, and the new domain can manage it. The bootstrapping and onboarding process should only recur if the user resets the device to factory defaults, or if ownership transfers to a new domain and owner.

The network access control systems, such as switches, controllers, routers, firewalls, or gateways should provision Access Control Lists (ACLs) to limit the device's communications to only those required for it to perform its intended function.

To facilitate the generation and provisioning of access control policies, device manufacturers should provide prescriptive guidance regarding the required communication profile of the devices manufactured. This manufacturer-driven policy serves to simplify and automate the PoLP based on detailed knowledge of the device's expected communications. Manufacturer usage description (MUD) is an example framework that enables vendors to prescribe required communications using centrally hosted MUD files. MUD files hosted on a MUD File Server define a device's expected communication profile in a form that allows translation into access control lists (ACLs) that networks and associated security mechanisms can enforce.

The MUD solution consists of the following three components at its core:

1) A URL that an IoT device emits when it connects to the network using methods like DHCP, Link Layer Discovery Protocol (LLDP), or attributes in the certificate.
2) An Internet-hosted file, also known as a MUD file, that this URL points to. This file contains an abstracted policy that describes the level of communication access that the IoT device needs to perform its normal function.
3) A core process that receives the URL from the IoT device, retrieves the file from the MUD File Server, and establishes appropriate access controls in the network for that IoT device.

Independent of the methods used to determine and apply access controls, the deploying organization shall monitor the behavior of each device and that of its peers for anomalous and unexpected communications.

4.4.7.1 Practices and processes

For onboarding a device:

a) The operator shall move the device into inventory using existing supply chain processes.
b) The operator shall register the device into inventory using existing asset management processes.
c) If the device requires connection to an existing system to download device and security configurations, and software updates, the operator shall connect it to the existing system to complete the configuration and receive them.
d) If devices use a wireless network for configuration that isolates the device from other devices on the network, no inbound connections from other networks shall be allowed by the deploying organization.
e) If the device does not require connection to an existing system, the operator shall connect it to an isolated network to configure, secure, patch, and update to remediate vulnerabilities.
f) After connecting to the network, the operator shall connect the device to other systems to interface with to get what it needs to complete configuration, such as Digital Imaging and Communications in Medicine (DICOM), FHIR, or HL7 configurations to send/receive data.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.4.7.2 Device identities

Mutual authentication between IoT devices and IoT servers is an important part of secure IoT systems. PKI certificates are an example of one of the most common and recommended methods to enable secure communication and control access to IoT devices and services.

Using PKI, one can provide trusted identities to IoT devices and services, allowing authenticated and encrypted communication without pre-determined cryptographic keys. PKI also supports the use of authorization certificates that authorize the certificate holder (a device or a service) to access a certain resource or to belong to a specific group.

When designing a PKI certificate management process, manufacturers shall establish and maintain trust in the IoT devices and servers throughout the entire device lifecycle and shall seamlessly control their identities. This means that manufacturers shall establish trusted identities for the device, server, or their components early in the product lifecycle.

Each IoT device shall go through the following steps:

— The IoT device registers on the IoT server.

— The IoT server issues a PKI certificate for the device.

— Provisioning of the certificate (and optionally of the private key) to the intended IoT device and server in a secure way. NIST SP 800-130 [B43] describes methods on how to accomplish this.

4.4.7.3 Secret material protection

Systems need to have the ability to protect critical information about subjects from unauthorized exposure to both internal and external threat actors. It is also critical that the processes used to manage the mechanisms used to protect this information, such as encryption and cryptographic hashing, have a commensurate level of protection based on established and tested industry standards.

4.4.7.3.1 Provisioning

Provisioning of certificates shall use a process aligned with NIST SP 800-57 [B40] during the device production or deployment process to help prevent certificate exposure.

Organizations shall implement secure certificate management processes to mitigate the risks of improperly provisioned certificates.

4.4.7.3.2 Protecting secure material on the device

Device manufacturers shall implement the Trusted Platform Module (TPM) standard (or equivalent), which enables the generation of cryptographic keys and other services that help protect the interactions between subassembly components.

— Device manufacturers shall perform in-circuit testing, burn-in testing, and functional testing prior to field deployment of those devices.

— Device manufacturers shall perform authenticity checks on all credentials, passwords, and certificates used to access secured material on the device.

— Device manufacturers shall deny access to secured material if the authenticity checks fail.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Device manufacturers shall use cryptography, encryption, and digital signatures, either by themselves or encompassed in protocols such as Kerberos, OAuth2, or SAML, to provide assurance and non-repudiation of the identities used to access secured information.

— Device manufacturers shall deny access to secure material if non-repudiation checks fail.

4.4.7.3.3 Confidentiality/Privacy

Encryption/Decryption methods, cryptographic hashing, and digital signatures shall utilize algorithms, methods, and key lengths discussed in ISO/IEC 19790:2012 [B25] and ISO/IEC 24759:2014 [B28] to protect secured material.

Device manufacturers shall check NIST SP 800-131A [B44] to verify that the methods, algorithms, and key lengths utilized meet their minimum-security standards.

Device manufacturers shall not use methods, algorithms, and key lengths not permitted by NIST SP 800-131A [B44], or not discussed in ISO/IEC 19790:2012 [B25] and ISO/IEC 24759:2014 [B28].

4.4.7.4 System management

The systems used to perform these functions need to initialize into a known good state utilizing software and hardware that provides reasonable and appropriate protection against tampering. Common provided anti-tampering techniques include encryption, hashing, and digital signatures in hardware and software. This is so users can trust the system to be a reasonable and appropriate guarantor of trusted information. The techniques of code signing and secure boot, along with the proper usage of encryption and hashing techniques, can help ensure that the system functions as a trust anchor.

4.4.7.4.1 Code signing

Code signing is the act of authenticating that actors have not tampered with or maliciously altered software, where the owner/creator of the (centralized versus decentralized) software sign all released software using a system involving a pair of keys, one public and one private, at a minimum.

4.4.7.4.2 Secure boot

Secure booting is a standard adopted by the computer industry to initialize a computer into a known good and secured state using trusted software as determined by the computer manufacturer. Accordingly, computer manufacturers shall utilize secure boot practices with boot software that is appropriately signed and then validated at boot time, such that control can be handed from the boot software to the computer operating system (OS). ISO/IEC 19678:2015 [B24] discusses this.

4.4.7.4.3 Trust anchors

The result of the utilization of these techniques is an authoritative entity that infers trust from the usage of numerous protection techniques to help ensure system integrity. This is known as a trust anchor. NIST [B40] defines this as “An authoritative entity for which trust is assumed.” The usage of approved encryption/hashing/digital signature algorithms and key lengths in software and hardware, along with Code signing and Secure boot techniques, provide a base for proving this assumption correct.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.4.7.5 Tokens

In many systems, once authenticated, the user shall obtain an access token. Tokens are pieces of data that allow application systems to perform the authorization and authentication process.

a) Access token: Access tokens are credentials used to access protected resources. Systems can use access tokens as bearer tokens. A bearer token means that the bearer (who holds the access token) can access authorized resources without further identification.

b) Refresh token: Access tokens may be valid for a short amount of time. Once the token expires, client applications can use a refresh token to "refresh" the access token. That is, a refresh token is a credential artifact that lets a client application get new access tokens without having to ask the user to log in again.

The system shall include access delegation capability with an appropriate granularity of permissions whenever feasible.

The system shall use a mechanism such as OAuth for applications or APIs that interact with CIoT devices.

OAuth2 and OpenID Connect are token-based authentication and authorization standards and profiles. OAuth2 uses issued tokens to enable delegated access to server resources on behalf of a resource owner and could allow a device to gain the necessary permissions to represent a user to internal and external services. Resource owners can quickly and easily revoke device permissions by simply invalidating the assigned OAuth2 access tokens. Privacy tools like UMA could provide needed granular consent capabilities by enabling control over what devices, services, and users can access data, for how long, and under what conditions. APIs allow two software programs to communicate with each other by providing a complete set of rules and specifications to facilitate interaction. A REpresentational State Transfer (REST) API framework adheres to constraints that make it attractive for connecting users, devices, and things to applications and services in an IoT environment. Statelessness, meaning that each call is independent and contains all the data necessary to complete itself successfully, and a uniform interface that allows communication in a single language, independent of the architectural backend of either side, provide the flexibility needed in an ecosystem consisting of a range of services and applications on many different platforms and languages. The REST API constraint of layered systems, with each layer having a specific functionality and responsibility and different layers of the architecture working together to build a hierarchy, can provide the necessary abstraction and modularity for a scalable IoT environment.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4.4.8 Provisioning

Provisioning is the process of managing access and entitlements to data and resources and making them available to users, devices, and systems. It may involve correlating different identifiers that exist in separate provisioning targets to a single identity. There are a couple of approaches to provisioning that are based on the timing of the provisioning process. One is just-in-time provisioning, and the other is just-in-case provisioning. Just-in-time provisioning means making an identity known to other systems at the point in time that the first attempted access to those systems occurs. Just-in-case provisioning refers to pre-loading all the identities that might potentially need access to a particular system and would be appropriate in situations where the timing of the first authentication for the identity is unpredictable and the need for prompt access is critical. A periodic purge of unused identities shall follow just-in-case provisioning.

4.4.8.1 Practices and processes

NIST SP 800-63-3 [B40] describes the industry best practices and standards that organizations and people can use to provision and manage access to systems and devices.

Copyright © 2024 IEEE and ULSE. All rights reserved.

4.4.8.1.1 Device usage

The use of a device occurs according to the declaration and validation of the device's intended use. Specifically, medical/healthcare devices such as those validated by the FDA or under MDR/IVDR require a declaration of and compliance with their intended use. Devices used outside the declared or intended uses are off-label, where users of off-label devices are subject to increased risks. Further, device manufacturers shall verify the intended use of their devices to help reduce risks to users.

Within the scope for devices used as intended, the use of those devices involves nine steps within and outside of the device manufacturing environment:

a) Device manufacturers shall collect and maintain device records.

b) Device records shall include all data related to the assembly/manufacturing of the device (including rework, testing, and validation).

c) Devices shall log and audit authenticated access to devices for operational and maintenance purposes.

d) Devices shall log all failed attempts to access the device.

e) Devices shall respond to valid commands from the device user.

f) Devices shall provide appropriate status notifications and alerts to device users.

g) Devices shall follow configuration commands and directives to store and process information.

h) Devices shall alert device users when an adverse device or security event occurs that compromises TIPPSS principles.

i) If enabled, devices shall send telemetry, logging, and auditing data to a configuration and/or monitoring system for monitoring and diagnostics purposes.

Depending on the device use case, risk, and available resources, regulators may not require all of the above. Manufacturers shall follow a formal requirement process and shall document any decisions, especially deviations from the previous list.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

4.4.8.2 Practices and processes

Device manufacturers shall comply with AAMI TIR57:2016 [B2] and all associated best practices and standards for applicable use cases and usage scenarios.

Reuse

Reuse of the device occurs when the operator/user determines that the device is no longer to be utilized in its current capacity and/or at its current location. It requires the deprovisioning of the device from its current location and setting and reprovisioning of it at its new location. There are two distinct types of reuse. The first type is reuse within the same organization, in which case the following applies:

— If the device requires connection to an existing system to utilize device and security configurations, and software updates, the operator shall disconnect from the existing system to remove existing configurations.

— The operator shall disconnect from other existing interfacing systems, such as DICOM, FHIR, or HL7.

— The operator shall remove any other site-specific configurations.

— The operator shall follow best practices for onboarding a device in 4.4.7 to prepare the device for usage in its new function and capacity.

Copyright © 2024 IEEE and ULSE. All rights reserved.

The second type is reuse outside the organization, in which case the following applies:

- If the device requires connection to an existing system to utilize device and security configurations and software updates, the operator shall disconnect from the existing system to remove existing configurations.
- The operator shall disconnect from other existing interfacing systems, such as DICOM, FHIR, or HL7.
- The operator shall remove any credentials, certificates, and identity-specific information from the device.
- The operator shall remove any other site-specific configurations.
- The operator shall sanitize the device to NIST SP 800-88 Rev. 1 [B42] or ISO/IEC 27001 Media Handling (A.8.3) standards to remove any configuration information or residual identity data.
- The operator should replace persistent storage media to reduce the risk of data remaining on the device.
- The operator should reinstall operating systems and application software on the devices to reduce the risks of non-default configurations, data, and system libraries presenting issues.
- The operator shall remove any configuration data, such as MAC Addresses or device identifiers, from network management and security systems.
- The operator shall remove devices from any inventory, supply chain, and asset management systems.

4.4.9 Deprovisioning

Deprovisioning is the removal of access to provisioned services and plays a key role in maintaining the security of electronic systems. It can be part of the decommissioning process. Decommissioning refers to the removal of a device from service, while deprovisioning refers to the removal of entitlements and access. A deprovisioned device can remain in service. It is often best practice in organizations to deprovision a device when moving it between locations, as just moving it may cause issues with the device still being configured to work in a previous role. It is also best practice to deprovision a device before resale.

A best practice with respect to deprovisioning is to remove the entitlements and authorizations to services rather than just disabling the authentication credential. This decreases the potential for someone to inherit inappropriate access, as would be the case if an organization recycles usernames and the new “johndoe” user automatically has access to all the services that the old “johndoe” had because the entitlements still exist for that username. It is important to have clearly documented and published rules and time limits regarding deprovisioning, for instance, specifying under what circumstances one loses eligibility to Service X. A best practice would be to send “pending service expiration” notifications or reminders to an individual during that grace period time. Not only does this build trust with users, but it also prevents the extra work of reinstating access if a mistake is made regarding eligibility or the user’s eligibility changes during the grace period.

Users shall be able to deprovision unauthorized or expired access.

Subclause 6.12.2 discusses deprovisioning processes and practices as part of the decommissioning process.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

5. Privacy

5.1 Overview

Privacy is defined by the National Institute of Standards and Technology as “assurance that the confidentiality of, and access to, certain information about an entity is protected.” In the connected healthcare domain, privacy includes safeguarding individuals against potentially harmful or problematic activities related to unauthorized access to personal information, including all types of personally identifiable information (PII) and protected health information (PHI) collection, processing, and dissemination.

Addressing privacy requirements in CIoT data and device interoperability is vital to developing trust in using IoT-based systems in the healthcare domain. CIoT systems require an appreciation of both the ethical and legal milieu as well as the sociopolitical landscape. One of the issues related to the limited adoption of IoT applications among end-users is the lack of trust in IoT devices concerning data protection, privacy, and safety.

The recommendations in this clause detail how to incorporate privacy by design and help maintain privacy throughout the data and device lifecycles for CIoT devices. Figure 10 depicts the approach this standard recommends for preserving privacy in CIoT. There are six key elements that are all interrelated. They are as follows:

a) Data protection frameworks: Considering data protection frameworks from around the world.

b) Privacy by design: Depicting the fact that privacy needs consideration throughout the lifecycle of the device and system design.

c) Data lifecycle: Privacy needs consideration throughout the full data lifecycle (data gathering, sharing, processing, and retention/destruction).

d) Privacy Impact Assessment (PIA): A framework to support developers in addressing privacy requirements.

e) Adaptive privacy solutions: Any privacy control measures put in place need to be adaptive and reconfigurable to address future privacy risks.

f) Context: The context or domain needs to be clear to assess privacy considerations.

This list is not exclusive. Users of IEEE Standards documents should consult all applicable laws and regulations, including those related to data privacy. Compliance with the provisions of this document does not constitute compliance with applicable regulatory requirements. Implementers of this standard are responsible for observing all such laws and regulations.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Figure 10—Privacy overview

The scope of this clause is twofold. First, it identifies privacy requirements for CIoT in data and device interoperability. Second, it develops a Privacy Impact Assessment (PIA) framework or customizes an existing PIA intended to help a system designer and developer determine whether the main privacy requirements have been respected in their design and usage of CIoT devices and data interoperability-based systems.

The audience for this clause includes medical device manufacturers, hardware, software, and service developers, as well as operators and users of connected healthcare systems, including payers, providers, patients, patient advocates, and regulatory experts.

The purpose of this clause is to identify the privacy requirements that the manufacturer should embed within the design and development of interoperable CIoT devices. In addition, it provides end-users and solution developers with a checklist of privacy requirements that should be provisioned in CIoT data and device interoperability systems and linked to the different data and privacy protection frameworks.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

5.2 Privacy requirements identification

The privacy requirements derive from reviewing global regulations and standards related to privacy. Privacy requirements are statements that reference key privacy principles [e.g., the Fair Information Practice Principles (FIPPs), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR) privacy principles] and specify capabilities and functions that those devices and systems shall be able to perform to show compliance with fundamental privacy objectives and applicable privacy regulatory guidance.

Many frameworks, standards, and regulations exist to address privacy in the digital domain around the world. Those elements need consideration when designing and developing CIoT devices and systems.

The privacy requirements identified in this clause are based on the privacy requirements derived from the use cases and listed in Table C.1, which details key topics for this standard as delineated by the lead, support,

Copyright © 2024 IEEE and ULSE. All rights reserved.

and consult (L/S/C) roles for each element of the standard for trust, identity, privacy, protection, safety, and security.

5.2.1 Privacy requirements

The privacy requirements that follow derive from a review of privacy frameworks from around the world, as listed in Annex E. Annex F contains a table representing privacy regulations/guidance and alignment with ISO/IEC 29100:2011 [B31] and additional requirements/comments.

Based on the principles across the frameworks listed in Annex E and Annex F, the following list represents the common privacy requirements that manufacturers shall follow in this standard when developing CIoT-based applications. The mapping of the privacy frameworks in Annex F to the requirements in ISO/IEC 29100:2011 [B31] provides a common base by which organizations can evaluate, develop, and engineer privacy solutions across industries. These requirements are as follows:

- Consent and choice: Applications shall only collect information from a data subject when informed legal consent has been obtained. The applications shall also provide the data subject with a choice to withdraw their consent at any stage.
- Purpose legitimacy and specification: Applications shall only allow the collection and processing of a data subject's data for specified and legitimate purposes for this collection/processing. Unless separately and subsequently authorized, applications shall forbid the processing of collected data for secondary usage.
- Data collection limitation and data minimization: The data collected by the deploying organization shall be the minimum necessary and limited to the purpose of use. Data subjects should have the right to start/stop the data collection process at any given time.
- Data usage, retention, and storage limitation: At the end of the data lifecycle, the application shall safely delete data. Applications shall keep personal data for no longer than is necessary for the purpose for which it was captured.
- Accuracy and quality: Data collected by the deploying organization shall be accurate and up to date, and applications shall delete or rectify incorrect data.
- Notice and access: Deploying organizations shall give data subjects notice when their data is collected, provide data subjects access to their data, and update them when required throughout the data lifecycle.

  NOTE—This includes data collected on the device as well as accumulated by a hosted service.

- Individual participation and transparency: Data subjects should have full control over their data and know who has access to it. They should also have the right to start or stop the data collection process at any given time.
- Accountability: Whenever there is a privacy breach, the application shall be able to maintain records related to the breach events.
- Data protection: Organizations shall use reasonable and appropriate methods determined by a risk management or Information Security process methodology such as ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework (NIST CSF), or OCTAVE to protect information about data subjects.
- Privacy compliance: Implemented systems and processes used to safeguard the privacy of data subjects' information shall be measured and demonstrated by the manufacturer using an industry-accepted framework or standard in conjunction with a corresponding Information Security management framework [such as ISO/IEC 27701:2019 [B30] or the NIST Privacy Framework 1.0 (or greater)]. Local (i.e., geographic) privacy regulations establish the environment in which CIoT

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

devices are intended to operate. As such, variations in regulatory frameworks will impact the capabilities and the associated compliance standards that devices shall meet.

5.2.2 Privacy requirements for Clinical IoT data and device interoperability

There is a need to map the identified privacy requirements in ISO/IEC 29100 [B31] to the different classes of CIoT interoperability as identified in Clause 10 and Clause 11. This mapping assumes that the RA, as adopted by the users of this standard, involves a Privacy Manager (PM) component as part of its architecture. The PM is a functionality that is part of the CIoT with TIPPSS reference architecture that can control the personal and medical information transmitted between various components of a CIoT system. Organizations should design the PM as a distributed authorization privacy protection architecture that takes into consideration the user's privacy preference and consent, stores the access log, and keeps track of collected data. The PM shall store access control policies, and the data subjects shall have the ability to configure their preference through the PM.

5.3 Privacy Impact Assessment

The purpose of a Privacy Impact Assessment (PIA) is to conduct a systematic risk assessment to identify privacy threats and make recommendations regarding technical, administrative, and physical controls to mitigate threats. Privacy threats include unauthorized disclosure, linkage, profiling, and processing of personal information (PI) without consent to share or use the information. A PIA in CIoT is important because of the sensitive data collected and used. Both the manufacturer of the device itself and the organization deploying it within their organization need to complete this. To help protect the privacy of end-users, including patients and healthcare providers, the PIA shall be completed at the earliest possible stage of the system design and implementation processes.

A sample PIA framework for the concepts identified in this standard is shown in Table 1, including an "objective" and a set of "PIA documentation" for each topic. These questions serve as a guide to initiate the conversation about privacy. To completely evaluate the system's privacy impact may require other assessments in addition to the PIA. The deploying organization shall assign owners, typically in the form of roles, to each of the activities in the PIA.

Table 1—Privacy Impact Assessment framework

Privacy requirements	Objective	PIA documentation to complete
Data collection minimization	Reduce the quantity of data collected to the minimum required for the specific purpose.	Document the kinds of personal data that the system/device will collect and process. Document why this data is necessary to achieve the functionality of the system/device. Document the procedural and technical controls that organizations have implemented or will implement to reduce data collection.
Purpose legitimacy and specification	Verify that organizations collect only the data necessary to fulfill the stated purpose	Document for which purposes organizations will collect and process this data. Include the functionality of the system/device, as well as technical processes (e.g., backups), further processing (e.g., big data analysis), and monetization.

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Privacy requirements	Objective	PIA documentation to complete
Usage, data retention, and storage limitation	Reduce the amount of data stored if it is no longer necessary.	Document the purposes and duration for data retention. Consider legal requirements, functionality, and technical processes. Document the implementation of procedural and technical controls to remove data outside the required retention period. Document the verification of successful and secure transmission before deletion.
Consent and choice	Provide users the ability to participate or withdraw from the collection, use, and disclosure of personal information.	Document the obtaining of users' consent to process their data for every type of use foreseen. Document the use of that accessible language. Document the procedures and technical controls implemented to capture and track consent.
Notice and access	Inform users about the collection, use, and disclosure of their personal information and provide access.	Document the notification of users about the collection, use, and disclosure of personal information. Document the processes to give users access and control over their data. Document the usage of accessible language. Document the mechanisms in place for users to exercise their preferences, including procedures and technical controls implemented for users to access and interact with their personal information.
Individual participation and transparency	Detail the policies and procedures about the management of personal information and make them publicly available.	
Accuracy and quality	Keep data accurate, complete, and up to date and confirm it satisfies the intended usage purposes.	Document the procedural and technical controls implemented in the system/device to help avoid unlawful access and tampering and verify integrity.
Accountability	Comply with privacy and data protection laws.	Document processes to identify and address incidents that affect remotely stored data or explain why the processes are not relevant to the system/device. Document successful compliance with all privacy and data protection laws and who, if anyone, is accountable for complying with the law in this area.
Data protection	Demonstrate protection of data using reasonable and appropriate methods.	Use an established Information Security Framework such as ISO/IEC 27001/27002 or the NIST CSF to demonstrate the effectiveness of the data protection schemes used to protect subjects' data.
Privacy compliance	Demonstrate methods, processes, and techniques for safeguarding data subjects' privacy.	Use an established privacy risk management framework such as ISO/IEC 27701 [B30] or NIST SP 800-53 Rev. 5 [B39].

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

5.4 Premarket and postmarket privacy requirements

The following provides a reference for CIoT device manufacturers on the specific privacy requirements that shall be considered during the premarket and postmarket phases of the device lifecycle. Specific requirements, including additional requirements not listed here, may vary based on the device use case as well as regional privacy laws in the intended target markets. Those requirements may also vary depending on the results of the PIA.

Further, these requirements, although focused on the device itself, shall include the larger target operating environment and any device-related infrastructure utilized to process and store sensitive data, for example, on the device-supporting network or manufacturer-provided infrastructure, whether on-premise or in the cloud.

Examples of design implementations that enable privacy that manufacturers shall implement are as follows:

- Security of personal data collected: patient, caregiver, clinician, operator, service provider.
- Application of cryptography to enable protection of confidentiality and integrity of sensitive data and assurance of authenticity, e.g.,
    1) Protection of sensitive data at rest (e.g., in the case of device theft or infiltration).
    2) Protection of data in transit (e.g., clear text HL7 or DICOM data transmission).
    3) Authentication of source validity (e.g., code signing to be confident updates are legitimate).
    4) Features supporting decommissioning and reliable data removal.
    5) Definition of permitted data collection and technical implementation.
    6) Safeguarding data transferred as part of servicing or complementary services.
    7) Controls to enable assurance of data usage only for legal and specified purposes.
    8) For mobile or remote use cases, enable use-case-specific privacy features like a remote wipe or device tracking.

The CIoT device shall manage and protect the following privacy-related sensitive data including:

- Identities and identifying data, including secondary data elements such as location.
- Health data.
- Billing and payment information.
- Secret materials: account credentials, device identifiers, network credentials, cryptographic keys, or certificates.
- Intellectual property.
- Proprietary business information.
- Network and integration-related information.
- Technical information pertaining to device location, operation, or maintenance, e.g., patch, update, or repair history.

5.4.1 Premarket privacy requirements

Manufacturers should address privacy requirements throughout the device lifecycle. Manufacturers should design devices during the premarket phase to include capabilities commensurate with the deployment and usage of the device. Manufacturers and potential distributors, including healthcare organizations, should also

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

collaborate premarket to develop processes that monitor consumer privacy experiences and collect the data to make privacy enhancements.

a) The device manufacturer shall establish the roles required to meet international standards and local privacy regulations, requirements, and laws. These roles can provide education and empowerment to enable their success. Such roles may, for example, include a Privacy Officer, Data Protection Officer (DPO), or HIPAA Compliance Officer. Smaller organizations may opt for a shared-role model. However, when combining privacy roles with other functions, organizations shall avoid conflicts of interest.

b) Manufacturers shall identify and define high-level privacy requirements as determined by device type, system integration, interoperability, use case, applicable international standards, and local laws and regulations. These privacy requirements shall be determined based on considerations such as the following:

   1) Where the manufacturer intends to approve and sell the device from a regulatory perspective. This includes the definition of local legal nuances, for example, the definition of what constitutes private and personal data, what protections each region requires, or what disclosures each requires.

   2) The types of data the device collects.

   3) Other purposes for data collection and usage.

   4) Protections are needed for the data collected.

c) Manufacturers shall derive specific privacy requirements from the high-level requirements and realize them via the following:

   1) Governance and business objectives.

   2) Policies and procedures.

   3) Management of supply chain and contractors.

   4) Device architecture and design.

   5) Target operating environment and system-level integration.

   6) Engineering implementation and realization of privacy controls.

   7) Auditing, reviews, assessments, and testing.

   8) Market release processes and approvals.

   9) Regulatory filings required for market approval.

   10) Production, storage, and delivery.

   11) Education and training of staff, business partners, users, operators, and patients.

   12) Documentation, as appropriate for each role involved in privacy, including staff, business partners, users, operators, patients, and regulators.

   13) Supporting contracts and legal agreements.

d) Manufacturers shall perform and maintain a security risk assessment throughout the device lifecycle.

e) Manufacturers shall perform a privacy risk assessment in alignment with the security risk assessment and maintain it throughout the device lifecycle.

f) The privacy risk assessment shall be performed by the manufacturer as applicable related to all personal data that may be collected by a device, including but not limited to patient, caregiver, clinician, operator, and service provider.

g) As part of the market release process, the manufacturer shall perform the following:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

1) Privacy-specific verification to be confident that established requirements have been met
2) Privacy-specific validation to be confident that privacy laws and regulations as appropriate for the target market have been met
3) A security risk assessment

h) The manufacturer shall comply with international standards as well as local laws and regulations as those standards pertain to the following:

1) Data collection limitation and data minimization
2) Purpose legitimacy and specification
3) Data usage, retention, and storage limitation
4) Consent and choice
5) Notice and access
6) Individual participation and transparency
7) Accuracy and quality
8) Accountability
9) Information security
10) Privacy compliance

i) Device local and remote access shall provide for the specified level of access security and provide role-based authorization features to enable proper segregation of device operational functions (e.g., clinical or service functions) and mapping to specific roles (e.g., clinician or service provider). Manufacturers shall avoid insecure access practices (e.g., weak, default, or hard-coded passwords or shared account names).

j) The CIoT device or CIoT integrated system shall incorporate features and functions that allow the operation of the device in compliance with international privacy standards and local laws and regulations and throughout the operating device lifecycle, including data removal or sanitization between users or at device end-of-life if required. Manufacturers shall document and make these functions accessible to the user or operator of the CIoT device.

5.4.2 Postmarket privacy requirements

Manufacturers shall implement processes that capture privacy feedback from consumers, vendors, and healthcare providers. Vendors and providers share postmarket privacy requirements and have a responsibility to collect and submit privacy issues to the device manufacturer and other organizations identified through the regulatory framework.

a) Manufacturers shall perform regular reviews of changes in clinical practice, device usage, international standards, and local laws and regulations and, as applicable, lead to an updated privacy risk assessment as well as result in the implementation of changes and updates to the device.

b) Manufacturers shall establish regular processes that enable the detection and documentation of privacy failures and violations, including, for example:

1) Customer (user, operator) feedback.
2) Information obtained by sales, service, and support staff.
3) Implementation of policies and tools that enable monitoring for privacy violations on manufacturer-provided infrastructure (e.g., a manufacturer-provided cloud service).
4) Log and event data analysis of devices in operation.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

5) Analysis of returned devices.

6) Private and government entities' collection and analysis of data on privacy violations, including security researchers or law enforcement.

7) Use of third parties for tracking, monitoring, and/or support of devices, especially with tracking "cookies."

8) Security risk assessments and corresponding privacy risk assessments of the supporting environment and infrastructure using established industry frameworks (e.g., ISO/IEC 27001, ISO/IEC 27702, NIST Privacy Framework, NIST Cyber Security Framework.)

c) The manufacturer shall perform regular reviews of processes, design features, and documentation to be confident in the continued applicability of international privacy standards as well as local privacy laws and regulations pertaining to the following:

1) Data collection limitation and minimization

2) Purpose legitimacy and specification

3) Data usage, retention, and storage limitation

4) Consent and choice

5) Notice and access

6) Individual participation and transparency

7) Accuracy and quality

8) Accountability

9) Information security

10) Privacy compliance

5.5 Summary

Privacy in CIoT interoperability shall meet several requirements to protect individual data and related rights, as outlined in this standard. In this clause, privacy requirements have been identified based on global privacy frameworks and laws. To fulfill these privacy requirements, the need for a PM has been identified to configure the privacy policy and support the end user (data subject) to manage their privacy preferences, as well as a PIA to help ensure consideration of privacy within CIoT systems. Finally, premarket and postmarket privacy requirements in CIoT data and device interoperability have been discussed.

6. Protection

6.1 Protection overview

CIoT devices with TIPPSS systems should include technology and process measures that can help maintain device and system safety, effectiveness, reliability, and security and help protect the device, data, environment, and humans from harm. This includes (but is not limited to) built-in protections in device and system design, cybersecurity controls, information protection, maintenance and management of protective features, backup and restore capabilities, fail-safe operating modes, and decommissioning features. Device protection (and, by extension, safety and security) needs to be part of the device lifecycle from the very beginning and extend through market release, production, maintenance, and device end-of-life.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Protection of CIoT devices, data, and humans in a connected healthcare system should be enabled through several mechanisms, which this clause enumerates, namely: device pairing, authentication, access control, communications, updates, replacements, resilience, documentation, and decommissioning.

6.2 Device pairing

Solution providers shall consider trusted, secure, and vetted best practices for device-to-sensor pairing, rather than creating a new protocol or method, to maintain consistency and leverage the experience of other proven methods, to prevent the following:

- Unintentional pairing with other smart devices.
- Malicious attempts to pair with the sensor and/or device app.
- The pairing of unauthorized sensors (gray market, refurbished, rogue, insecure, etc.).

When combining a dedicated purpose device, e.g., a CIoT sensor, with a general purpose device, e.g., a smartphone, tablet, or computer, the solution providers shall identify, assess, and mitigate any new risks that result from this combination. For example, users can combine a sensor's data with the smartphone's location data, resulting in new risks such as stalking.

6.3 Authentication

Solution providers of CIoT devices with TIPPSS shall employ industry-standard methods for authentication that adequately protect and uniquely identify the sensor, device, and data, and the following:

- Shall provide mutual authentication of a sensor to a device and vice versa (mutual authentication).
- Shall provide authentication of the device to the backend, gateway, or another system (local, remote, or cloud) and vice versa.
- Shall provide for adequate levels of authentication of users depending on role (administrator, patient, operator, service provider, healthcare provider, etc.). Authentication for an administrator with high-level system privileges may require stronger authentication than for a patient or provider, for example.
- Based on the device use case and use environment, the solution provider should consider the use of other access control methodologies, such as discretionary access control (user can allow); mandatory predefined (e.g., military or controlled situations); or attribute-based (location, ID, other properties).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

6.4 Access control

CIoT with TIPPSS device solution providers shall implement RBACs that:

- Shall provide access control depending on user role and the required level of security.
- Shall implement the least privilege access principles for the respective user roles.

The solution provider shall carefully evaluate any access control features against identified risks that the feature may introduce, e.g., delayed or less reliable access due to MFA. If security features introduce new risks (e.g., to patient safety), the solution provider shall carefully evaluate the feature-benefit tradeoff and shall document the decision. Should the safety risk outweigh the security benefit, manufacturers may decide not to implement a security feature or provide additional compensating controls.

Copyright © 2024 IEEE and ULSE. All rights reserved.

6.5 Communication between components

6.5.1 Communications between device and sensor

The solution provider shall consider and implement the most suitable and most secure communication protocols between the device and the sensor that it expects to operate in proximity (e.g., BAN, PAN). This includes such protocols as IEEE 802.15, IEEE 802.11, wireless standards, end-to-end encryption independent of the transport layer, and support for the latest available encryption protocols (such as TLS 1.3). Solution providers shall maintain standards-based encryption protocols at the latest and most current supported levels as defined by industry standards.

When a connection traverses across multiple types of networks and the security of each individual network segment cannot be assured, the device manufacturer shall enable the implementation of end-to-end encryption to enable data protection across multiple hops (e.g., via short-range wireless technology to a local device, via an IEEE 802.11 network to a local router, via public internet to a cloud service, and via enterprise network to a clinical workstation).

The solution providers shall consider secure and vetted best practices for updating the protocols and algorithms used for communications to support the latest versions.

6.5.2 Communications between device and aggregator/gateway

The solution providers shall consider the most suitable and most secure communication standards between the device and the aggregator/gateway (see Figure 11), which may be at either a short or long distance. This includes such protocols as cellular communications, wide area network (WAN), local area network (LAN), personal area network (PAN), end-to-end encryption independent of the transport layer, and support for the latest available encryption protocols (such as TLS 1.3). Solution providers shall maintain standards-based encryption protocols at the latest and most current supported levels as defined by industry standards.

The solution provider shall consider secure and vetted best practices for updating the protocols and algorithms used for communications.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

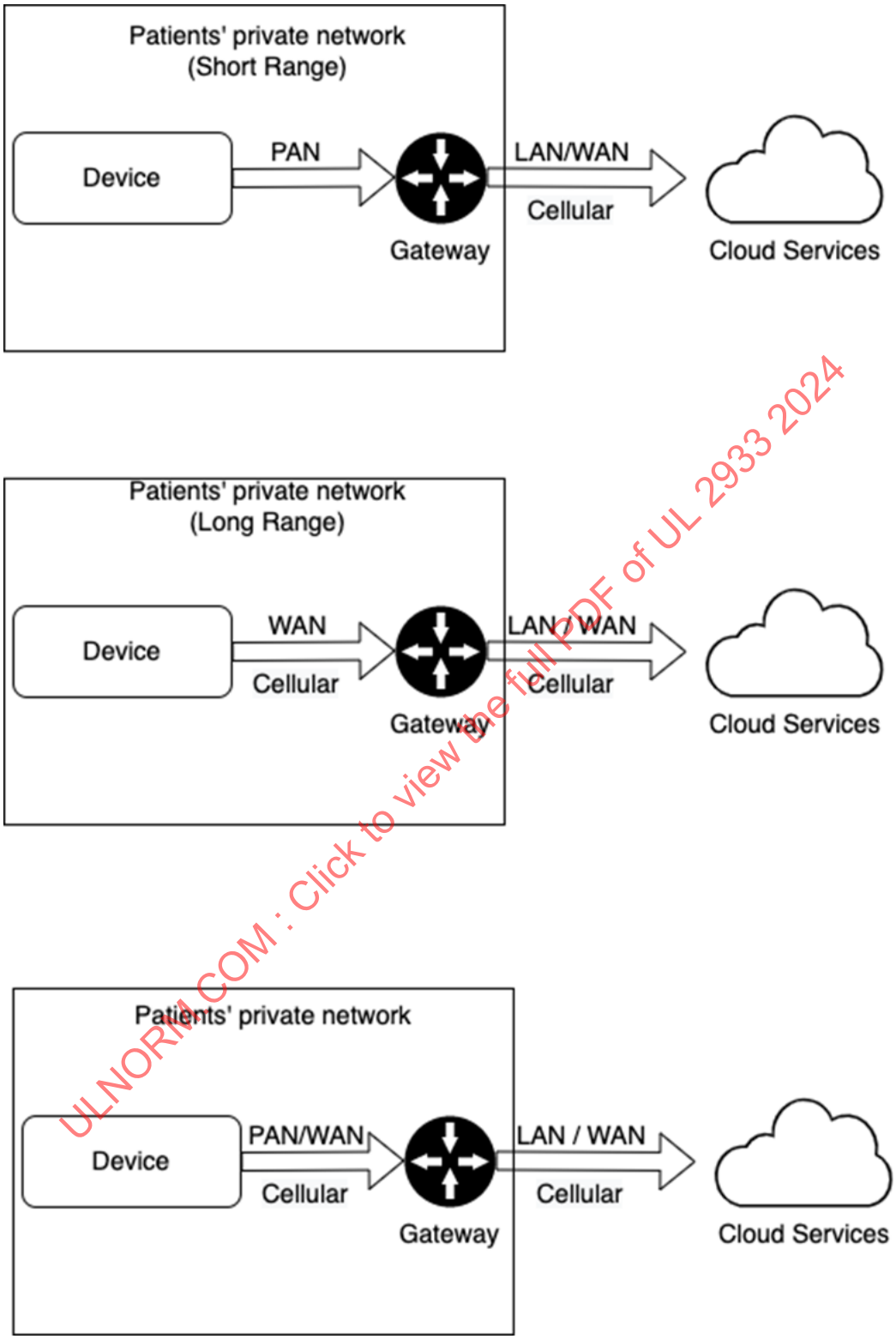

Figure 11 —Device to gateway and backend communication

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

6.5.3 Communications between aggregator/gateway and backend

The solution provider shall consider the use of multiple connectivity methods (5G, IEEE 802.11, internet, etc.) to maintain uninterrupted and secure data transmission between the gateway and the backend (see Figure 11).

The solution provider shall utilize the most suitable and most secure communication standards between the aggregator/gateway that are expected to operate at long-distance proximity (WAN). This includes protocols such as 4G/5G cellular communications, end-to-end encryption independent of the transport layer, and support for the latest available encryption protocols (such as TLS 1.3).

The solution developers shall consider and utilize trusted, secure, and vetted best practices for updating the protocols and algorithms used for communications.

6.5.4 End-to-end encryption

The solution provider shall use end-to-end encryption where it cannot be assumed to have control over the security of individual hops or segments. For example, in a scenario where a device connects via short-range wireless technology to a smartphone, which connects over an IEEE 802.11 network to a home router, which connects via TLS over the public Internet to a cloud service, sufficient security at all hops or segments shall be effectively managed by the deploying organization and cannot be assumed.

6.6 Updates

The solution provider shall provide the means and processes to update sensors, software applications, locally connected devices (e.g., smartphone or another connected device), backend, gateway, and other systems in a secure manner that provides protection from intentional or environmental factors.

The solution provider shall consider and utilize established principles of a secure update process to:

a) Maintain critical functions of the device and sensor during the update.

b) Provide for sensor and device security updates throughout their lifetime.

c) Verify the integrity of the updates.

d) Monitor for failures of the sensor, software, or device to take and apply updates.

e) Back up critical data and configuration files so that the update does not affect their confidentiality, integrity, or availability.

f) Provide a roll-back function for failed updates, critical data, and configuration files.

If feasible, the solution provider should consider the use of automation and/or intelligent statistical analysis to determine optimal times to update devices. The solution provider should optimize this analysis based on system parameters, such as remaining battery time, available bandwidth, operating state, and other relevant factors.

The solution provider should consider whether it is best to provide a manual override capability so that the end user or caregiver can specify that an update should not take place at a certain time, for instance, during a medical emergency, or that an authorized user needs to explicitly approve an update before it commences.

The solution provider should determine the optimal time to back up devices. The solution provider should optimize this based on system and operating parameters such as remaining battery time, available bandwidth,

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

and other relevant environmental factors to update medical devices and/or install security patches. Intelligent technologies such as artificial intelligence or machine learning (AI/ML) can be used to assist stakeholders in making these determinations.

When devices have not been updated in a timely manner, the solution provider should consider using a device management system. This system may use intelligent technologies such as AI, ML, and/or intelligent statistical analysis to analyze devices and their risks. This system should identify outlier devices in need of updating, pinpoint susceptible devices, identify potential threats, and identify devices in need of preventative maintenance.

6.6.1 Third-party and open-source components

The solution provider shall monitor open-source and third-party software in use for newly discovered or disclosed vulnerabilities and important updates impacting the security and privacy of the applications and their data.

The solution provider shall provide timely communications and updates according to established best practices.

6.6.2 Sensor

The solution provider shall provide for the sensor to receive and apply updates throughout its lifetime.

During the update process, the solution provider shall do the following:

- Follow best practices for protecting the integrity of the update package (e.g., through code signing).
- Validate that installation occurred without tampering.
- Provide update information to the backend (e.g., success or failure of the update to a newer version).

The solution provider should consider creating a “minimal function mode” for the device during updates that may update the critical functioning of the device. By “minimal function,” it means that the device shall continue to perform its critical functions during the update when deemed to be necessary for the purpose of the usage of the device and the protection and safety of the patient.

Where applicable, the solution provider shall help ensure that the backend monitors the device update status and detects when devices have not been updated in a timely manner. The solution provider should consider utilizing automation and/or intelligent statistical analysis for the proactive identification of devices that may be vulnerable.

6.6.3 Smart device application

The solution provider shall provide maintenance and updates for the smart device apps throughout their lifetimes.

6.6.4 Backend/Gateway

The solution provider shall provide updates for the backend and/or gateway throughout their lifetime(s).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

6.6.5 Requirement for update independence

The solution provider shall maintain reliable operation, including when updates for sensor firmware/software, smart device app software, and/or the backend/gateway do not occur at the same time. Solution providers should avoid dependencies between components that require simultaneous updates. If the solution provider cannot avoid dependencies, solution providers shall document and provide appropriate instructions for managing them.

6.7 Backup

The solution provider shall provide methods to back up and duplicate firmware, the operating system environment, applications, configuration files, and data from devices. The solution provider shall also provide methods to restore copies of these data to either the device from which the data originated or to a like device. The methods provided by the solution provider shall be executable by the deploying organization.

Backup and restore methods shall protect the confidentiality, integrity, and availability of backups. The solution provider shall protect backup data by encrypting it using approved encryption methods discussed in 8.3. Backup and restore methods can help maintain data integrity and protect against tampering by utilizing approved hashing methods discussed in 8.3. These methods can also help maintain the availability of backups and protection of critical backup data.

Devices shall provide the means to backup and restore via removable storage, a dedicated backup section on the devices themselves, or network or cloud-based locations. Backup methods should include executable programs and/or application programming interfaces (APIs).

6.8 Requirements for replacements

If the solution provider replaces the data aggregator, backend, smart device (e.g., phone), and/or sensor, the solution provider shall consider whether to transfer the configuration data and/or patient data to the new device.

6.9 Tamper-proofing and integrity

The solution provider shall implement measures to help prevent tampering with the smart device, software (e.g., smartphone app), sensors, and data. Specifically, the solution provider:

a) Shall provide mechanisms to help prevent unauthorized users (including the patient) from altering the smart device app and/or the device. This includes code and critical settings for both the smart device and software. Solution providers shall implement options such as digital signatures and/or other techniques for this purpose.

b) Shall provide tamper-proofing of the sensors appropriate to the level of risk, considering the following options:

    1) Documentation and labeling

        i) Specific warning related to tampering

        ii) A specific description of risks related to off-label use or use in a way that is not consistent with the intended use or use environment, as defined by the solution provider

    2) Physical protection

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

i) Tamper-proof casing

ii) Tamper-resistant design

iii) Physical security (locks, etc.)

3) Tamper protection

i) Tamper evidence

ii) Tamper detection

iii) Tamper response

c) Shall detect intrusion of either the smartphone app or the sensor. Depending on the complexity and security requirements of the device, this may include the use of artificial intelligence/machine learning (AI/ML), automation, intelligent statistical analysis, distributed ledger technologies, and other ways of detecting intrusion.

d) Should detect tampering with the sensor and alert the backend of any tampering.

e) Shall encrypt selected data at rest on the device, sensor, and app, as dictated by applicable privacy requirements.

f) Shall provide integrity mechanisms for the data at rest, such as error detection and correction technologies and digital signatures.

6.10 Resilience and fail-safe mode

To maintain device and system resilience, the solution provider shall consider ways for the device and system to fail safely, in case any component of the system fails, including but not limited to situations where the following occurs:

a) The device loses connectivity (either between sensor and device, device and backend, or sensor and gateway).

b) The device is offline (e.g., the device battery or phone battery died, or the device or phone rebooted).

c) The sensor goes offline (e.g., the sensor runs out of power).

d) There is a component failure(s).

e) The system detects tampering.

f) The system detects a security event or compromise.

g) The system detects signal jamming or interference.

In these situations, the sensor and/or device should save data locally on either the sensor or device and transmit data when the sensor and/or device restores communications.

In case of signal loss and loss of signal coverage, the CIoT device shall continue to operate safely.

6.10.1 Updates and alerts to trouble

The solution provider shall provide a “heartbeat” to the device and backend and shall provide alerts when the solution provider notices any of the following conditions and other critical conditions:

— Loss of connectivity (increasingly critical as time goes by).

— Lack of receipt of heartbeat for more than a certain period.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

- Low battery power.
- Inability to update to the latest version.
- Changed status of system resources (memory, disk space, CPU usage, power consumption, etc.).
- Cryptographic key verification failures.
- Security events such as malware detection.
- Denial-of-service (DoS) attacks.
- Other considerations as determined via a thorough risk assessment.

Solution providers shall consider whether the patient or caregiver should be alerted when the app, device, sensor, and/or aggregator are not communicating results to the clinical backend. For instance, if the patient or caregiver believes that the device or sensor is telling their clinical staff that their blood pressure or other vital signs are deteriorating, the patient might not call for assistance because the patient assumes that the clinical staff has already been alerted to the situation.

6.10.2 Signal jamming and interference

6.10.2.1 Signal jamming

Signal jamming may be employed under some circumstances, and the device, sensor, and backend systems should account for this possibility and reduce the risk to the patient.

For example, a patient may attend an event where the venue actively engages in signal jamming for some frequencies or may go to a location where signals are routinely jammed, such as at an airport, within a secure facility, or in a prison.

Signal jamming shall not cause any harm to the device or sensor or the person using the device or sensor.

6.10.2.2 Signal interference

The solution provider shall provide protection against interference due to environmental concerns (e.g., power lines, electronic equipment, operation in an ambulance) based on its intended uses.

The solution provider shall provide protection against interference or degradation of signal due to a situation with many other similar devices in the vicinity.

6.10.3 Backup and restore capabilities

The solution provider shall consider, depending on the criticality of the data, whether there should be backups of firmware, configuration, device clinical data, or patient data.

The solution provider shall consider ways to back up custom data on each device, app, and sensor that may be specific to that user.

The solution provider shall assess the required recovery point objective (RPO), (i.e., the point of time in history to which data needs to be restored as it relates to the time frame of data that can be lost) and recovery time objective (RTO), (i.e., the time it takes to restore data and device functionality). The solution provider

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

shall design backup and restore capabilities to meet defined RPO/RTO requirements. For example, if there is no need to retain device data (RPO = infinite), then the fastest RTO can be achieved by resetting the device.

The solution provider shall encrypt any data backed up to external smart devices or external services if it is sensitive (e.g., PHI, PII, credentials, sensitive technical data).

If the device use case and data criticality warrant, the solution provider shall store multiple backup copies on different media and in separate locations.

If data backup is the responsibility of the user or operator, the solution provider shall provide appropriate instructions.

If the device use case and data criticality warrant, the solution provider shall retain several historic backup versions and rotate them on a first-in, first-out (FiFo) basis.

The solution provider shall provide a means to restore technical or clinical data as required for the use case.

The solution provider should determine the optimal time to backup devices. The solution provider should optimize this based on system parameters, such as remaining battery time, available bandwidth, and other relevant operational and technical factors.

6.10.4 Data integrity and quality

The solution provider shall implement data integrity and quality mechanisms to help prevent erroneous data use as appropriate for the device, use case, and use environment. For example, the solution provider:

- Should analyze the data to determine if it is within the expected “physiologic range” for the patient, and if it is not, then create an alert to either question the data or determine if it is a signal for a medical emergency.
- Should assess the plausibility of the data., e.g., to assert with reasonable confidence a patient’s identity based on historical data; identify faulty or failing devices or accessories; identify the need for maintenance or calibration.
- Should detect and manage unexpected and out-of-range data, e.g., by escalation to a “human in the loop.”
- Should provide features that prevent safety compromises resulting from erroneous data.
- Should detect unauthorized, expired, or reused accessories if their use could impact patient safety.

Depending on device design and capabilities, solution providers can perform these data quality and plausibility checks on the device or the device backend. This includes the use of multiple and/or alternative methods for patient identity validation, especially if the reliable assertion of identity is related to safety risks, as discussed in Clause 4.

6.11 Documentation and labeling

The solution provider shall provide clear, plain documentation and labeling to adequately inform the patient about all of the following:

- Requirements for provisioning and configuration of devices.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Security and privacy risks.

— Actions to take during an incident—such as loss of connectivity or non-responsive applications and/or devices.

— Detection of a security breach or another compromise.

The solution provider shall provide clear written information so that healthcare staff and caregivers who are not IT or cybersecurity experts can understand all the following, as needed:

— Requirements for provisioning and configuration of devices.

— Types of adverse events that may occur—loss of connectivity, loss of data, application integrity compromise, etc.

  1) Potential impact of such adverse events.

  2) Appropriate steps to respond to such adverse events.

6.12 Decommissioning

At the device end of use, the sensor, smart device, app, backend, and all data stored in these systems shall be considered so that the device can be disposed of without exposing the data, thereby protecting the data through the end of use and end-of-life of the device.

The solution provider shall provide an industry-standard way to securely destroy data on the device, sensor, and backend so that forensic or brute force methods cannot recover it.

Removal of sensitive data shall include the following considerations:

— Sensitive clinical data (e.g., patient name or medical history)

— Sensitive technical data (e.g., credentials and site-specific configuration data)

— Intellectual property

The data controller is responsible for initiating the proper disposal of the data with the data processor. The data controller is the natural or legal person, organization, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. The data processor, on the other hand, is the entity that performs the data processing on the data controller's behalf.

When the solution provider manages a backend that stores the data, the solution provider shall be responsible for its secure disposal.

However, when another party stores data on a device under their control, that party is responsible for the secure disposal of the data. The solution provider shall be responsible for providing a means of securely disposing of data and documenting such processes.

To properly provide for data removal across the ecosystem, this may require specific technical features as well as contractual agreements between parties. When making design decisions on device and system memory technology, solution providers shall consider the requirements for device decommissioning and data destruction as part of the decision process.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

6.12.1 Decommissioning legal and regulatory background

There are numerous regulations around the world related to when a device reaches the end-of-life and is prepared for reuse/recommissioning or disposal/decommissioning. Per the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rules, no PHI or personal data shall remain on the device when it reaches the end-of-life. Section 25 of the Singapore Data Protection Act, The Retention Limitation Obligation, requires organizations to cease to retain documents containing personal data when their purpose is no longer being served. Article 5(e) of the European Union General Data Protection Regulation (GDPR) requires that Data Controllers or Data Processors keep personal data in an identifiable form for no longer than is necessary for the personal data to be processed. The EUNetInfo group collaborated on CoreHTA standards for medical devices. As part of their health technology assessments (HTAs), Issue F0101, “Does the technology invade the sphere of privacy of the patient/user?” requires that question to be answered.

Solution providers shall utilize technology to reasonably protect the privacy of patients and shall utilize decommissioning procedures to provide affirmative compliance with applicable requirements. When a device is being prepared for reuse/recommissioning outside the organization or disposal/decommissioning, solution providers shall remove all stored credentials on the device, such as usernames, passwords, wireless passwords, or digital certificates, along with personal data. While this standard provides the U.S., EU, and Singapore as examples, it is critical to understand the regulations of the target markets for the device(s) so that compliance with them can be achieved. Removing stored credentials and personal data can provide a first step toward compliance in multiple target markets.

While the manufacturer shall provide features, processes, and documentation that allow for the automation of removal of this information, the operator shall verify and validate them (healthcare provider or hospital) to help protect data from inadvertent disclosure in compliance with the HIPAA Security Rule, Singapore PDPA Section 25, and GDPR Article 5(e). The HIPAA Security Rule, U.S. 45CFR 164.310(d)(i) codifies this by requiring organizations to address the final disposition of electronically PHI, and/or the hardware or electronic media on which the information is stored. Part (ii) of that component of the Security Rule requires organizations to implement procedures for the removal of PHI from electronic media before the media are available for reuse.

The Health Information Technology for Economic and Clinical Health Act (HITECH), which was enacted under Title XIII of the U.S. American Recovery and Reinvestment Act of 2009, has a component called *Breach Notification for Unsecured Protected Health Information*. This requires organizations to clear, purge, or destroy media consistent with the requirements in NIST SP 800-88 Rev. 1 [B42] such that the PHI cannot be retrieved.

This standard is concerned with mechanisms that exist and have been tested to the NIST SP 800-88 Rev. 1 [B42] or ISO/IEC 27001 Media Handling (A.8.3) standards so that PHI, personal data, credentials, and intellectual property can be erased in compliance with respective national regulations from a device or remote/cloud-based storage to meet HIPAA and HITECH standards. Compliance with this document does not constitute compliance with applicable regulatory requirements. Users are responsible for observing all applicable laws and regulations, including those related to data privacy.

Device data such as calibration data, maintenance histories, parts replacements, service histories, and recall replacements/services may not be considered PHI or personal data. The Joint Commission, a U.S.-based nonprofit tax-exempt organization that accredits U.S. healthcare organizations and programs, and other accrediting agencies may check the service and maintenance histories of devices as part of program or service accreditation. Organizations such as the American College of Radiology have checked the integrity and availability of Device Data. Service providers shall keep this Device Data separate and under different retention conditions from PHI or personal data. Service providers shall keep this data in a separate logical partition from PHI or personal data. Service providers shall also keep site-specific configuration data, such as passwords, identities, and network credentials, in a separate logical partition.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

6.12.2 Decommissioning processes and practices

The decommissioning processes and practices are as follows:

a) The manufacturer shall provide mechanisms to erase site-specific configuration data, network and user credentials, personal data, and PHI, to NIST SP 800-88 Rev. 1 [B42] (or equivalent) standards from:

   1) Transient storage areas such as random-access memory (RAM).

   2) Attached persistent storage, including operational information stored in firmware, erasable programmable read-only memory (EPROM), persistent memory, hard disks, and solid-state disks.

   3) Removable persistent storage, including secure digital (SD) cards, Universal Serial Bus (USB)-attached storage such as flash drives, hard drives, and solid-state disks, Compact Flash-based storage, and PCI Express-based removable storage, such as CF Express, NVMe, and SD Express.

   4) Cloud-based or remote storage.

b) The manufacturer shall make the following mechanisms available from the device configuration menus and shall allow the device operator to:

   1) Erase all attached transient and persistent storage areas containing site-specific configuration data, PHI, or personal data, and return them to an initial state with all data overwritten to NIST SP 800-88 Rev. 1 [B42] standards to a zero state with no data remnants. Provide affirmative confirmation to the operator/production associate (PA) to conduct this operation.

   2) Erase removable persistent storage inserted in the device and overwrite it to an initial state with all data overwritten to NIST SP 800-88 Rev. 1 [B42] or ISO/IEC 27001 Media Handling (A.8.3.) standards to a zero state with no data remnants. Provide affirmative confirmation to the operator/ PA to conduct this operation and identify:

      i) The bus/connection of the attached media.

      ii) The media serial number.

      iii) Identified media capacity.

      iv) Volume label of attached media.

   3) Erase cloud-based and/or remote storage containing site-specific configuration data, PHI, or personal data.

   4) The mechanism shall perform tests to verify that no data remnants exist in the target device or system.

   5) If either the erasure or verification steps fail for the given target device, the device shall notify the operator/PA.

   6) Provide affirmative proof to the operator/PA of media erasure or failure to erase in alignment with the Breach Notification Rule, GDPR, or other applicable privacy/security regulations.

      i) The report shall contain the following:

         — Operator/PA ID who performed the operation.

         — Date/Time of operation.

         — Device serial number.

         — Device model ID/number.

         — Data element types erased.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Validation that the operation was successful.

ii) For removable persistent storage, the mechanism shall provide proof via a report identifying the bus/connection, media serial number, identified capacity, and volume label.

iii) The report shall also contain the following for attached storage:

— Attached persistent storage capacities.

— Serial numbers of erased storage.

d) Device manufacturers shall:

1) Clearly identify PHI, personal data, site-specific configuration data, and device data specific to device operations, as well as where the data is stored.

2) Specifically, identify PHI or personal data elements that are stored in the cloud and how to process them.

3) Provide a means for the operator/PA to electronically transfer device data between owners upon proof of ownership transfer.

4) Provide contractual language to transfer and/or remove remote or cloud-based storage at the end of the contract or at customer request.

e) The operator/PA or solution provider working on their behalf shall:

1) Execute the erasure mechanisms on decommissioning or disposal of devices, data generated by devices and, if needed, data stored locally, remotely, or in the cloud, and document this according to applicable laws, standards, and regulations.

2) If the device does not properly execute erasure mechanisms:

i) Utilize alternative means, up to and including physical destruction, to meet NIST SP 800-88 Rev. 1 [B42] standards.

ii) Contact the manufacturer to address potential systemic issues involving media erasure and data remnants.

3) Maintain device and media controls and associated asset management records in accordance with U.S. HIPAA Security Rule General Principles 45CFR 164.310(d)(1) and (2).

4) Keep a list of disabled accounts to prevent reuse and potential accidental granting of entitlements.

5) Publish disabled certificates used for identification and validation to a certificate revocation list (CRL) when possible.

6) Have their software check the CRL for invalid certificates, and when presented with one on the list, deny entitlements and access.

7) Disable all access and entitlements on systems that depend upon the set of authentication credentials used by the device.

e) Healthcare organizations and users of these devices cannot be expected to have the capacity to independently verify or validate media erasure to appropriate standards or the ability to operate the vendor's cloud or remote environments to verify the deletion of data to those standards.

Manufacturers shall model data erasure use cases so that users of the devices are able to accurately erase data on these devices. This is so the users can credibly attest to accurate data erasure under applicable laws and standards, including the HITECH Act and NIST SP 800-88 Rev. 1 [B42] in the U.S., GDPR in the EU, ISO/IEC 27001, or ISO/IEC 27002, (or equivalent) as manufacturers are required to do so.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

7. Safety

7.1 Safety overview

Safety considerations are enabled in a TIPPSS context through the application of a risk management process to identify hazards, estimate potential harm from digital risks, implement and maintain risk treatment controls, and establish ongoing monitoring. See Clause 8, for further information on the TIPPSS risk management cycle.

For CIoT with TIPPSS solutions, implementation of controls and protective measures that reduce the likelihood of occurrence and/or impact to an acceptable level shall accomplish the prevention or reduction of the risk of harm. Manufacturers shall implement, document, and monitor safety controls regarding their risk reduction effectiveness, and in the context of the device's use environment and intended use.

Safety is multi-dimensional. In addition to a security context, safety also requires consideration of clinical, mechanical, electrical, etc. as well as environmental considerations including but not limited to electromagnetic interference, temperature, humidity, air quality, etc.

Unless related to CIoT data and device interoperability, these safety-related considerations are addressed by other standards such as ISO 14971:2019 [B20], ISO 24971:2020 [B21], ISO 81001-1:2021 [B22], etc. Specifically, IEC 60601-1 [B13] and its subparts address safety and performance requirements pertinent to TIPPSS-enabled solutions.

7.2 Mitigating safety risks

Although patient safety risks in general have been covered in other standards or regulations, there is a unique subset of safety risks resulting from the information compromises of data at rest or data in transit between interoperable systems. Examples of these types of safety compromises can occur from scenarios including:

- The inability of a CIoT device to collect or transmit data, which would disrupt the clinical data flow and could result in a detrimental impact on patient care and patient safety. This could lead to the risk of incorrect therapy or delivery of harmful therapy because of incorrect diagnosis or treatment.
- If a CIoT device or sensor were to be compromised by a hack or malware, it could provide inaccurate data from the patient. Thus improper decisions regarding health management may be made, whether for a self-managing patient utilizing the data or for healthcare providers using the data for patient care.
- The risk of compromise to a CIoT device or sensor to alter the patient identification (PID), which could compromise patient safety and patient care scenarios, as well as the admission, discharge, and transfer (ADT) processes for hospital-based clinical systems and modality worklists.

The positive aspects that the use of CIoT with TIPPSS devices may realize include the following:

- Reducing the risk of preventable severe adverse events (SAEs) using CIoT provided real-time clinical data and trends.
- Environmental monitoring to inform clinical care based on exposomes and environmental information.
- Leverage of clinical, environmental, patient lifestyle, research, and genomic data to better inform precision healthcare.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— CIoT with TIPPSS solution providers shall do the following to mitigate safety risks:

— Shall identify, document, and communicate the requirements for product safety based on established and applicable standards.

— Shall identify, document, and communicate the applicable laws, regulations, and standards that define specific safety requirements based on the use case, acceptable risk, and target markets.

— Shall develop a risk management process including a safety risk analysis inclusive of cybersecurity related risks. See Clause 8 of this standard for a risk management cycle overview to inform the development of a risk management process.

— Shall assess, document, and provide mitigation strategies related to potential safety risks from compromised CIoT devices and solutions and risks due to cybersecurity vulnerabilities, including but not limited to the following:

  a) Potential impact on the CIoT device.

  b) Potential impact on environmental monitoring systems (e.g., ambient temperature, humidity, pressure, and external weather).

  c) Potential direct and indirect impact on patient safety.

  d) Potential impact on the patient engagement process.

  e) Potential consequences of compromised operations and business processes.

  f) Potential impacts on clinical ordering and e-prescribing processes and devices.

  g) Potential impacts on the clinical device lifecycle management processes.

  h) Potential disruption to workflow automation, including the following:

    1) Business disruption.

    2) Loss of intellectual property.

    3) Loss of sensitive data.

    4) Compromise of user or network credentials.

See Annex G for more information on potential direct and indirect patient safety impact, and potential operations and business process impact, related to CIoT solutions.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

7.3 Quality assurance processes

Every deploying organization shall have internal quality assurance (QA) processes. These QA processes are important internal exercises that enable verification that the organization follows proper patient safety processes and serve as an important reminder to all healthcare providers and staff that patient safety processes should be followed. A compromised CIoT device or sensor could create a sequence of events that lead to a disruption of the QA processes, which in turn could threaten patient safety. Examples of internal QA processes are as follows:

— System monitoring of important patient care systems.

— Checking of battery condition in portable patient care devices.

— Error and pause protection.

Copyright © 2024 IEEE and ULSE. All rights reserved.

7.4 Other safety risk considerations

When considering the potential safety implications due to direct or indirect risks, organizations shall consider a broad range of scenarios that can lead to harm or can impact the safety and effectiveness of a given device. These considerations should include the following:

— Impact on device performance or function using unapproved accessories, e.g., the ad-hoc connection of non-approved devices via USB port.

— Impact on device performance or function due to unexpected network protocols, e.g., network vulnerability or discovery scans.

— Unavailability of clinical information due to device compromise or communications disruption.

8. Security

8.1 Security overview

In this standard, the role of security is to provide for the confidentiality, integrity, and availability of digital information applied to CIoT with TIPPSS devices and the environment the devices operate in, which includes the process of preservation of authenticity of information related to data, devices, systems, and people. This requires an initial understanding of risk, risk goals, and security controls applied to reduce these risks to an acceptable level, as well as the ability to maintain devices' security posture over their useful life. It includes capabilities to connect and share information securely, detect and support responses to security events, integrate with security infrastructure, and communicate security status information. CIoT with TIPPSS devices shall support a secure device lifecycle management approach with integrated, continuous improvement.

Security is a desired property of any interconnected CIoT device. Security is an enabler for safety, effectiveness, and privacy. Introducing any form of connectivity increases a device's exposure to security threats and the risk of security compromise.

Devices built on commercial platforms, e.g., common commercial operating systems, automatically inherit their security risks and therefore expose the device to all threats that are targeting the platform of choice. An example is that there may be a purely coincidental device compromise, not because it is targeted, but because it fits the profile of an attack or malware. Devices built on proprietary platforms and using proprietary interfaces, on the other hand, require a dedicated effort and a targeted attack.

Additionally, manufacturers shall take care not to introduce security risks through security functions themselves. Unfortunately, cases have been reported where a security vulnerability in a security tool (e.g., firewall or antivirus software) was exploited in an attack.

Security is the application of administrative, procedural, physical, and/or technical controls that reduce the risk of compromise due to cybersecurity threats. Security has also been defined as the "state of being protected," as "protective measures taken," as a "collection of tools and practices," or the "ability to protect." Stakeholders should also understand cybersecurity per ISO/IEC 27032 [B29], as preservation of confidentiality, integrity, and availability (CIA) of information in cyberspace.

TIPPSS builds on the classic CIA triad related to information to address requirements in the increasingly connected healthcare world, with devices that collect data with sensors and informing devices that are actuators related to healthcare and humans. Due to their CIoT use case and risk of harm to the humans that are using or depending on them, regulatory authorities and governments regulate these devices and data

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

further and more strictly than classic enterprise data and IT systems. CIoT devices require unique considerations for trust, identity, privacy, protection, safety, and security.

Specifically, this clause will:

a) Provide a general medical device taxonomy and catalog each individual key component (including but not limited to hardware, firmware, and software) and document risk-reduction requirements and safeguards to be built into each component of the medical device.

b) Define the secure device lifecycle, including design, development, manufacturing, supply chain management, and assurance of the untampered and unaltered delivery of the device to help maintain the security and continuity of medical devices and medical services.

c) Recommend approaches to architect a secure end-to-end connected healthcare system that extends from devices to the cloud. This includes defined, implemented, maintained, and documented security requirements for each component or device across the device lifecycle.

d) Recommend CIoT device security measures to be confident in the preservation of confidentiality, integrity, and availability of the PHI, PII, or other sensitive or critical data on the device. This includes built-in security controls to meet privacy requirements (see Clause 5), and protect data when acquired, stored, processed, or transmitted.

e) Recommend security best practices and controls that manufacturers can design into devices across their ecosystems, and across entire device lifecycles. Security controls need to be monitored, and users and solution providers alerted when a cybersecurity event occurs, the device detects an event, and/or the device malfunctions. For example, security best practices and controls could include the following:

   1) Auditing and accounting for access to data.

   2) Maintaining the integrity of health information.

   3) Maintaining continuity of medical services.

f) Provide approaches to address the potential need for updating or adjusting security requirements through regular review of changes to applicable laws and regulations, cyber threats, the security landscape, technology, applications, uses, implementations, and other pertinent considerations.

Security's purpose originates through a set of foundational objectives that are provided by governments (laws and regulations), the business itself (objectives and risk tolerance), and consumers or users of technology (needs and requirements). These provide the need for sufficient protection against ever-changing cyber threats. These foundational objectives typically include aspects of privacy, safety, functionality and reliability, legal and regulatory compliance (e.g., laws, standards, and market approval), business drivers (financial, operational, reputational), trust (identity assurance, authentication, and non-repudiation), and matters of national political and economic interests (e.g., protection of critical infrastructure, protection of intellectual property).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

8.2 Organizational cybersecurity foundation

Cybersecurity can only succeed if strategically established top-down and supported by the entire organization. Solution providers of TIPPSS-compliant CIoT devices and systems shall establish a cybersecurity foundation covering all aspects of people, processes, and technology, and do so across the entire organization from executive leadership through engineering and field service technicians.

Copyright © 2024 IEEE and ULSE. All rights reserved.

8.2.1 Cybersecurity governance

A solution provider of CIoT with TIPPSS devices or systems shall establish formal executive responsibilities for cybersecurity. With regards to cybersecurity for infrastructure, tools, partnerships, products, and services, executive leadership shall:

- Establish the organization's security governance.
- Make cybersecurity part of the organization's culture.
- Define the organization's business objectives and risk tolerance related to cybersecurity.
- Enable success through organizational structure, mandates, incentives, budgets, and staffing.
- Receive regular executive briefings on key cybersecurity aspects of the business, including programs, gaps, and critical events.

Based on the identified target markets' applicable laws, regulations, and standards, the CIoT with TIPPSS device and solution provider shall establish security governance to address the following:

a) Management responsibilities.
b) Resource requirements (people, organization, process, technology).
c) Security skills and training requirements.
d) Secure development lifecycle and corresponding high-level design security controls.
e) Supply chain and SBOM security management plans.
f) Plans for development, production, and maintenance infrastructure security, such as the following:
    1) Engineering tools
    2) Secure production transfer
    3) Production environment
    4) Third-party supplier or contract manufacturer security
    5) Remote and local service/support
    6) Security management of warehouse devices
g) Postmarket security surveillance and gathering of cybersecurity signals.
h) Processes for postmarket security management as well as vulnerability and change management.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

8.2.2 Security as part of the quality management system

A solution provider of CIoT with TIPPSS devices shall have a formal Quality Management System (QMS) in place that defines the overall quality processes to be followed in the specification, development, release, production, and maintenance of the devices. Such QMS shall provide for and include specific processes and requirements for cybersecurity.

8.2.3 Secure Software Development Lifecycle

Solution providers shall establish formal Secure Software Development Lifecycle (SSDLC) processes that enable an organization to develop and produce devices that meet the required level of security. Such SSDLC processes shall govern the complete device lifecycle, including the following:

- Concept and planning

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Requirements definition

— Design and architecture

— Development and implementation

— Verification and validation

— Release and production transfer

— Postmarket management and maintenance

The goal of an SSDLC-based TIPPSS development process is to enable the identification of security risks, reduction of these risks to an acceptable level through design and architecture decisions and implementation of security controls, and through security testing, which is the positive confirmation that all identified risks have been mitigated and that security controls are effective.

Once a CIoT with TIPPSS device is released for sale and is in operation, the solution provider shall perform dedicated postmarket surveillance activities and shall monitor the continual effectiveness of the device's security controls, detect, and respond to incidents, identify newly discovered vulnerabilities, assess security risks, and provide mitigations to customers.

These activities shall be performed by the manufacturer consistent with TIPPSS privacy requirements (see Clause 5) and any related agreements the solution provider has with the responsible organization.

8.2.4 Risk-based approach

Different use cases result in different risks that shall be considered. Similarly, differing designs provide different security capabilities. The challenge is to define the right level of security for a given device and in the context of its use cases.

Manufacturers need to establish a balance between security features and device safety and effectiveness. The solution provider shall perform a careful analysis to prevent the design and use of security measures that may compromise usability, safety, or effectiveness and, conversely, safety or usability measures that may negatively impact device security.

Security should be right-sized, neither too weak nor too restrictive. For example, it has been demonstrated that implementing unsuitable security measures in the healthcare setting can have negative consequences, e.g., a higher mortality rate.

Therefore, during the relevant development lifecycle phases, the device manufacturer and solution provider:

— Shall determine the security needs based on legal and regulatory requirements in the target markets, as well as customer, user, operator, and patient expectations.

— Shall specifically assess laws and regulations pertaining to privacy and safety and how these apply to security.

— Shall perform a formal security risk assessment to determine the security level required for a given device in its use case(s) and use environment(s) and balanced with the device's technical capabilities.

— Shall determine security requirements and implement security controls that balance the desired level of security with aspects of device safety, effectiveness, usability, and capability.

— Shall perform a formal risk-benefit analysis to assess whether certain security features and controls may result in other compromises, e.g., device usability. Any risk-benefit decision shall be supported by the appropriate rationale and shall be documented.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Shall consider whether security controls and measures are appropriate for the device's technical capabilities, use environment, and use case.

8.2.5 Establishing security requirements

Defining the correct set of security requirements can be challenging. Once defined, organizations should codify security requirements in their security governance and device and system design. Some security requirements are prescriptive; for example, compliance with HIPAA privacy and security rules is a mandate for U.S. healthcare providers. Other aspects of security governance are more difficult to establish, for example, how to define a business' risk tolerance and require thoughtful consideration and expertise.

Establishing the right security governance and requirements goes beyond meeting certain regulations. Once governance is established, organizations can determine the detailed and technical security requirements and apply existing frameworks (e.g., NIST CSF) and standards (e.g., ISO 27000 series) to help with the implementation, as appropriate.

8.2.6 Identified security requirements

To deliver on the foundational principles of safety and privacy, the CIoT with TIPPSS solution providers shall develop and maintain a set of common security requirements and perform specific security activities that protect devices and systems, the development and production environment, and the maintenance infrastructure.

This shall result in CIoT devices and systems that provide the desired security baseline, can be securely operated in the intended target environments, and allow for the maintenance of their security posture over the device and system's useful life.

A security risk management-based approach shall lead to the development and implementation of appropriate security controls and shall be supported by security-specific testing activities.

CIoT device and related solution design shall support required security features for the CIoT use cases and technology capabilities, including the following:

— Unique device and version identification.

— Secure authentication and authorization.

— Design features protecting device and solution security and data confidentiality, availability, and integrity.

— Secure device configuration and maintenance.

— Data protection.

— Logical and physical access security.

— Cybersecurity state awareness, event detection, and logging.

Security activities throughout the secure CIoT solution development lifecycle shall include:

— Secure device lifecycle management best practices, e.g., threat modeling and risk assessment.

— Identification and following of secure engineering best practices as well as adherence to coding and hardening conventions.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

- Policies and processes to enable supply chain security from discrete component selection and implementation through production and maintenance.
- Security assessment and testing activities, e.g., application security testing such as Static Application Security Testing (SAST) or Dynamic Application Security Testing (DAST), malformed input testing (fuzzing), boundary value analysis (BVA), known vulnerability assessment, malware testing, and penetration testing.
- Effective vulnerability management and remediation of discovered vulnerabilities by internal and external stakeholders.
- Verifying that code/programs that run on both devices and supporting infrastructure operate and execute under the PoLP to help protect infrastructures from potential malware infections.

Security activities, including solution development, testing, and release, shall result in the development of the required regulatory documentation and artifacts to demonstrate confidence in the secure design and maintainability of the device and solution. Typical documentation shall include the following:

- SBOM.
- Traceability matrix with mapping of identified risks to implemented controls.
- Testing plans and reports.
- System diagrams.
- Security properties and features documentation [e.g., via a NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2) [B4]].
- Risk and vulnerability management plans.
- Security maintenance plans.
- End-user/operator documentation including a description of security capabilities and constraints.
- Justification for not implementing specific risk controls and mitigation or dispositioning of resulting risks.

To enable security management and maintenance activities during development, production, and operation, the CIoT with TIPPSS solution providers shall establish a device and software versioning scheme that enables matching and maintenance of device version with the respective documentation, premarket security management activities (e.g., testing), and postmarket maintenance (e.g., updates).

The CIoT with the TIPPSS solution provider shall continually monitor for changes in the pertinent regulatory environment, technology, device use cases, and threat landscapes, and assess whether security processes and controls need to be adjusted.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

8.3 Basic security principles

There are four basic security objectives that a CIoT solution shall adhere to in its integrated target operating environments throughout the solution's useful life, as follows:

- The solution shall meet a security baseline as determined by a risk-based approach to architecture, design, and requirements development, which is balanced with use cases, solution capabilities, applicable laws, and regulations.
- The solution design and supporting processes shall be such that the security baseline can be managed in the intended use environments and can be maintained during its expected life.

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Devices shall be able to communicate securely within their intended integration environments and shall provide a unique identity so that operators or other devices can establish trust.

— Devices shall be able to communicate their security status digitally and shall be able to detect, assert, preserve, and communicate relevant security information and events.

CIoT device and solution security capabilities continue to evolve, including the potential to leverage technologies such as AI/ML, quantum computing, and quantum cryptography, which may be adapted in the future to address current and future security considerations. Solution providers should stay abreast of technologies and innovations to advance security solutions in response to potential new and evolving security threats.

8.3.1 Developing a security baseline

CIoT solution providers shall develop a security baseline by analyzing security risks through a formal risk assessment process, architectural security review, and/or threat modeling. The solution providers shall consider a complete system view and security relationship of all the elements of the solution, with an integrated systems view, from the devices to the environment. Any device or solution introduced into an ecosystem poses a security risk to that ecosystem; for instance, attackers may use a device as a beachhead for an attack such as a denial-of-service (DoS) attack, or as a vehicle for malware infection. The security risk assessment process should lead to the development of a security baseline for the CIoT solution and devices, which may include a recommendation for implementation of security practices such as hardened design, least/minimum privilege, or zero trust.

8.3.2 Meeting a security baseline

To meet the established CIoT solution baseline, the solution provider shall develop and deploy guidelines for people, process, and technology as follows in 8.3.2.1 and 8.3.2.3.

8.3.2.1 People

— Solution providers shall identify regulatory and legal liabilities and define, communicate, and acknowledge individual responsibilities to address them based on role.

— During the development of the SSDLC process, solution providers shall sufficiently staff security activities.

— Solution providers shall train all security-responsible personnel as required for their respective responsibilities.

— Solution providers shall train all staff in general security principles and basic security hygiene.

— Solution providers shall regularly update all training to account for changes in state of the art security laws, regulations, and standards.

8.3.2.2 Process

— Solution providers shall establish and follow device management plans, policies, and procedures that align with the FDA's Total Product Lifecycle for Medical Devices (TPLC) approach, and/or the EU Medical Device Regulation, MDR; 2017/745, and/or other applicable and dependent regulations.[22]

[22] See https://www.fda.gov/about-fda/cdrh-transparency/total-product-life-cycle-medical-devices.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Solution providers shall establish and follow SSDLC plans, policies, and procedures.

— Solution providers shall define and establish formal security roles and responsibilities.

— SSDLC security activities shall include security considerations during architecture and design, such as threat modeling, security requirements specification, risk assessment, and vulnerability management.

— Solution providers shall document, maintain, and archive process outputs as well as decisions and approvals.

— Solution providers shall establish and analyze security measures and metrics to improve the individual product and solution security posture, as well as to continually improve security processes and practices.

— Solution providers shall establish and follow secure coding conventions.

— Solution providers shall identify and follow platform hardening practices established by providers of solution elements, e.g., by the OS supplier.

— Solution providers shall continually perform security activities, e.g., code review or testing, during the SSDLC, both at the level of individual modules and at applicable integration stages.

— Solution providers shall establish a formal supplier security management program. This shall include security assessments, documentation, contracting, auditing, and dedicated supply chain and SBOM risk management.

— The solution provider shall select a platform and other third-party components used in the solution or during development, production, or maintenance to:

  1) Provide the desired security baseline.

  2) Provide security maintenance throughout the device and solution's expected life.

— The solution provider shall perform dedicated security assessment and testing during device and solution verification and validation to provide for the successful implementation of security controls and confirmation of meeting requirements.

— The solution provider shall establish and document full end-to-end traceability during the individual stages of the device development lifecycle, including risk assessment, risk mitigation, security requirements, controls implementation, and testing.

8.3.2.3 Technology

Security is typically implemented at various architectural levels: platform (hardware, OS), application and third-party software, information (data), communication (e.g., network), and at the integrated system or solution level. Different security practices and technologies are required to realize security controls at varying levels. For example, anti-malware software may be chosen to protect the OS but may provide little protection for data being transmitted, for which encryption may be a better choice. Similarly, encryption is highly effective in protecting sensitive data, yet may do little to protect an OS from malware.

Solution providers shall consider security controls at every level for the overall integrated solution architecture and design across the platform, applications, information, devices, and network. As appropriate for the device use case and technology capabilities, the CIoT with TIPPSS device solution provider shall establish general security best practices and common principles. Solution providers will realize them in the solution design, development, and release. The solution architecture and design shall follow commonly accepted security practices, including the following:

a) Security, protection, safety, effectiveness, and privacy by design

b) Principle of least privilege

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

c) Defense in depth architecture:

1) Layered security at the hardware, firmware, software, and service levels

2) Compensating security controls in case the primary controls fail

3) Default to the highest level of security.

d) Zero trust approach and integration capabilities

e) Use of security trust zones

f) Hardened design for all solution elements, including applications and third-party components

g) RBAC and segregation of duties (SOD)

NOTE—Role-based access control is the policy-neutral prevailing paradigm that restrains access to system resources based on the roles granted to users. The model consists fundamentally of role definition, role assignment, role authorization and, subsequently, permission authorization, ensuring that an entity has exactly the permissions that its role specifies. RBAC allows simultaneous exercising of permissions for multiple roles. Solution providers can extend flat RBAC to cover role hierarchies (hierarchical RBAC) and separation of duties (constrained RBAC). Solution providers can also modify RBAC to implement other less generic access control technologies, e.g., discretionary access control (DAC) and mandatory access control (MAC).

h) As appropriate for devices and use cases, solution providers shall implement authentication best practices, including the following:

1) Architecting for least/minimal privilege access and operation, including minimum necessary (need to know).

2) Avoid default, easy-to-guess, or hard-coded user or device credentials.

3) Providing means for separate and unique identities for devices and users.

4) Enforcing minimum requirements for credential length, complexity, and update frequency.

5) Implementing local and remote session control features, e.g., limit of failed log-ons, re-authentication.

6) Enabling the use of inactive mechanisms (e.g., time-out, automatic log-off).

7) Implementing cryptographically secure credentials management.

8) Providing MFA where needed and acceptable (e.g., for remote access or high-privilege system access).

9) In case the device use case or underlying technology requires alternate authentication mechanisms, carefully evaluating for equivalency and any potential reduction in security posture and communicating that to the user/operator.

10) In the case when devices utilize API communications, utilizing an API gateway or similar proxying technologies to examine for and protect against threats as part of the overall architecture to reduce threats to the individual devices.

i) Data minimization.

j) Interface security:

1) Close/disable all unused ports and processes.

2) Close/disable all test and debug ports and features.

k) Fail-safe mode and capabilities/maintenance of essential functions in case of security compromise or loss of connectivity.

1) Design for a fail-safe and/or minimal function mode.

2) Provide device recovery and restoration functions.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

l) Protect confidentiality, integrity, and authenticity of data at rest and in motion through the appropriate cryptographic methods.

   1) Cryptographic module security: Cryptographic modules used shall meet the security requirements defined in the most current version of ISO/IEC 19790 [B25], which specifies the security requirements used by cryptographic systems to protect sensitive information.

   2) Solution providers shall test cryptographic modules using methods conformant with the most current version of ISO/IEC 24759 [B28], which specifies conformance testing requirements.

   3) Enable secret material protection on the device as well as during provisioning, maintenance, and device lifecycle management.

m) Implement supporting physical security.

n) Reduce the need for environmental/external and procedural security controls.

o) Support device recommissioning/decommissioning processes and data sanitization.

p) Solution providers shall assess security features and capabilities for inclusion in the design based on device capabilities, integration and use environment, patient risk, and use case. The solution provider shall identify and determine security features to be implemented. Solution providers should reference standards, guidance, and best practices, e.g., IEC TR 80001-2-2 [B16] and features like automatic logoff (ALOF), audit controls (AUDT), health data integrity and authenticity (IGAU), or malware detection/protection (MLDP).

8.3.3 Maintaining a security baseline

The CIoT with TIPPSS solution provider shall provide security maintenance features and processes that enable the maintenance of a device's security posture, as follows:

a) Shall provide for the maintenance of the device's security baseline for the expected economic life of the product.

b) Shall protect the production environment to enable device quality and help prevent device security compromise.

c) Shall protect the device operational infrastructure, the production environment, and device maintenance infrastructure, against cyber threats.

d) Shall provide or recommend supplemental security protection through commercial technologies [e.g., antivirus, host-based intrusion detection system (HIDS), firewall] as appropriate for the device use case, desired security posture, and maintainability.

e) Shall provide all necessary security documentation and instructions to the device buyer and operator, including:

   1) Documentation that allows the buyer to assess the device's security capabilities (e.g., SBOM, MDS2), which should be provided in machine-readable format as such standards become available.

   2) Instructions on secure operation, security maintenance, recognition of security events and compromise, and handling of security events.

   3) Documentation about integration with network and enterprise security systems.

   4) Information about known vulnerabilities and risks.

   5) Description of security risk considerations in the intended use environment as well as risks outside the intended use environment.

f) Shall provide documentation to support operator implementation, operation, and security maintenance, including:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

1) List of external interfaces and protocols used for local and remote access, including description of use during normal operation and maintenance.

2) Relevant system security information, e.g., SBOM, system diagrams, security properties and features, secure operating environment, and security integration.

3) Description of device security event detection and logging capabilities.

4) Security risk assessment and plans for continual postmarket risk and vulnerability management.

5) Traceability matrix (identified security risks to implemented security controls).

6) Security testing plans and reports.

g) Shall establish and perform postmarket surveillance policies and processes to collect and analyze cybersecurity signals and monitor for changes, including:

1) In technology or device use cases.

2) The threat landscapes.

3) Application and supply chain vulnerabilities, as reported by vendors, users/operators, security researchers, government entities, and regulators.

4) Security events as provided by device and infrastructure detection capabilities, user and operator reports, service personnel reports, or returned devices.

h) Shall establish a formal postmarket vulnerability and risk management program, including:

1) Acquisition of and analysis of cybersecurity signals.

2) User/operator communication.

3) Communication with the public, regulators, government agencies, or law enforcement.

4) Release of interim and final mitigation.

i) Shall establish formal policies and processes for the deployment of risk mitigation, including:

1) Communication and distribution via established business and technical channels.

2) Secure deployment and update (e.g., utilizing cryptographic technology like code signing).

3) Version and change management and tracking.

j) Shall provide all relevant procedures that describe its postmarket security activities, including:

1) Postmarket vulnerability and security risk management plans.

2) Security update plans, e.g., how organizations will communicate, provide, and deploy patches and updates.

3) Incident management and disclosure plans.

4) Procedures for collecting and analyzing postmarket security information (new vulnerabilities, threats, incidents, and root causes) as well as user experience.

5) Update of device design as well as premarket and postmarket security procedures based on analyzed findings.

6) Procedures for reporting security incidents as required by applicable laws and regulations.

7) Publication of regular postmarket surveillance reports.

k) Shall provide documentation and instructions pertaining to the device's technical security capabilities and integration requirements, including:

1) General product security specifications:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

i) Intended operating environment (firewall rules, ports, interfaces, protocols, addressing schemes, etc.).

ii) System diagrams.

iii) Security configuration guidelines.

iv) Minimum platform/hardware/integration requirements.

v) Supporting infrastructure requirements and recommended external security controls.

vi) Secure networking/integration (network requirements and diagram).

vii) Safe combination/performance characteristics.

2) Implemented security controls:

i) Security and hardening features.

ii) Features that protect critical functionality.

iii) Fail-safe mode.

3) User roles and privileges:

i) Authentication.

ii) Access control.

iii) Account and password features and management.

4) Description of interfaces and ports:

i) Network, Bluetooth, USB, proprietary, etc.

ii) Interfaces and encryption of data transmitted by or stored externally to the device.

iii) Open/closed/required interfaces and ports and description of their function.

iv) Network data streams (protocol types, origin/destination of data streams, addressing scheme, etc.).

5) If applicable: Description of remote hosting environment (what, where, and how data is stored and managed and applicable security controls).

6) Security event and incident logging features and log management:

i) Forensic evidence captures and retention capabilities.

ii) Event trigger(s).

iii) Types of data captured.

iv) Format and integration [e.g., Security Information and Event Management (SIEM)].

v) Protection and forensic integrity/immutable log.

vi) Event metadata (where, when, how, etc.).

7) Device cybersecurity end-of-life/end of support (EOL/EOS information).

8) Device capabilities to detect and respond to anomalous conditions and events.

8.3.4 Software Bill of Materials (SBOM)

The support and use of SBOM is an emerging requirement within the CIoT ecosystem. Within an SBOM, it is required that the identity of every software component (API, SDK, library) used in the CIoT device, shall be included. Currently, there are three primary formats for an SBOM: Software Package Data Exchange (SPDX), Software Identification (SWID) tag, and CycloneDX. SBOMs have been identified as a piece of

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

critical technology standards and infrastructure. This is driving significant innovation in this sector and manufacturers should invest the time to stay abreast of the changes.

Per National Telecommunications and Information Administration (NTIA), minimum elements for SBOMs shall show, for each software component: supplier, component name, version, any unique identifiers like CPE SWID or persistent uniform resource locator (PURL), dependency relationship, and the author of this information along with a time/date stamp for when the solution provider generated it.

These minimum elements, according to NTIA, include the following: SBOM, NEMA MDS2, product description, operating system, network ports and services, sensitive information and data transmitted, sensitive information and data stored, network and data flow diagram, malware protection, authentication, network controls, physical controls, encryption, audit logging, remote connectivity, service handling, end-of-life and end-of-support, risk summary, third-party certification or attestation, vulnerability and patch communication and management processes, information about data storage and data removal.

Others to consider are as follows:

— User information pertaining to the device's cybersecurity controls, potential risks, and other relevant information.

— Global system view: overall system, including the device itself and all internal and external connections. For interconnected and networked devices, this view should identify all interconnected elements, including any software update infrastructure(s), healthcare facility network impacts, intermediary connections or devices, cloud connections, etc.

— Description of security maintenance tasks that are relevant to the operator, including how the manufacturer will communicate cybersecurity information.

8.4 Communication security

8.4.1 Interoperability and security

The solution provider shall recommend appropriate security controls and safeguards. The operator/user shall implement these for safe and secure interoperability aligned with the TIPPSS principles. These requirements can be further categorized into the following interoperability scenarios:

— Technical interoperability

— Semantic interoperability

— Syntactic interoperability

— Organizational interoperability

— Regulatory interoperability

Technical interoperability is accomplished through communication links, protocols, and infrastructure that enables the transmission of data between solution components, devices, and systems. It refers to the lower layers of the Open Systems Interconnection (OSI) model (i.e., transport layer and lower). To enable secure technical interoperability, solution providers and organizations using CIoT solutions shall do the following:

a) Shall enable information communication from different protocols via protocol conversions (e.g., converting from Zigbee to Bluetooth).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

b) Shall conduct risk assessments of the devices, operating environments, ecosystems, and use cases using well-known frameworks.

c) Shall tailor risk assessments to use standards and requirements applicable to the target devices, operating environments, ecosystems, and use cases.

d) Shall secure information exchange and confidentiality, integrity, and authenticity.

e) Shall define information elements pertaining to the exchange of security risks, including:

   1) Threats/Exploits

   2) Vulnerabilities

   3) Events/Incidents

f) Shall apply commonly accepted frameworks, guidance, standards, models, and practices (e.g., NIST CSF, MITRE D3FEND) as part of a risk mitigation plan.

g) Shall develop plans to address and track risk mitigation scenarios and issues.

h) Shall maintain safety, effectiveness, and secure interoperability during normal operations as well as during crises (e.g., natural disasters).

i) Shall develop plans to receive information from stakeholders on security issues and concerns, assess them, and address them in accordance with ISO/IEC 29147 [B32] and ISO/IEC 30111 [B33].

j) Shall enable data validation and authentication.

Semantic interoperability is enabled through the definition and standardization of information to be shared and processed, ensuring it is well-understood by the interoperable systems, without ambiguity. Strategies for semantic interoperability include the utilization of unambiguous codes and identifiers for health information, e.g., clinical terminologies, taxonomies, or ontologies, such as LOINC, SNOMED-CT, ICD-10, etc. To enable secure semantic interoperability, the CIoT with TIPPSS solution provider shall do the following:

k) Shall provide a level of security that enables safety, effectiveness, quality of care, and trust in care received.

l) Shall define semantic elements pertaining to the definition of security risks for the following:

   1) Threats/Exploits

   2) Vulnerabilities

   3) Events/Incidents

Syntactic interoperability defines the data structure and data formats, including the communication and exchange rules for different kinds and types of data, how to put them together, and in which order. Examples of syntactic interoperability approaches are the definition of data formats, well-defined syntax, and encoding (e.g., message content structure, size of headers, size of message body, fields contained in a message), such as different versions of HL7 or ISO/IEEE 11073. To enable secure syntactic interoperability, the solution provider and organizations deploying CIoT solutions shall do the following:

m) Shall implement secure exchange and information confidentiality, integrity, and authenticity.

n) Shall define syntactic elements pertaining to the enumeration of security risks, including:

   1) Threats/Exploits

   2) Vulnerabilities

   3) Events/Incidents

o) Shall enable data validation and authentication.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Organizational interoperability focuses on coordination of distributed workflows and activities between systems, organizations, and people interacting in business processes. This includes defining how business services and consumer services interact, understanding pertinent information and sharing the information, using the correct format for the correct business processes. To accomplish secure organizational interoperability, organizations shall do the following:

- Shall conduct risk assessments of the devices, operating environments, ecosystems, and use cases using well-known frameworks.
- Shall tailor the assessments to use standards and requirements applicable to the above.
- Shall apply commonly accepted frameworks, guidance, standards, models, and practices (e.g., NIST CSF, MITRE D3FEND) as part of a mitigation plan.
- Shall develop plans to address mitigations and issues and track them.
- Shall maintain safety and effectiveness as well as secure interoperability during normal operations as well as during crises (e.g., natural disasters).
- Shall develop plans to receive information from stakeholders on security issues and concerns, assess them, and address them in accordance with ISO/IEC 29147 and ISO/IEC 30111.

Regulatory interoperability focuses on ensuring that organizations operating under different legal frameworks, policies, and strategies can work together and exchange information. Organizations shall do the following to enable secure regulatory interoperability:

- Shall implement secure exchange of clinical, identification and technical information between devices and systems across the ecosystem including all stakeholders (operators, users, patients, etc.).
- Shall enable the meaningful and actionable sharing and management of information among stakeholders as it pertains to security risks: threats, vulnerabilities, events, and incidents.
- Shall enable encryption of data at rest and in motion.
- Shall enable secure identity and access management practices.
- Shall validate and authenticate critical data (e.g., clinical data, firmware updates).

8.4.2 Communicate securely

In case of communication failure, the device shall provide a fail-safe mode and shall continue its operation without connectivity until the service provider or user/operator resolves the issue and reinstates communication.

CIoT with TIPPSS devices and solutions shall use a level of cryptographic information protection as appropriate for the use case and based on the device's capabilities, as follows:

- Devices and solutions shall use cryptographic technology to support confidentiality, integrity, and authenticity of critical data, including patient medical and demographic data, user and device credentials, device settings and configuration, software updates and patches, intellectual property, etc.
- Solution providers shall respond to cryptographic errors or exceptions in consideration of the device use cases.
- The device shall communicate through end-to-end encryption rather than relying on the security provided by the transport layer for multiple reasons, including:
    1) It may not support the device use case.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

2) All network segments that the data traverses may not support it.

3) It depends on the actual implementation, thus leaving room for user error and compromise.

Specific considerations shall be applied to the certificates or keys (secret material) used in the cryptographic process, as follows:

— Cryptographic secrets (certificates and keys) require special consideration and protection:

1) Devices and solutions shall protect them during the provisioning process, in memory, and during updates.

2) Devices and solutions shall never be exposed to third parties (e.g., a contract manufacturer) and shall always be protected.

3) Devices and solutions shall never use identical (i.e., the same) keys between devices or groups of devices.

— Devices and solutions shall use different keys and certificates for different device functions to enable the separation of risk between said functions. (e.g., the certificate used for managing device network traffic should differ from the one used for software updates).

— Certificate hierarchy shall reflect organizational and product line structure so that solution providers and/or users/operators can specifically manage key revocation for individual lines of business.

Solution providers and users/operators can use cryptography to address many different use cases that improve the device's security posture, provide privacy, and protect business interests. However, correct implementation requires that solutions address all aspects of cryptography, as follows:

— Algorithms, keys, and certificates shall be selected by the deploying organization such that each fits the use case, provides the desired level of protection, and can be implemented without undue burden on device hardware.

— Solution providers shall design a supporting infrastructure to avoid compromise or corruption of cryptographic functions or secret material. This includes memory protection, secure provisioning and device lifecycle management, and appropriate error and exception handling.

— Asymmetric cryptography with a supporting PKI should be the preferred approach. If a symmetric key solution is chosen (e.g., due to resource limitations), the trade-off in security and higher risk of compromise shall be carefully evaluated and formally accepted as part of the manufacturer's design decision process.

8.4.3 Communicate about security

CIoT with TIPPSS devices and solutions may be operated in an infrastructure of existing security tools and workflows. Therefore, those devices and solutions shall provide the following features that also shall be documented in the device and solution's installation and operating instructions:

— The devices and solutions shall be able to withstand interrogation by typical network security tools, e.g., enterprise asset and risk management systems and discovery and vulnerability scanners.

— The devices and solutions shall be able to provide version and patch level information when queried.

The user documentation shall describe the type of network handshake or user interaction required to read or transmit device version and patch information.

If the device or solution includes specific configurable security capabilities and/or if the security features require management, the device or solution shall be able to provide status information of these capabilities, e.g., antimalware software installed and running, virus definition file up to date, last date of update.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The devices and solutions shall be able to detect security events and, as appropriate for the use case and capabilities:

  1) Provide features enabling security event detection, logging, and user/operator notification.

  2) Support integration with security management infrastructure.

  3) Transmit security event information to enterprise security tools or services [e.g., SIEM or Security Operations Center (SOC)].

  4) Store and immutably retain security events information and other forensically relevant security event data and metadata for later analysis, including time, location, trigger, indicator of compromise (IoC), etc.

  5) Provide event and forensic logs.

  6) Provide information on its operating state, e.g., if the device is operating in a fail-safe mode due to security compromise.

8.4.4 Communication as a security risk

In addition to the need to communicate securely and to communicate about its security status, a CIoT with TIPPSS device or solution shall also protect its interfaces and external communications from compromise, i.e., prevent a device's connectivity from becoming a security risk. Examples of security risks due to device connectivity include known vulnerabilities in short-range wireless technology or Transport Layer Security (TLS) protocols, exploitation of Remote Desktop Protocol (RDP), or the security risks associated with Simple Network Management Protocol (SNMP).

CIoT with TIPPSS solution providers shall consider that any interface and connectivity may introduce security risks, no matter the function. In other words, any function that executes via connectivity, including functions for the purpose of security (e.g., patch download or security event data upload) is an operational security risk and shall be analyzed and mitigated as part of the security risk assessment process.

The CIoT with TIPPSS solution provider shall apply common security strategies to prevent unnecessary exposure to security risks through connectivity, for example:

— Close unused network ports.

— Disable unused protocols.

— Use, and update to, the latest known version of a communication protocol.

— Consider additional security controls, e.g., hardware or software firewalls.

8.5 Processes, practices, principles, and controls

8.5.1 CIA triad

In information security, it is common to use the CIA triad, which comprises three core elements that describe and characterize the main properties of data security—confidentiality, integrity, and availability. These are the building blocks upon which organizations design security systems, and the essential aspects the systems assess, when discussing security processes, features, safeguards, etc.

Confidentiality restricts access of unauthorized entities to a resource. Integrity signifies that unauthorized entities will not improperly alter or remove the resource. Availability helps ensure that authorized entities are able to access and use the resource as and when required.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Numerous scholars, including Jeff Rothenberg of the Council on Library and Information Resources, have added the preservation of information authenticity as a fourth dimension as that provides the assurance that the data source can be uniquely and undeniably identified.

8.5.2 Confidentiality

Confidentiality means that unauthorized individuals, entities, or processes are not able to gain access to or disclose information. Confidentiality is a component of privacy and protects information from access by or disclosure to unauthorized persons or processes.

Secure design and the use of security technologies can help reduce the risk of a confidentiality breach. The CIoT with TIPPSS solution provider, as part of their privacy risk assessments, shall determine which data elements require protection as well as the level of protection provided within the limits of the device use case and capabilities. For details on privacy considerations, please see Clause 5.

The CIoT with TIPPSS solution provider should implement security technologies that solution providers, users, and operators can apply to achieve the desired level of confidentiality, including:

- Protection of operating system and application software.
- System hardening best practices.
- Access control principles: role-based, least/minimal privilege.
- Encryption of data at rest and in transit.
- Data minimization.
- Digital hardware protection.
- Physical security measures.

Commonly used technologies to protect data confidentiality rely on various cryptographic schemes that solution providers can use and apply as appropriate for the device or solution use case and its capabilities. However, these may also require complementary controls, such as physical security measures.

8.5.3 Integrity

Information integrity means assurance and maintenance of accuracy and completeness of data over its device lifecycle, i.e., the protection of data from accidental or intentional alteration or destruction by unauthorized persons, processes, or conditions. The solution provider shall implement controls to maintain integrity and protection against intentional and unintentional threats, as follows:

- Protection of critical information:
  1) Hashing, i.e., the calculation of a unique digital fingerprint of a file or string that allows comparing the file or string against the hash to detect unauthorized changes.
  2) Encryption to obfuscate data to prevent deliberate and unauthorized changes.
- Separation of processing and data:
  1) RBAC.
  2) Least privilege access and operation.
  3) Automatic logoff and timeout functions.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Protection of device integrity, i.e., functionality:

1) Protection of kernel and core functions.

2) Use of software update and runtime security measures, e.g., code signing and secure boot.

8.5.4 Availability

Availability refers to ensuring that data remains accessible by authorized persons or processes. This includes the computing or storage systems used to store and process data, the security controls used to protect it, and the reliability of communication channels used to access it.

Availability covers a wide range of requirements, including prevention against intentional or accidental destruction, preservation of access, and also preventing denial-of-service or similar network attacks.

The solution provider shall maintain device and information availability through design and security controls, including:

— Role-based access control.

— Hardware and physical protection.

— Redundancy and backup.

— Roll-back and restore functions.

8.5.5 Preservation of authenticity

Research and analysis can attribute every type of compromise to either one or several elements of the CIA triad. For example, installation of malware or compromise of the software supply chain are examples of system integrity compromises. However, it does make sense to look at the property of Authenticity separately as it takes on a unique function in today's interconnected world.

Authenticity includes the following:

— Assurance of people or systems' unique identities through user credentials or cryptographic certificates.

— Trust in the communication between and information provided by devices and/or people.

— Assurance of the authenticity of information including identification of the source.

— Providing for non-repudiation.

CIoT with TIPPSS solution providers shall support Authenticity as required for the device use case and for information and data, devices, systems, and people (users, operators, patients).

8.6 Security assurance

Security assurance requires demonstration that security efforts resulted in sufficiently reduced risk, helping to prevent device, data, and solution compromise. Demonstrating compliance with security standards and best practices, the use of tools like vulnerability scanners or standards managers, and services like penetration testing and independent security assessments can help provide security assurance.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Ultimately, continual assessment and timely response to reduce risks can help demonstrate security assurance. Solution providers can accomplish this by applying frameworks that are relevant to the domains of the system and the environment it operates in and documenting the results of such. The system and environment are dynamic and need re-evaluation on an ongoing basis to maintain security assurance.

Security implementations need to be measured against established requirements, which in turn shall be continually adapted based on threat landscape trends and observed security events. Demonstrating compliance with requirements and regulations may be sufficient to satisfy an auditor, but the auditor is not the adversary, and ultimately, sufficient security assurance requires continual reassessment and adjustment.

8.7 Risk management and security

8.7.1 Risk management overview

Risk is always present. It is not possible to totally eradicate risk, and it should be mitigated and reduced to acceptable levels. Solution providers, users, or operators may accept, share, transfer, or avoid risk. When it comes to healthcare, proper risk management is imperative.

The intent of this subclause is not to comprehensively describe risk management practices and processes, but rather to focus on the role risk management can play in enhancing security. To comprehend the intricacies of risk management's association with security, it is important to understand the key components that play a critical role in risk assessment. To focus on healthcare, there have been slight alterations to the definitions provided.

Figure 12 shows the relationship between threats, vulnerabilities, and assets, while Figure 13 includes the concept of risk.

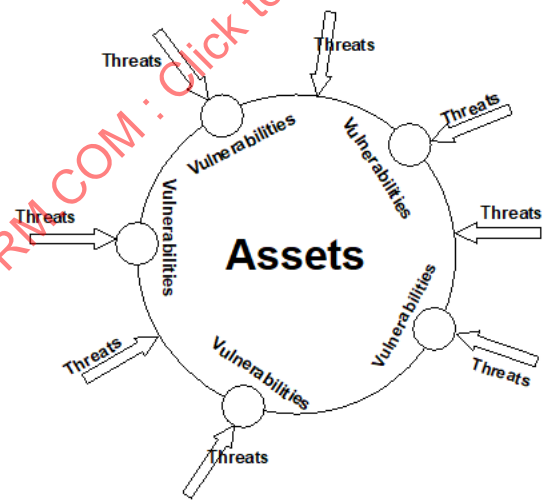

Figure 12—Relationship between threats, vulnerabilities, and assets

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

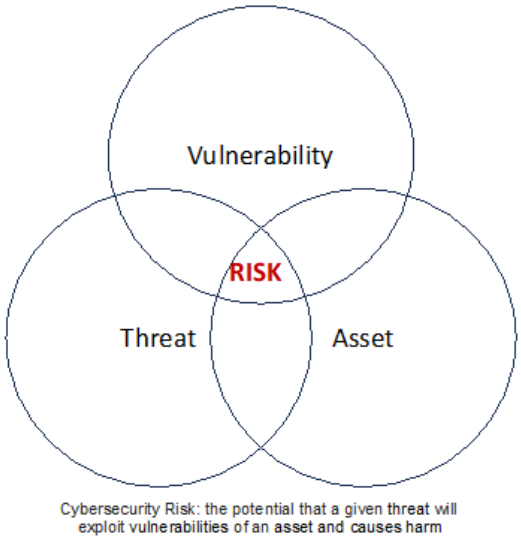

Figure 13—Cybersecurity risk—Conceptual

ULNORM.COM : Click to view the full PDF of UL 2933 2024

- Asset: An item of value. Including, but not limited to, medical devices, patients, healthcare providers, users, operators, service deliverers, information systems, but also non-tangible components like reputation or patients' decisions about where to seek care or which life-supporting technology is chosen.
- Threat: Any circumstance or event with the potential to adversely impact medical/healthcare operations and assets, including, but not limited to: medical devices and information systems; individuals such as service recipients, service providers, diagnosticians; treatment and therapy planners; other organizations via unauthorized access, destruction, disclosure, or modification of information and data being acquired, processed, stored and/or modified; and/or denial of service.
- Vulnerability: A weakness in a system that a threat can exploit, which could lead to an adverse event or result.
- Risk: The potential that a threat exploits a vulnerability leading to the compromise of an asset, leading to consequences, and impacting medical patient care devices, healthcare environment, information systems, ecosystems, data, diagnostics, delivery of services that have the potential to cause harm to the patient, operator, healthcare provider, organization, or environment.

As conceptually depicted in Figure 13, cybersecurity risk requires the presence of a threat, a vulnerability, and an asset of a given value to an organization. All three shall be present for a risk to exist with the level of risk being a function of the probability of occurrence (i.e., of a threat exploiting a vulnerability) and the severity of harm to the asset's value to the organization.

A method to quantify risk is by estimating probability (as a function of threat and vulnerability) and severity (as a function of vulnerability and asset value). Specifically in cybersecurity, risk estimators can sometimes replace or redefine probability as a measure of exploitability. Since statistical analysis of historical or testing data cannot always predict cybersecurity threats, an estimate of how easy it would be for an attacker to exploit a vulnerability is generally preferred.

Organizations can express these concepts as follows:

$Risk = f$ (threat, vulnerability, asset value)

Copyright © 2024 IEEE and ULSE. All rights reserved.

Quantifying risk requires an estimate of the following:

Probability of occurrence = *f* (threat, vulnerability), e.g., on a 1–4 scale, and

Severity of harm = *f* (vulnerability, asset), e.g., on a 1–4 scale.

Calculate the estimated risk level as follows:

Estimated risk = *Severity* × *Probability*

As shown in Figure 14, a matrix plot can identify the highest priority risks and the resulting estimate.

		Probability of harm			
		1 = Improbable	2 = Remote	3 = Occasional	4 = Probable
Severity of harm	4 = Catastrophic	4 Low priority	8 Medium priority	12 High priority	16 High priority
	3 = Critical	3 Low priority	6 Medium priority	9 High priority	12 High priority
	2 = Marginal	2 Low priority	4 Low priority	6 Medium priority	8 Medium priority
	1 = Negligible	1 Low priority	2 Low priority	3 Low priority	4 Low priority

Figure 14 — Example for a Risk Level Rating Methodology

Risk quantification notes:

— Organizations may use other scales for probability and severity.

— Synonyms and other terms may be used, e.g., likelihood or exploitability instead of probability or impact instead of severity.

— Organizations may choose to use other quantitative approaches or qualitative models.

8.7.2 Asset classification

The classification of a CIoT device's asset information and data shall be based on asset risk and value to the organization.

Assets under consideration that could pose a security risk and should be classified as such are as follows:

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Hardware shall include appropriate security classifications for appropriate use cases, environments, and local regulations.

— Subsystem and software shall include system categorizations and data classifications for appropriate localities of use.

— Information assets shall include the following:

1) Sensitive clinical, personal, and operational information.

2) User, device, and network credentials.

3) Intellectual property that requires safeguards.

4) Virtual—Infrastructure as a service (IaaS), servers, virtual network devices.

5) Cloud-based information assets.

— SBOM or equivalent shall include system assets and dependencies.

8.7.3 Data classification

Data shall be classified according to locally applicable regulations (HIPAA, PHIPAA, GDPR, etc.) and handled in accordance with all applicable legal and regulatory guidance that applies.

Device, network, and user credentials shall be classified as sensitive.

8.7.4 Vulnerabilities

Vulnerabilities exist along the healthcare technology value chain. Vulnerabilities shall be evaluated for each step undertaken in CIoT solution design and development and deployment, commencing from technology, system, and solution design to utilization, including the following:

— Design (component, device, software, subsystem, system, solution).

— Development (component, device, software, subsystem, system, solution).

— Manufacturing (flaws, supply chain management).

— Use (administering, workflow).

— Maintenance (spare parts, updates and patches, supply chain management, EOL, all components including hardware, firmware, software, and services).

Vulnerabilities shall be documented and disseminated to CIoT solution providers and users. This applies throughout the device lifecycle and its associated risk management processes, including the introduction of new risks triggered by new threats, which could appear in the form of software updates, new components, improper maintenance, or supply chain management, for example.

Organizations should have the following:

— A vulnerability disclosure policy in line with ISO/IEC 29147 [B32].

— The ability to easily receive vulnerability information from external sources.

— A vulnerability handling policy and associated organizational processes and frameworks in line with ISO/IEC 30111 [B33].

— The ability to responsibly and respectfully communicate and collaborate with vulnerability finders and reporters to verify, reproduce, and remediate the discovered issues.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The ability to disseminate advisories and resolutions through the appropriate channels (Healthcare ISAC, vendor advisories, press, etc.).

— The ability to drive appropriate internal and external post-resolution activities.

8.7.5 Threats

The cybersecurity threat landscape is constantly changing. New threats are emerging all the time, and with each new threat, the potential of an existing vulnerability being exploited is always present. Threats shall be classified by an organization into the following categories and evaluated continuously, albeit frequencies might differ for each category:

— Natural

— Environmental

— Human-made

Threats shall also be categorized into:

— Internal

— External

— Advanced persistent threat (APT)

— Emerging

8.7.6 Risk management cycle

Organizations using CIoT solutions and devices shall assess the state of their CIoT systems, assets, domains, and vulnerabilities regularly following a formal risk management process (see Figure 15). This evaluation shall include an assessment of the current state and vulnerabilities of all system elements, plus any changes and their impacts. Risk assessments shall be conducted on a regular basis. The organization shall also assess its ability to mitigate risks and whether the appropriate controls and safeguards are in place, including building them into devices during design, development, manufacturing, and deployment phases.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

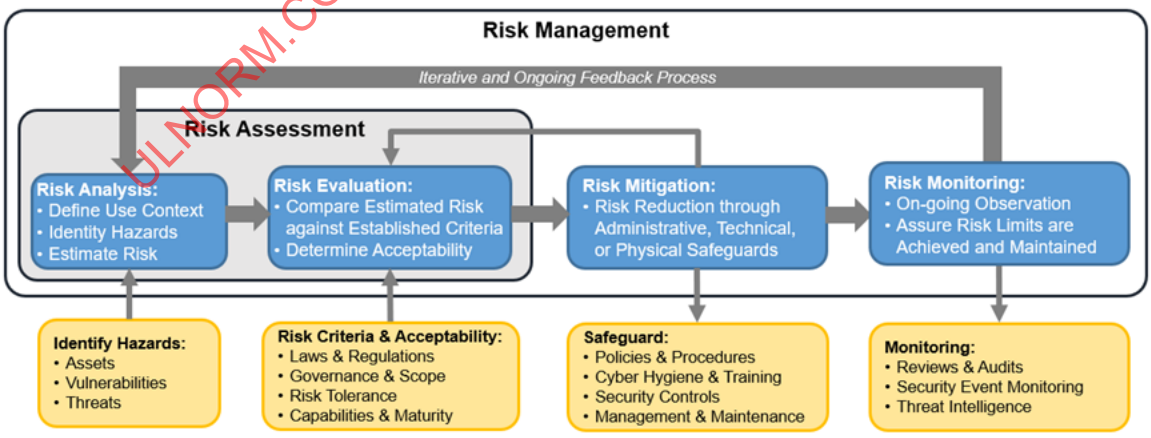

Figure 15—Risk management cycle

More detailed frameworks and standards on risk management, including ones specific to medical devices, are available, e.g., via ISO/IEC, NIST, HSCC, and AAMI.

Copyright © 2024 IEEE and ULSE. All rights reserved.

9. Human factors and usability

9.1 Overview

The use of IoT connected sensors, actuators and devices continues to increase for the clinical observation and treatment of patients. While most of these components are typically developed as medical devices, any device used in a clinical use case is considered within scope of this standard.

Use errors caused by usability issues have become an increasing cause for concern. CIoT devices are sometimes non-intuitive, difficult to learn, and difficult to use. As healthcare evolves, and as our use cases demonstrate in Annex B of this standard, less skilled users, including patients themselves, are now using CIoT devices while the devices are becoming more complicated. Usability engineering is intended to identify and minimize use errors and thereby reduce use-associated risks.

There are several usability/human factors standards, including standards specific to medical device design, such as IEC 62366-1:2015 [B14]. IEC 62366-1 defines Human Factors Engineering as the application of knowledge about human behavior, abilities, limitations, and other characteristics to the design of medical devices (including hardware and software), systems, and tasks to achieve adequate usability. In addition, ANSI/AAMI/UL 2800-1:2022 [B3] includes requirements for human factors analysis with a specific focus on interoperability.

This clause of the standard provides guidance and normative requirements for CIoT devices such as sensors, actuators, and applications (apps) to address CIoT connectivity and technical issues related to human factors. It focuses on usability related to the technical aspects of topics such as interoperability, validation, and TIPPSS-related requirements that apply to products that may be deployed by both professionals and untrained users such as patients or caregivers. It does not deal with general usability aspects related to the clinical aspects of the device since this is out of scope of this standard.

This clause deals with requirements related to the human factors/usability aspects of connectivity establishment, loss of connectivity, troubleshooting, etc. It is intended to be technology agnostic to the extent possible and avoid implementation specifics. It does not deal with the human factors aspects of the clinical application, such as setting infusion rates, alarm limits, display of measurements, etc.

This clause is driven by requirements derived from the use cases and identified in the Lead/Support/Consult (L/S/C) table in Annex C.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

9.2 Summary process for Usability Engineering

The manufacturer of a CIoT device shall establish, document, implement, and maintain a Usability Engineering process that addresses not only the clinical functionality but also the technical setup, operation, and maintenance of the CIoT device.

This process is based on IEC 62366-1 [B14], hence further background and guidance can be found in that standard. The following are key requirements for the manufacturer regarding additional CIoT device usability requirements when a device connects to a network.

9.2.1 Prepare the technical use specification

The manufacturer shall prepare a technical use specification that shall include the following:

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Intended user profile(s)

— Intended use environment(s)

9.2.2 Prepare hazard analysis related to technical user interface use cases and scenarios

The manufacturer shall identify technical user interface characteristics related to device network connectivity that could be related to safety. Manufacturers and solution providers may accomplish this by conducting a hazard analysis (typically in accordance with ISO 14971 [B20]) to identify risks due to technical user interface issues and help reduce the risk of harm to a level that is as low as reasonably possible using the following options:

— Inherent safety by design.

— Protective measures in the CIoT device itself or in the manufacturing process.

— Information related to safe use in the instructions for use (IFU).

The hazard identification and analysis shall include the following:

— Identification of known or foreseeable hazards and hazardous situations related to device IoT connectivity.

— Identification and description of hazard-related use cases and scenarios focusing on device IoT connectivity.

— Selection of the hazard-related use cases and scenarios for summative evaluation.

— Incorporation of feedback from user testing during concept and product validation related to device IoT connectivity.

9.2.3 Establish a technical user interface specification

The user interface specification shall include the following:

— Testable technical requirements relevant to the user interface concerning the device IoT-related setup and operation.

— Required included indications of content in the accompanying documentation related to the device IoT connectivity.

— Indications as to whether training is required for device IoT connectivity setup, operation, and removal from service.

9.2.4 Establish a technical user interface verification plan

The manufacturer shall establish and maintain a technical user interface verification plan that documents the objectives and methods of the various verification activities.

The manufacturer shall verify that the system has properly implemented the technical user interface specification.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

9.2.5 Establish a technical user interface validation plan

The manufacturer shall establish and maintain a technical user interface validation plan that documents the objectives and methods of the various formative or summative validation activities.

The validation activities should reproduce/simulate the actual user environment to the extent possible.

9.2.6 Perform a technical user interface design, implementation, verification, and formative validation

The manufacturer shall design and implement the CIoT device user interface, including the accompanying documentation and training as described in the technical user interface specification.

Verification shall be undertaken by the CIoT device manufacturer at each stage of the design.

Formative validation should be used as appropriate during the implementation process to test the usability of specific aspects of the design.

9.2.7 Perform technical user interface summative evaluation/validation

Summative evaluation/validation shall be used to evaluate the usability of the overall design of the CIoT connectivity functionality.

The manufacturer shall use summative evaluation/validation in a simulated or actual user environment with the participation of people representative of the intended users.

9.3 Requirements for the technical aspects of the Clinical IoT device user interface

The requirements in this subclause derive from the L/S/C table in Annex C, which can be consulted to trace the appropriate user needs/requirements to these technical requirements.

9.3.1 General—Human factors requirements

The requirements are as follows:

- The CIoT device shall notify users of communications connectivity issues.
- The CIoT physical device shall alert when it is time to change or replace the physical device battery or it encounters other technical issues.
- The CIoT device shall indicate that data from a CIoT physical device requiring battery replacement is questionable.
- The CIoT device shall notify the user and any connected CIoT devices of any software (SW) and/or firmware (FW) update failures.
- A CIoT device shall allow the user to disable its non-critical technical alerts.
- Return Instructions for the CIoT physical device should be accessible on the CIoT device as well as any connected CIoT devices.
- All systems should consider accommodations for regional cultural norms.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The CIoT device shall advise users of the result of remote change commands (on the user interface) that were requested in a timely fashion.

— The CIoT device shall allow local or remote users to distinguish between distinct types of failures and notify the user.

— The CIoT device shall notify users of any remote settings changes made to their devices.

— The CIoT device shall alert users of any failures of connected CIoT devices.

— All CIoT devices and systems shall consider user interface accommodations for the intended user group, including those with disabling (visual, auditory, cognitive, mobility, etc.) conditions as well as cultural and linguistic accommodations.

NOTE—Consider the fact that a user who is also a patient may have one or more disabling conditions.

9.3.2 Accompanying documentation—Human factors requirements

The requirements are as follows:

— The manufacturer shall disclose the data communication capabilities of the CIoT device.

NOTE—Data communicated includes clinical data communicated, technical data communicated, control capabilities, personal data communicated.

— Instructions for technical setup and use of the CIoT device shall be readily available.

— The manufacturer shall disclose disclaimers and warnings for the CIoT device in the accompanying documentation.

— The manufacturer shall provide clear instructions concerning proper environments of use for the CIoT physical device.

— The manufacturer shall disclose connectivity troubleshooting information in the accompanying documentation, if applicable.

NOTE—Connectivity includes wired connectivity such as USB or RS-232 and wireless connectivity such as IEEE 802.11, cellular, IEEE 802.15, etc.

— The manufacturer shall disclose which jurisdictional regulatory requirements it complies within the accompanying documentation.

— The manufacturer shall disclose their accommodations for regional cultural norms in the accompanying documentation.

— The manufacturer shall disclose the size of the CIoT device log.

— The manufacturer shall provide detailed installation, provisioning, troubleshooting, and deprovisioning instructions for users to follow.

NOTE—Users include patients, caregivers, service providers, integrators, etc.

— Deployment organizations (integrators, service providers, etc.) and end-users (patients, caregivers, etc.) shall follow the manufacturer-provided instructions for provisioning and deprovisioning of CIoT devices.

— The manufacturer shall disclose whether the CIoT device contains AI/ML in the accompanying documentation.

— All CIoT devices shall disclose their accommodations for individuals with disabling (visual, auditory, cognitive, mobility, etc.) conditions in the accompanying material.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

9.3.3 Trust—Human factors requirements

The requirements are as follows:

- A CIoT device shall indicate data from an expired or partially functioning sensor or actuator as questionable on its display.
- A CIoT device shall indicate data from a sensor requiring battery replacement as questionable on its display.
- A CIoT device shall alert the user if it suspects any connected CIoT device is counterfeit.
- A CIoT device shall notify the user if the connected CIoT device does not meet the requirements for its intended use and, as a result, should not use it.
- Patients shall be able to authorize specific caregivers to view results in any portal applications provided by the deploying organization.

9.3.4 Identity—Human factors requirements

The requirements are as follows:

- The CIoT physical device shall support NFC or Radio Frequency Identification (RFID) or Bar-Code or label or similar with CIoT device attributes/identity on the CIoT physical device.
- CIoT physical devices should have a mechanism for entering their physical locations in the hospital, such as bed number, room number, care unit, hospital name, etc.
- Authenticated caregivers shall be able to establish accounts in any portal applications provided by the deploying organization.

9.3.5 Privacy—Human factors requirements

The requirements are as follows:

- If the CIoT device log contains electronic protected health information (ePHI), the CIoT device should give the patient the opportunity to consent to its collection.
- The manufacturer shall enable deployment organizations or end-users to temporarily disable CIoT device communication to a portal.
- The manufacturer shall enable deployment organizations to authorize authenticated users/caregivers to only view results of specific patients.
- The CIoT device shall allow the patient to acknowledge/provide permission for any remote change commands.
- Applications (apps) shall support the management of data acquired via user consent.
- Privacy notices shall be easily accessible via the user interface of the CIoT device.
- Users should be able to disable part or all the results reporting from their CIoT devices.
- CIoT devices shall only acquire the minimal amount of data required to meet their intended use.
- The manufacturer shall establish and implement a process to evaluate privacy risks when starting a new IT project or changing a business process—Define what “high risk” or “risk” means for the organization from the manufacturer’s perspective and the deploying organization of the CIoT devices.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The manufacturer shall establish processes to identify, prioritize, and report or disclose data privacy incidents reported to the manufacturer, as required by local regulations.

— The manufacturer shall establish technical measures to implement secure deletion of data upon the request of the patient.

— The CIoT device accompanying documentation shall state the intended use of data.

— The CIoT device shall limit data collection to the minimum required.

9.3.6 Safety—Human factors requirements

9.3.6.1 General safety requirements

The requirements are as follows:

— Solution shall support limited but safe operation without complete setup of patient information.

— The manufacturer shall provide information to the user regarding the safe and secure use of its products.

— CIoT device shall alert when it is time to charge or replace its batteries.

— Guardrails/limits shall be inherent in any algorithms to limit actuator actions.

— The manufacturer shall enable the deployment organization to authorize authenticated users to enable/disable the control panels of the remote CIoT devices.

— The solution shall notify the remote user/caregiver if the connection to a specific CIoT device has failed.

— The solution shall notify the remote user/caregiver if the connection to all CIoT devices has failed.

— The solution shall notify the user of any settings changes made remotely and not made by them.

— The CIoT device shall have a well-defined method for managing potentially conflicting commands.

9.3.6.2 Technical log safety requirements

The requirements are as follows:

— The CIoT device shall incorporate a technical CIoT device log that:

1) Shall capture detected technical errors such as connectivity disruptions, connectivity failures, etc.
2) Shall capture login attempts, both successful and unsuccessful.
3) Shall capture configuration changes.
4) May capture data streams.

— The manufacturer shall disclose the capacity/size of the technical CIoT device log.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

9.3.7 Security—Human factors requirements

The requirements are as follows:

- The CIoT device shall detect potential FW or SW compromises and notify the local user and other connected CIoT devices.
- The CIoT device shall notify connected CIoT devices of any SW and/or FW update failures.
- The CIoT device shall support Human intervention to control software and firmware updates.
- CIoT device shall communicate the need for SW and/or FW update to the user.
- CIoT device shall notify the user of any SW and/or FW update failures.
- The CIoT device shall support secure remote software and firmware updates.
- CIoT device shall update its FW/SW on user acknowledgement.
- The CIoT device should preserve critical functionality/primary operating functions of the CIoT device as justified by risk management in the presence of SECURITY controls.
- The CIoT device should support emergency override (“Break the Glass”) provisioning (i.e., safety considerations override SECURITY considerations in certain cases that are rare and exceptional by definition).

9.3.8 Interoperability—Human factors requirements

NOTE—The current version of the standard does not specifically address interoperability.

The requirements are as follows:

- A CIoT device shall communicate expiration date(s) to other CIoT devices.
- A CIoT device shall communicate battery status to connected CIoT devices.
- All CIoT devices should communicate known user disabling (visual, auditory, cognitive, mobility, etc.) conditions to Connected CIoT devices.
- The CIoT device shall communicate known user allergy and irritation issues, if available.
- The CIoT device shall alert the user if it has not been communicating with connected CIoT devices after a period determined by risk analysis.
- The CIoT device shall indicate the CIoT physical device change only after confirmation from the actual CIoT physical device.
- All CIoT devices should communicate user culture-based accommodations to connected CIoT devices.

9.3.9 Verification and validation—Human factors requirements

NOTE—This version of the standard does not specifically address verification and validation.

The requirements are as follows:

- The manufacturer shall evaluate the accompanying documentation (including training) from a usability perspective and validate that the information is:
  1) Perceivable by the intended users

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

2) Understandable by the intended users

3) Supports the intended user workflow

4) Supports correct use by the intended users.

— The deployment organization shall be able to validate proper CIoT device to CIoT device connectivity.

— The manufacturer shall execute the various summative validation activities as specified in the technical user interface plan.

10. Integrated systems design (ISD)

The integrated systems design (ISD) approach provides meaningful guidance for the design, development, and deployment of connected healthcare solutions that function and safeguard human interests. The delivered value from CIoT devices and systems has the greatest potential when CIoT-based solutions facilitate companies of all sizes and all types of stakeholders, including clinical/medical service providers, patients, and researchers, to leverage CIoT devices and integrated systems safely and securely through independent as well as collaborative efforts. The CIoT healthcare ecosystem can benefit from this standard to enable integrated, collaborative, and complex systems that can more easily address many diverse health disparities and serve many more patients with important clinical functions and services. This can potentially increase the positive impact on public health and individual health beyond what individual companies, services, or technologies can achieve alone while delivering high-quality and high-reliability services.

10.1 ISD attributes and characteristics requirements

There are some general attributes or characteristics that any interoperable CIoT system should possess from an ISD perspective. Namely, the design and system should be as follows:

— Extensible, to allow the addition of new technologies, devices, functions, analytical capabilities, connectivity, standards, etc.

— Scalable, to be capable of growth by increasing the number of connections, systems, devices, new patient populations, other stakeholders, geographic areas, etc.

— Transparent, enabling stakeholders, developers, users, and regulators to understand the system components, connections, interoperability, and device features, as well as roles and responsibilities of stakeholders, users or devices that organizations can provide approved access to for system devices and data. Please refer to Clause 4 (trust and identity), Clause 5 (privacy), and Clause 9 (human factors and usability).

— Modular, such that subsystems, devices, or information can be swapped out or recombined for maintenance, enhancements, upgrades, or growth. Please refer to Clause 4.

— Interpretable, such that authorized users and stakeholders can understand outcomes, recommendations, and elements of the system. Please refer to the Clause 9.

— Robust, such that it can withstand internal and external attacks and enable failsafe mechanisms. Please refer to Clause 7 and Clause 8.

— Adaptive, to be capable of integrating recent technologies, regulations, environmental considerations, new or different patients with different conditions, etc.

— Maintainable, to be capable of being supported by stakeholders and users so that the system can operate within appropriate operating tolerances with a minimum of service provider intervention.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

This includes updating and upgrading the system and its underlying software and hardware components to address operational and security findings that would otherwise impede operation.

Overall, integrated CIoT systems should be designed to address the TIPPSS attributes, along with human factors, usability, connectivity, data and device interoperability, reliability, dependability, stability, performance, and robustness. Since such devices operate in uncertain environments (in clinics, at home, in vehicles, away from home), the devices are required to perform with robustness and acceptable levels of risk.

As such, the CIoT system shall include software components to verify data is properly collected, sensors and actuators are properly functioning, and that data is securely transmitted or stored locally while maintaining privacy, either to its intended destination(s) in real-time or in the event of a system or communication failure, to be uploaded after connectivity establishment or re-establishment. A closed-loop approach to system and data interoperability, confidentiality, integrity, and availability creates a robust, dynamic, accessible, and highly functioning system.

10.2 Documentation requirements

Documentation requirements are as follows:

- The CIoT system manufacturer shall define and document the subject, purpose, and intended use of the CIoT system.
- The intended-use documentation shall contain information on users, the environment of use, off-label use, and use as described by regulations, authorities, and premarket testing processes for which the manufacturer has submitted the device, and for which it has received approval, if applicable. Manufacturers, systems, and service providers shall utilize the intended-use document to provide a reasonable and understandable description of intended use that matches needs, provides direction to each user group, and which also identifies any populations excluded from the test population(s).
- The CIoT system/device manufacturer shall update electromagnetic compatibility (EMC) and radio frequency (RF), as well as humidity and atmospheric conditions, information for the home user, if applicable, in the documentation.
- The intended-use documentation shall contain information on the device performance study protocol(s) for premarket testing and postmarket testing. This presented information can also include other data points:
- Study description that accounts for factors such as disease state, patient condition, physiological state, and medications that might affect device performance in the intended use population, or excluded population, for that device.
    1) Clearly described methods, processes, information flows, and training.
    2) Identification and study of patient subpopulations are necessary.
    3) Any inclusion/exclusion criteria related to the environment of use and specific end-user population(s).
    4) The identification of risks.
- Manufacturers shall provide an intended-use summary to end-users of the CIoT system that clearly specifies the device classification and certifications (medical device, home-healthcare medical device, consumer wellness, etc.), the approved environments of use (e.g., clinical, non-clinical), and the end-users included in device testing.
- The documentation shall specify the types and profiles, or scope of practice, of end-users expected to interact with the system.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The manufacturer shall identify the target user group(s) for each instruction guide/document/technical manual.

— If a medical professional prescribes a CIoT device for "off-label" use (i.e., not in agreement with the stated "intended use") the medical professional shall clearly explain to the patient/caregiver that the device's use is off-label and the medical professional should affix a GENERAL WARNING/NOTICE about off-label use to the device.

— The IFU shall clearly define and document the context, i.e., all physical locations where end-users will interact with the system, or environment, connectivity requirements, and data access in which stakeholders can or cannot deploy the system.

— The IFU shall clearly list and explain any technical limitations related to the context and/or user profiles.

— The CIoT system manufacturer shall compile and periodically maintain documentation describing various system requirements, test results, and verification and validation activities.

— The CIoT system manufacturer shall provide an IFU, which shall be available to the user.

— The CIoT system manufacturer shall make the IFU accessible on the web in one step with active links to other referred clauses in the document; not behind paywalls/subscriptions or nested in other documents making them inaccessible by reasonable and appropriate means. Manufacturers shall make available any references made in manufacturer documentation, websites, and supplemental materials to all users, regardless of subscriptions for the documents.

— The IFU shall describe all connections of the system and/or device(s) with external networks and/or devices, including the purpose of each connection and device.

1) If the system requires periodic maintenance, this shall be stated in the IFU along with maintenance instructions.

2) The CIoT system manufacturer shall publicly publish and maintain a vulnerability disclosure policy. (ISO/IEC 29147 [B32])

3) Manufacturers shall write language and explanations in documentation that is understandable to the home user, advocates, and caregivers.

4) Manufacturers should, whenever possible, generate all forms of documentation using pictures as well as alternative media, which may be a more understandable form of communication.

5) Manufacturers should check translated and/or interpreted documents for accuracy and language after translation by user groups who, following the translated documentation, access functions and features of the CIoT device or system.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

10.3 Research and development (R&D) and pre-production requirements

The requirements are as follows:

— The CIoT system manufacturer shall identify and define the target user group(s) and point of use for the CIoT system/device.

— The CIoT system manufacturer shall establish pre-defined thresholds for all critical data types to indicate expected normal system behavior.

— The CIoT system manufacturer shall establish and execute risk and hazard analysis, mitigations, and design considerations, including (but not limited to):

1) Assessment of residual risk and risk acceptance criteria.

2) A specific list of all considered risks in the design of the CIoT system.

Copyright © 2024 IEEE and ULSE. All rights reserved.

3) A specific list and justifications for all established risk controls for the CIoT system.

4) Traceability matrix linking actual risk controls to the risks.

5) Summary describing the plan for providing validated software updates and patches as needed throughout the CIoT device lifecycle.

6) IFU and product specifications related to recommended risk controls appropriate for the intended use environment.

7) A plan to protect PII and PHI.

8) A documented method for reconciling competing TIPPSS attributes based on a locally defined hierarchy.

— The CIoT system or device manufacturer shall provide clear and transparent information regarding any personal information, including all types of PII and PHI being used by the system, being stored, and/or processed by the CIoT system.

10.4 Postmarket requirements

— The CIoT system manufacturer shall establish and execute postmarket surveillance and evaluation.

— The CIoT system manufacturer shall record the following in a medical manufacturer device registry for each postmarket evaluation, as covered in Clause 4. Namely, record the following:

1) The number of devices

2) The time (in hours) that each device was in use since the last evaluation and since production,

3) The number and types of device malfunctions (if any)

4) The number and types of human injuries for each device since the last evaluation (e.g., could cause harm, did cause harm, caused moderate harm, caused severe harm, or caused death)

5) The number and type of when each device may have exceeded pre-established boundaries or thresholds

— The CIoT system manufacturer shall establish and execute risk and hazard analysis, mitigations, and design considerations after the initial usage of the system/devices.

— The CIoT system manufacturer shall periodically review the CIoT system and devices for security vulnerabilities.

11. CIoT reference architecture (RA)

The CIoT RA for ISD of a complex, integrated, interoperable system of systems adhering to TIPPSS in a connected healthcare context was developed considering several RAs from related fields. The Open Group Architecture Framework (TOGAF), S3 RA for business-driven service-oriented architecture (SOA), and Homecare Architecture for health smart homes laid the foundation.[23] Additional complementary factors/layers were included to address interoperability, TIPPSS attributes, healthcare information architectures, data-driven healthcare and system failure predictions, and international healthcare policies and regulations. The ArchiMate reference framework was used to develop the Minimum Viable Reference Architecture (MVRA) described herein.

The MVRA presents the requirements in alignment with the functional layers of a conceptual RA (see Figure 16) for CIoT with TIPPSS, comprised of five key layers, a services quality and integration/reconciliation of

[23] Rodriguez, Lina Maria Garcés. “A reference architecture of healthcare supportive home systems from a systems-of-systems perspective.” (2018). DOI: DOI:10.11606/T.55.2018.TDE-16102018-111654

Copyright © 2024 IEEE and ULSE. All rights reserved.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

TIPPSS (SQIRT) Layer, and two upper-level layers, namely the Information Architecture Layer and Governance & Policies Layer, that interact with all other layers of the MVRA.

The five key layers, some corresponding to similar layers in TOGAF Framework include the following:

— Context Layer

— Technology Layer

— Application Services Layer

— Healthcare Workflow Services (HWS) Layer

— End-User Services (EUS) Layer

Each of the five key layers addresses one or more interoperability designs (technical, semantic, syntactic, operational, regulatory), information architecture, or governance and policies requirements. The SQIRT layer manages all interoperability and data/device TIPPSS attributes to be achieved, reconciling conflicts between TIPPSS attributes and coordinating processes and communication between five key layers and the Information Architecture Layer and Governance & Policies Layer. Refer to Annex D for more details on the MVRA for CIoT with TIPPSS as well as a Hospital @Home use-case example.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

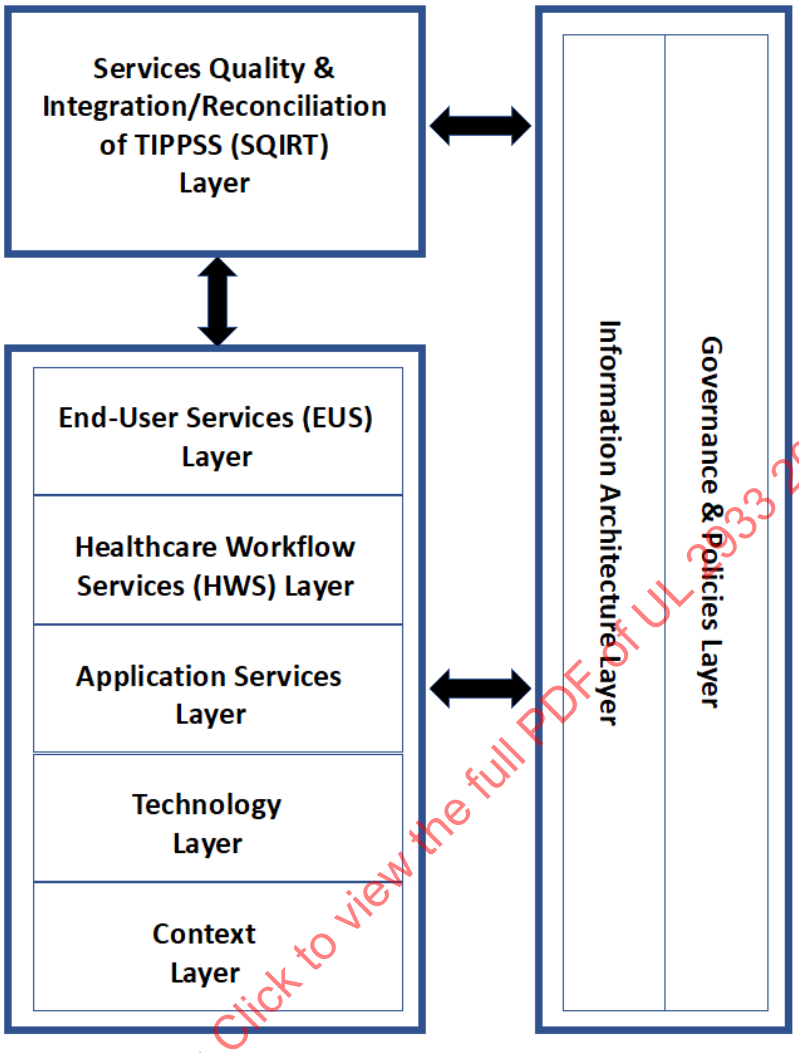

Figure 16—Conceptual view of a Minimum Viable Reference Architecture (MVRA) for integrated CIoT systems with TIPPSS

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Figure D.4 presents a functional view of the MVRA for a CIoT system with TIPPSS; it details the minimum functional requirements of components, devices, services, management servers, and information within each layer. See D.1 for more details on the components shown in the functional view. The requirements that follow directly align with the layers and the items depicted within each layer.

It should be noted that each of the five layers (EUS, HWS, Application Services, Technology, and Context) can be further decomposed into Interoperability Levels. The Interoperability Levels include the following:

- Technology interoperability
- Syntactic interoperability
- Semantic interoperability
- Organization interoperability
- Regulatory interoperability

Copyright © 2024 IEEE and ULSE. All rights reserved.

Each layer may include one or more of these levels, which is explained in the following subclauses. There is also additional information in Annex D.

11.1 Context Layer requirements

The Context Layer represents and describes where the system is intended to operate (environment, home, vehicle, hospital) and who may interact with the system (patient, caregiver, first responder, clinician, healthcare professional). It does not describe actual system implementation. The components of the Context Layer have direct contact with the sensors/devices and system(s) in the Technology Layer.

The Context Layer refers to all physical aspects of the system, other than the IoT device itself, including stakeholders (patient, caregiver, healthcare professionals), and the physical location environment (home, hospital, clinic, etc.). The stakeholders and end-users may change as the patient moves between various locations. At home, the caregiver and patient need to interact, or may need to intervene, with CIoT system operations. In contrast, at a medical facility, experienced medical professionals are expected to be available. The level of risk to the patient and system will also be a function of the location and stakeholders for each of the different TIPPSS attributes.

Figure 17 shows that the Context Layer only has a relationship with the Governance & Policies Layer. Refer to D.5 and Table D.1 for additional information.

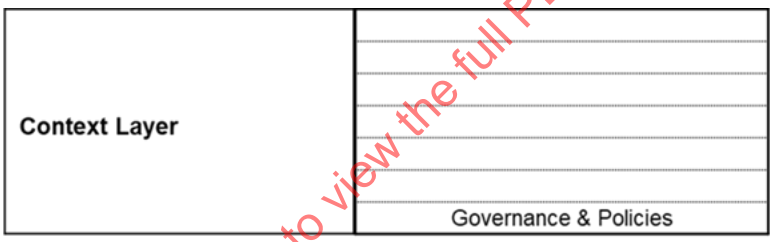

Figure 17—Context Layer relationships

Because the stakeholders and environment define the Context Layer, there are no specific normative requirements.

11.2 Technology Layer requirements

The Technology Layer includes physical and virtual CIoT devices and associated network devices.

CIoT physical devices (HW) refer to the following:

- Physical networking devices such as gateways, physical servers, mobile phones, tablets, and TVs.
- Other technical parts of the system, e.g., remote IoT server (e.g., including cloud), data processing (processor), physical network security device/security system, and device for data storage (hard drive).
- Technology infrastructure: Cellular, IEEE 802.11, broadband, cloud servers, network management, enterprise network services, etc.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

CIoT virtual devices (SW) refers to the following: technical software such as firmware, operating systems, device drivers, system services, networking services, application software, supporting software libraries containing functions, SaMD, and associated configurations.

The Technology Layer also includes third-party devices, which are addressed via interoperability.

Figure 18 shows that the Technology Layer only has a relationship with the Technical and Semantic Interoperability Levels as well as the Information Architecture and Governance & Policies Layers. Refer to Annex D and Table D.1 for additional information.

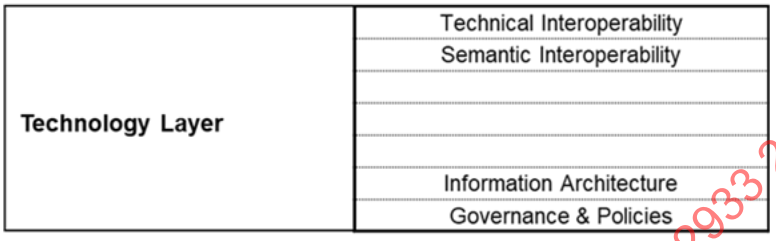

Figure 18—Technology Layer relationships

11.2.1 System software requirements

The system software requirements are as follows:

- All software components in the CIoT system, including device firmware, gateway software, and remote server software, shall have update capabilities. Bootloaders can be excluded from this requirement.
- A CIoT system software update shall have roll-back functionality, meaning that in case of update failure, the CIoT device(s) shall remain functional with its current software version.
- Each CIoT system software component in the CIoT system shall periodically, as described by best practices, manufacturers, security oversight, and or consistent with communications standards, at least within up to one-month intervals, check for available software versions, warnings, security notices, and/or updates.
- In case a potential system software update fails, the system shall log this failure along with the failure reason, date, and time.
- Once the CIoT system manufacturer discovers and reports a system software update failure, open communication shall be established with the deploying organization and shall provide a resolution (i.e., the release of a software update) within the terms of the agreement and in no longer than 90 days.

11.2.2 Technology Layer general requirements

The general requirements for the Technology Layer are as follows:

- The CIoT system manufacturer shall define all critical hardware (mechanical, electrical) and software features of the CIoT system and its components.
- The CIoT device or system SQIRT Manager shall hold and monitor critical system parameters required for proper system functionality.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The CIoT system components shall have a built-in test (BIT) of critical hardware and software features and parameters related to the CIoT system manufacturer, defining all critical hardware (mechanical, electrical) and software features of the CIoT system and its components.

— The CIoT system components shall alert the CIoT system SQIRT Manager of any pending degradation of function or performance.

— The CIoT system SQIRT Manager shall send an alert signal to appropriate operators and dependent system components of a critical mechanical device failure.

— The CIoT system SQIRT Manager shall send an alert signal to other system components of a critical electronic device failure.

— The CIoT system SQIRT Manager shall send an alert signal to other system components of a critical software component failure.

— The system shall monitor and record all single fault conditions (IEC 60601-1 [B13]).

— In case the system requires periodic maintenance, it shall record any occurrence of maintenance locally (if applicable) and on the remote server.

— The system should use an open communication protocol to allow the user to exchange devices from different manufacturers.

— In case a device tries to connect to the CIoT system but uses the wrong communication protocol, the SQIRT Manager shall alert other system components.

— The CIoT system should support geo-location reporting.

11.2.3 Requirements associated with CIoT system hardware and firmware

11.2.3.1 Default password requirements

All factory passwords shall be unique per device or have forced replacement by the user during first use.

All factory passwords should be generated using a mechanism that reduces the risk of automated attacks and be at least six characters long.

11.2.3.2 Medical device marking and labeling requirements

The requirements for medical device marking and labeling are as follows:

— Each device shall have a unique ID assigned by the CIoT system manufacturer.

— All device recordings, clinical, technical, and all others, stored on the remote server shall include the unique ID of the device.

— The manufacturer shall clearly mark each device with at least the following information:

1) CIoT system manufacturer name
2) Model/part number
3) Manufacturing date
4) Unique ID
5) Device classification

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The manufacturer can display the above information on the device UI, label, or any other visible means.

— CIoT system manufacturers shall define the classifications for their device(s) according to the classes and criticality applicable to localities of manufacture and/or usage and make this classification available online.

11.2.3.3 Personal data requirements

The requirements for personal data are as follows:

— Network devices or components shall spatiotemporally synchronize data collection from the CIoT devices that monitor the patient's status.

— Network device or component shall spatiotemporally synchronize data transmission between the CIoT devices that are monitoring the patient's status and other components within the system.

— Network device or component shall spatiotemporally synchronize the use of stored data from the CIoT devices that are monitoring the patient's status.

— The design of the CIoT system shall allow coupling a specific CIoT device to a specific user.

— The CIoT system shall collect PII and PHI only if required for clinical analysis and proper system functionality and labeled as such. The CIoT system shall not collect non-essential PII and PHI and notes them as not being available to the system.

— The CIoT device shall remove any PII or PHI once transmitted to the edge device conducting data fusion, forecasting, etc., and/or the remote server, unless required for local analytics, prediction, forecasting, etc., and/or proper device functionality.

— The remote server and the IoT gateway shall secure shared sensitive patient data, mitigating the risks of the threat of exposures like malware and ransomware attacks.

11.2.3.4 Remote server requirements

Remote server requirements are as follows:

— The CIoT system and the remote server shall cryptographically encrypt communications between each other.

— Each CIoT device shall use a unique encryption key.

— In the case of data communication loss between the CIoT device and the remote server, the device shall store critical data for up to 24 hours and upload it to the remote server upon communication restoration.

— In the case of loss of data communication between a CIoT device and a remote server, the remote server shall alert the user as well as other system components.

— Each CIoT device shall send its firmware and software versions to the remote server at least once per communication session.

11.3 Application Services Layer requirements

The Application Services Layer includes application services that support the goals of the EUS Layer, the Healthcare Workflow Services (HWS) Layer, and the applications that realize them.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

The Application Services Layer provides services to patients, caregivers, and service providers, and provides information about patients and their environment.

This layer contains all services related to the medical software part of CIoT, including healthcare software, SaMD, Software in a Medical Device (SiMD), and AI/ML.

This layer contains all services and higher-level software associated with the purpose of the device, as provided by the physical IoT devices, sensors, gateways, servers, etc.

The Application Services Layer refers to all application services that process raw data and output clinical and other parameters, such as patient SpO2 level, body temperature, insulin level, blood pressure, etc.

Application services examples are as follows: Patient SpO2 Levels, Patient Body Temp, Patient Insulin Level, Patient BP.

Figure 19 shows that the Application Services Layer only has relationships with the Technical, Semantic, and Syntactic Interoperability Levels as well as the Information Architecture and Governance & Policies Layers. Refer to Annex D and Table D.1 for additional information.

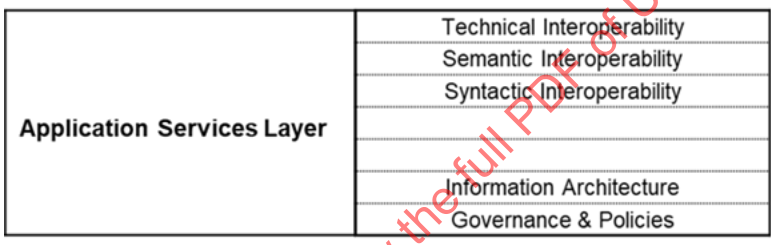

Figure 19—Application Services Layer relationships

In case the CIoT system relies on pre-defined data sets for its operation, the datasets shall employ traceable information.

11.4 Healthcare Workflow Services (HWS) Layer requirements

The Healthcare Workflow Services (HWS) Layer is responsible for capturing and communicating patient status through signs and symptoms monitors.

This may include applied clinical services once patient clinical data is available from the Application Services Layer. For example, once a certain parameter is above/below its pre-defined threshold, services in the Healthcare Workflow Services (HWS) Layer may trigger a notification to the healthcare team to provide treatment to the patient.

Services in this layer represent macro-flow activities required to bring healthcare to the required level and quality of services to a patient (e.g., activities provided by the healthcare team, whether local or remote, including through telehealth) and to provide communications, security, and functionality to enable service providers to access resources, information, and permissions needed to view, change, interoperate, interact with systems, and communicate to successfully manage a patient's condition, consistent with applicable data privacy requirements.

Services in this layer could make use of AI/ML algorithms to identify abnormalities in the patient's health status.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— *Healthcare Workflow Service:* Patient Status and Signs and Symptoms Monitor

— *Patient Status and Sign and Symptoms Monitor:* Its aim is to establish patient physical status (including the use of AI/ML algorithms), through a physical or virtual patient examination, and monitor their signs and symptoms, demographics, transcriptions, and patient-provided information.

Figure 20 shows that the Healthcare Workflow Services Layer has relationships with all layers except for the Technical Interoperability Level. Refer to Annex D and Table D.1 for additional information.

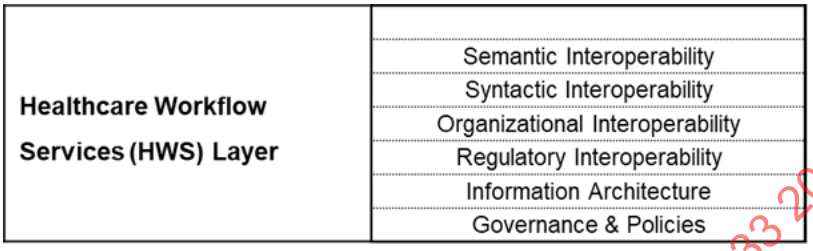

Figure 20—HWS Layer relationships

CIoT healthcare workflow services shall provide access to the patient's personal data that was collected since the time the system added the device.

11.5 End-User Services (EUS) Layer requirements

Services in the EUS Layer intend to achieve the requirements of end-users who directly interact with the entire CIoT system, including home healthcare teams, healthcare providers and organizations, human IT system managers, etc.

The EUS Layer includes all types of user applications for patients, caregivers, physicians, etc., including interfaces to third-party systems and applications such as EMRs and health organization records. Applications can include web and mobile applications, as well as other types of user interface (UI)-based services.

Figure 21 shows that the EUS Layer only has a relationship with the Syntactic and Organizational Interoperability Levels as well as the Information Architecture and Governance & Policies Layers. Refer to Annex D and Table D.1 for additional information.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

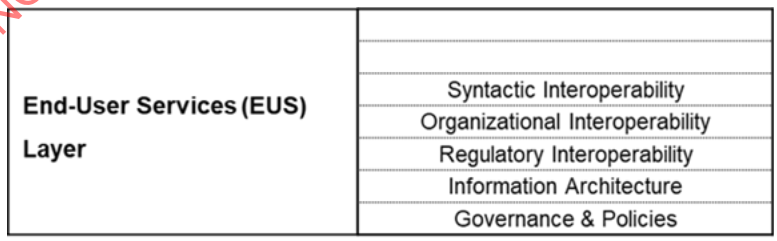

Figure 21—EUS Layer relationships

The EUS Layer contains four service categories: patient, home healthcare team, healthcare provider, and EUS Manager. Refer to Figure D.4.

Copyright © 2024 IEEE and ULSE. All rights reserved.

11.5.1 Patient

Services for the patient include access to all EMR, PHI, etc., and associated data and reports, secure communication with healthcare providers for purposes of transferring images (photos, video), documents, prescriptions, etc., and for telehealth purposes, control of CIoT system devices and monitoring/alerting features, among others.

11.5.2 Home healthcare team

Services for the home healthcare team (family member or other home healthcare provider) handle interactions with other end-users such as professional and non-professional caregivers (see Figure D.6.

The EUS Manager enables the home healthcare team to provide or deny access to other end-users for the following services:

- Information
- Transaction negotiation: financial, insurance, and related information
- Hardware
- Software
- Service features and functions
- Provision and manage professional and consumer devices
- Schedulers
- Interoperability of all components, including home networking equipment and features

11.5.3 Healthcare provider

The services for healthcare providers, which may be individuals and/or organizations, offer functionalities required in emergency situations. For example, these services often recommend clinicians as backup to take over services provided by architecture for accessing and recording information in health records and managing healthcare plans.

Services contained in this layer allow CIoT systems to be part of a broader e-Health ecosystem.

11.5.4 End User Services (EUS) Manager

EUS is concerned with the user interface (UI) or forward-facing interfaces/interactions that an end-user can have. This includes patient and medical professionals (GUI) all the way to the IT professionals (override decisions, write code/new apps, improvements, updates, security patches, etc.), as well as payers and regulatory [review medical/clinical coding (e.g., ICD codes), logging reports of adverse events, incidents, postmarket surveillance data, etc.]

The EUS Manager offers capabilities to manage configurations (interactions) and modifications of services (applications) allocated in the SQIRT Layer, Information Architecture Layer, and Governance & Policies Layer. It also monitors, assesses, and reports on the quality of the end-user services.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

11.5.4.1 End-User Services (EUS) Manager requirements

- The CIoT system manufacturer shall provide access to training materials to enable all people involved with the system to perform their assigned functions. This includes contact websites, phone numbers, etc. to get further information without having to pay for access and/or information especially any information referenced in device related information, documents, FDA filings, studies, reports, user guides, etc.
- The CIoT system, acting in this case as an EUS Manager, shall spatiotemporally synchronize data collection from the CIoT devices that are monitoring the patient's status.
- The CIoT system, acting in this case as an EUS Manager, shall spatiotemporally synchronize data transmission from the CIoT devices that are monitoring the patient's status and other components within the system.
- The CIoT system, acting in this case as an EUS Manager, shall spatiotemporally synchronize data storage from the CIoT devices that are monitoring the patient's status.
- The CIoT system, acting in this case as an EUS Manager, shall make the patient's personal healthcare data collected available for authenticated end-users upon request.
- The CIoT system, acting in this case as an EUS Manager, shall alert stakeholders of mechanical device failure.
- The CIoT system, acting in this case as an EUS Manager, shall alert stakeholders of software device failure and execute failsafe functions to help safeguard patients' data, including PII and PHI.
- The CIoT system, acting in this case as an EUS Manager, shall alert other system components of mechanical device failure.
- The CIoT system, acting in this case as an EUS Manager, shall alert other system components of an electronic device failure.
- The CIoT system, acting in this case as an EUS Manager, shall alert other system components of software device failure.
- The CIoT system, acting in this case as an EUS Manager, shall verify that the CIoT device is located on the patient, near the patient, or remote from the patient and is consistent with the defined context.
- The CIoT system, acting in this case as an (EUS Manager, should log and monitor technical details of all CIoT system devices, components/elements to identify the system within the context (location) of normal use. This is so the various system functions can identify and properly address any movement or new location.
- If the device location is not consistent with the defined context, then the CIoT system, acting in this case as an EUS Manager, shall comply with the following:
  1) Log information related to patient and device locations, and actions to occur.
  2) Flag the data for future analysis and determination of whether the data is valid.
  3) Send an alert(s) to the patient, healthcare provider, and system operator to request confirmation that the device is still with the patient, device compromise did not occur, and remove the "flag" for subsequent data collection.
- The CIoT system, acting in this case as an EUS Manager, shall verify that data stored on the device, near the device, or on the remote server is consistent with expected values and not corrupted.
- If the data structure in a particular location is not consistent with the defined context for that location, then the CIoT system, acting in this case as an EUS Manager, shall comply with the following:
  1) Log information related to each data location and actions to occur, e.g., data is out of bounds for all storage locations, or data becomes corrupted between any two data storage locations, or

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

one data point indicates it is necessary to analyze multiple data points to infer the status of the patient.

2) Flag the data for future analysis and determination of whether the data is valid.

3) Send an alert(s) to the patient, healthcare provider, and system operator to request confirmation that the device is still with the patient, device compromise did not occur, and remove the “flag” for subsequent data collection.

— The CIoT system, acting in this case as an EUS Manager, shall monitor the data transfer to its final storage location and send an alert to the patient, healthcare provider, and system operator if the amount and structure of the data have changed or transfer interruption occurred.

— The user interface shall provide means for the user to adjust alert thresholds and to set escalations to engage additional processes and/or staff.

— Even in the case that the device was not provided patient information, the CIoT system shall support limited or full operation.

— The CIoT system shall support alerts for blind and hearing-impaired users.

— The CIoT system, acting in this case as an EUS Manager, shall provide means for the user and/or system administrator to modify the authentication value.

— Upon first user login, the CIoT system, acting in this case as EUS Manager, shall force the user to change their password.

— In case a user activated a command via the system UI, the UI shall display a confirmation message notifying the user of successful or failed command execution.

11.5.4.2 End-User Services requirements

An end-user refers to the patient, the home healthcare team, and the healthcare provider, and the associated service categories depicted in Figure D.1.

— The manufacturer shall enable the deployment organization, end-users, etc. with the ability to approve software updates prior to installation as appropriate.

— All end-users should have secure access to a CIoT integrated system communication portal for the transfer of personal documents, reports, prescriptions, and other documents containing sensitive personal health information and replies compliant with contracts and regulations during business hours of the patient and provider location.

— Once an event triggers an alert, it shall stay active until manually acknowledged by a user (latching alert).

— The SQIRT Manager shall alert end-users of the pending failure of a non-critical component.

— The CIoT system shall have redundancy to avoid a single point of failure, or single fault condition that enables notification to the end-user. In a single point of failure there is a record of the failure.

— In case the CIoT system periodic maintenance of the physical CIoT devices and components/elements did not occur on time, the system shall notify the end-users accordingly and stop CIoT system operation.

— In case the CIoT system periodic software updates did not occur on time, the system shall notify the end users, and if the updates still have not been initiated within 1 week, the end-users are notified that the system is going offline, and a data store and forward functionality shall begin.

— In the case that a software update modifies basic system functionality, the system should inform the user accordingly.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— The manufacturer shall make the personal information gathered by the devices available to the patient, or other authenticated end-users on-demand in a digital form. See 11.6.4 regarding personal information.

— The CIoT system manufacturer shall obtain user consent for any personal data mentioned in the requirements of 11.6.4.

— The CIoT system manufacturer shall provide means for the user to withdraw their consent for personal data use at any time.

— The CIoT system, acting in this case as an EUS Manager, shall authenticate the user and make sure that the system is able to access only authorized system content and data.

— The CIoT system should allow high-privileged users (i.e., administrators) to remotely lock devices and/or wipe their data.

11.6 Services quality and integration/reconciliation of TIPPSS (SQIRT) Layer requirements

The SQIRT function of a CIoT system with TIPPSS is concerned with how the data gets to where it needs to be for end-users to use the data; what systems devices/components/elements with which the data is shared, or devices/components/elements where data is not to be shared; and whether and how the data is verifiable to be correct, and the resolution of the data sampling is specified for functions of the system and elements. This also includes the actual CIoT system configuration and whether the CIoT system is scalable, reconfigurable, allows the addition of new devices, etc. The IT professional responsible for the CIoT system shall verify the SQIRT function of the CIoT system is effectively overseeing all manager operations and system changes.

SQIRT functions include the following:

— Overseeing the integration and interoperability activities and services of the CIoT System.

— Capturing, monitoring, logging, and alerting noncompliance with non-functional requirements (i.e., TIPPSS) that relate to the service qualities.

— Observing the Healthcare Workflow and EUS Layers, and the interoperability (mediation) operational design requirements and emitting events when it detects or anticipates noncompliance of TIPPSS attributes.

— Resolving conflicting requirements between multiple TIPPSS attributes to help ensure the best possible compromise of services related to TIPPSS.

The goal is to help ensure the CIoT systems, devices, and components/elements meet their TIPPSS requirements.

Thus, the aim of the SQIRT Layer is to help ensure the CIoT systems, devices, and components/elements meet their non-functional requirements (TIPPSS).

To meet the SQIRT requirements, the Technology Services/Managers: the SQIRT Manager, the Availability Manager, and the TIPPSS Managers have been identified, one for each of the six TIPPSS attributes.

11.6.1 SQIRT Manager requirements

The SQIRT Manager coordinates with the other seven managers (Availability Manager and six TIPPSS Managers) and integrates the repositories of information from the Information Architecture Layer and the Governance & Policies Layer into system processes. It coordinates and allows the transfer of information

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

between the EUS Manager and the Information Architecture Layer and the Governance & Policies Layer. It brings in all system logs; applicable integration, interoperability, TIPPSS policies and plans, interoperation standards, and healthcare plans. The SQIRT Manager also helps ensure that the TIPPSS attributes are adhered to and can reconcile any conflicting TIPPSS attributes.

— The SQIRT Manager shall determine if an existing system can include a new device in an existing system and notify the relevant TIPPSS Managers that the new device is now part of the CIoT system.

— The SQIRT Manager shall make sure that each device is associated with a unique user and notify the EUS of the device-user relationships.

— The SQIRT Manager shall determine whether multiple devices share data, and track and report the interoperability relationships between different CIoT system devices and components/elements.

— The SQIRT Manager shall determine how multiple devices share data, and track and report the specific data types shared between different CIoT system devices and components/elements.

— The SQIRT Manager shall determine and implement proper data conversions for data sharing between different CIoT system devices and components/elements.

— The SQIRT Manager shall manage and log all software updates.

— The SQIRT Manager shall manage and log all software version numbers.

— The SQIRT Manager shall provide for (backward) compatibility.

— The SQIRT Manager shall provide a mechanism for an end-user to opt out of data collection.

— The SQIRT Manager shall notify the CIoT system manufacturer at specific intervals, up to 1-year in length, that a postmarket evaluation of the device is necessary.

— The SQIRT Manager shall notify the relevant end-users when patient data is out of boundaries or thresholds.

— The SQIRT Manager shall notify the CIoT system/device manufacturer when any critical data type is out of boundaries or thresholds. See O.3 and H.3 for examples of critical data types.

— Then the CIoT system/device manufacturer shall investigate the reason for the critical data type out-of-bounds readings.

— The SQIRT Manager shall check compatibility between multiple (CIoT, network, other) devices.

— The SQIRT Manager shall check compatibility between multiple (CIoT, network, other) inputs.

— The SQIRT Manager shall check compatibility between multiple (CIoT, network, other) servers.

11.6.2 Availability Manager requirements

The Availability Manager observes the current state of all subsystems, devices, and components/elements of the CIoT system to whether an entity (part) of the system is online and ready when needed for a process or service. It notifies the relevant system managers to take appropriate action and notifies all end-users of a potential system breakdown. This may make use of AI/ML strategies to infer the unavailability or impending failure of a system entity (part) or overall system degradation.

— Network device or component shall periodically check connectivity to other devices (if applicable) and the remote server.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

11.6.3 TIPPSS Managers

The TIPPSS Managers are lower-level managers within the SQIRT Layer that do most of the lower-level monitoring and control, and report to the SQIRT Manager. The SQIRT Manager tells the TIPPSS Managers what to do and what actions to take.

11.6.3.1 Trust Manager requirements

The Trust Manager monitors and controls the CIoT devices and components/elements for all requirements related to trustworthiness of the CIoT system.

11.6.3.2 Identity Manager requirements

The Identity Manager monitors and controls the CIoT devices and components/elements for all requirements related to their unique identification and authentication and related processes. It also monitors and authenticates all end-users of the CIoT system.

— The Identity Manager shall verify the authenticity and integrity of each software update prior to installation.

— Authentication mechanisms used to authenticate users against a device should use best practice technology.

11.6.4 Privacy Manager requirements

The PM monitors and controls the CIoT devices and components/elements for all requirements related to maintaining privacy of patient personal and sensitive information and data, and related processes.

— The PM shall provide clear and transparent information regarding any personal information, including all types of PII and PHI used, stored, and/or processed by one or more devices and components/elements of the CIoT system. Consider compliance with the privacy laws of appropriate localities. Examples include the HIPAA Privacy Rule, PIPEDA, GDPR, or ISO/IEC 27701 [B30].

11.6.5 Protection and Safety Manager requirements

The Protection and Safety Manager monitors and controls all safety related requirements and processes for protection of the patient, the CIoT devices and components/elements, and the environment.

— The Safety Manager shall alert the SQIRT Manager of pending failures of a critical component.

11.6.6 Security Manager requirements

The Security Manager monitors and controls all security related requirements and processes to assist in the prevention and/or mitigation of internal or external threats to the CIoT system and end-users. The security manager comprises the current day SIEM service manager (at the time of initial publication): The SIEM service manager analyzes and manages events to security properties. SIEM service is related to the quality and security of the entire CIoT system. In the event of a breach of security anywhere in the system, the SIEM shall quickly notify the SQIRT Manager about the breach, which in turn notifies the other affected TIPPSS Managers and directs each manager to act based on the information from the Governance & Policies Layer related to TIPPSS plans. The notification shall be sent to all end-users so that appropriate actions can take place (e.g., one or more components may need to be isolated, or the entire system may need to go offline),

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

and send alerts to all CIoT managers (SQIRT, EUS, Application Configuration, etc.) for each manager to initiate corrective actions. A SIEM service manager should minimally detect and mitigate any well-known security vulnerabilities such as Denial of Service (DoS), and follow the pre-determined protocols to manage these attacks.

- Manufacturers shall utilize best practice technology to deter well-known outside security breaches at the time of the system's design and throughout the device lifecycle. See 10.3 and H.3 related to R&D and pre-production requirements, which detail what the CIoT system manufacturer shall establish and execute related to risk and hazard analysis, mitigations and design consideration, and the postmarket requirements in 10.4 and H.4.
- The CIoT system should introduce a single authentication system or means to use various systems via federated access (FA).
- The CIoT system shall use data encryption at rest and in transit. Specifically, the system shall encrypt or hash sensitive data, such as PII and PHI, using methods defined in the Protection, Safety, and Security clauses.
- The IoT device shall have a limitation on the number of authentication attempts within a certain time interval. Once the limit has been reached, the device shall not accept authentication for at least 30 min.

11.7 Information Architecture Layer requirements

The Information Architecture Layer guides all data operations and interoperability.

It contains structured knowledge, represented as repositories/ontologies, offering "intelligence" to CIoT devices and/or systems to achieve their goals.

The Information Architecture Layer impacts the whole CIoT system. All CIoT system layers also impact it.

- *Data Objects:* Other relevant standards, e.g., SNOMED-CT, LOINC, ISO/IEC/IEEE 11073-10201 [B34], ISO/IEEE 11073-10207 [B36], ISO/IEEE 11073-20601 [B37].
- *Transformation Rules:* It provides transformation rules between technical protocols and semantic standards. Its brokers use these rules to allow the transformation of messages for interoperable purposes.

Information Architecture requirements are as follows:

- Data communicated in CIoT systems shall use open standards-based nomenclature and information models such as ISO/IEC/IEEE 11073-10201 [B34], ISO/IEEE 11073-10207 [B36], etc.

11.8 Governance & Policies (G & P) Layer requirements

The Governance & Policies Layer includes standards, policies, guidelines, etc. for data and device verification and validation, interoperability, trust, identity, privacy, protection, safety, and security (TIPPSS).

This layer covers all aspects of managing the CIoT devices and systems operations lifecycle.

It provides guidance and policies for managing service-level agreements, including performance, security, and monitoring.

This layer interacts with all other layers of the reference architecture, so it encompasses the entire 3D RA.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Therefore, this layer applies to all other layers of the reference architecture. Specifically, this layer contains quality plans, reconfiguration plans, repositories of missions, services and contract specifications, and system logs.

The CIoT System EUS Manager located in the End-User Services Layer utilizes and modifies the information contained in this layer.

— *G & P Data Objects:* Trust Plans, Identity Plans, Privacy Plans, Protection Plans, Safety Plans, Security Plans, Interoperability Plans, and Integration Plans

— *G & P System Logs:* Records all systems operation for audit purposes (a Trust/non-repudiation tactic)

11.8.1 Requirements associated with interoperability and integration plans

The requirements are as follows:

— Network device or component shall recheck compatibility between all CIoT devices with each device software upgrade.

— Network device or component shall recheck compatibility between all CIoT devices with each device firmware upgrade.

— Network device or component shall recheck compatibility between all CIoT devices after device replacement.

— Network device or component shall recheck compatibility between all CIoT devices after a new device is introduced to the system.

11.8.2 Requirements associated with TIPPSS policies and plans

The requirements are as follows:

— CIoT should consider the individual features of the TIPPSS architectural framework set to determine the overall system configuration that satisfies all mandatory (shall) and as many desirable (should) elements of the standard as possible while maintaining TIPPSS and interoperability.

11.8.3 Requirements associated with system logs

The requirements associated with system logs are as follows:

— The system shall store log files of all critical actions and events, along with the date and time.

— The system should store log files of all data and information exchanged between the remote server and CIoT devices, along with the date and time.

— The system shall store security log files of all security-related events, along with the date and time.

— The system shall store critical and security log files for at least 7 years, or until the system or user exports them to external storage.

— The system shall store any PII and PHI in log files that are cryptographically encrypted.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

11.9 Lifecycle design and management

In general, a complete view of the device lifecycle includes four distinct sub-cycles aligned via certain defined interaction points, as depicted in Figure 22. However, it is important to understand that these sub-cycles "spin" at different speeds, each within its own scope and encompassing different processes not necessarily directly intertwined with other sub-cycles. For example, the device manufacturer lifecycle typically applies to an entire product line or version, whereas the healthcare operator/provider device lifecycle (in the healthcare organization) is typically per the individual physical device.

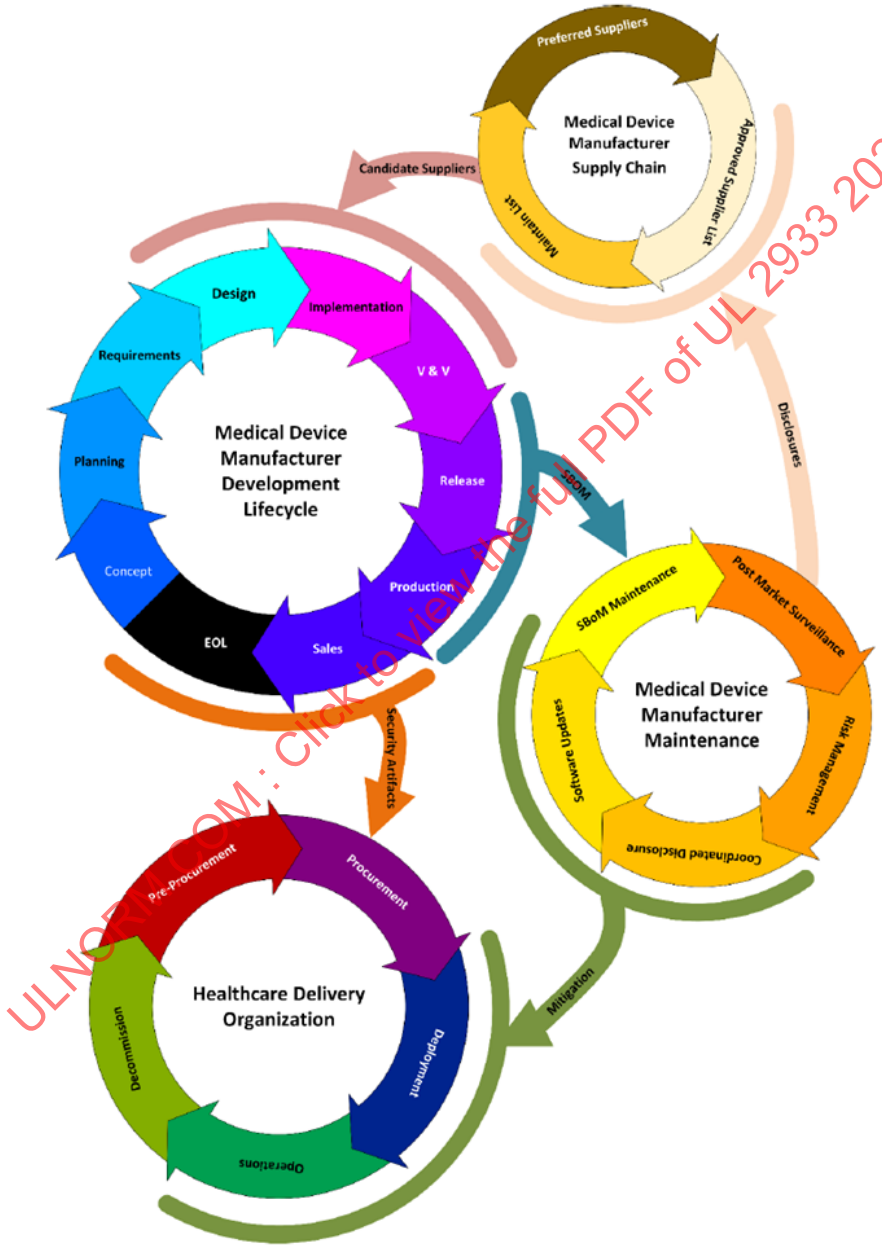

Figure 22—TIPPSS device lifecycle[24]

[24] Figure reprinted with permission from Health-ISAC, "Medical Device Cybersecurity Lifecycle Management" whitepaper (https://hisac.org/medical-device-cybersecurity-lifecycle-management/), ©2020.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

These subsets of the device lifecycle are applicable to general development practices, and shall apply as a best practice to realize the defined TIPPSS principles as follows:

11.9.1 CIoT device manufacturer lifecycle

During the respective lifecycle phases the device manufacturer shall perform the following activities regarding the TIPPSS principles:

- Concept phase: Identify target markets; assess risks; identify regulatory strategy; establish high-level TIPPSS considerations.
- Planning phase: Define TIPPSS-specific performance activities; identify roles and responsibilities; define high-level TIPPSS goals and requirements.
- Requirement phase: Define TIPPSS strategy and requirements; determine desired outcomes of TIPPSS activities.
- Design and architecture phase: Identify assets and vulnerabilities; perform detailed and TIPPSS-specific risk assessment; determine how to remediate and mitigate identified risks.
- Implementation phase: Follow software engineering and TIPPSS best practices; integrate and test supply chain components; perform TIPPSS assessments and testing throughout the phase.
- Verification and Validation (V&V) phase: Determine product compliance with TIPPSS principles through V&V activities; demonstrate and document meeting of TIPPSS requirements.
- Release phase: Obtain market approval with regulators as needed; transfer to production; release for sale.
- Maintenance phase: Manage newly identified TIPPSS-related risks; remediate and mitigate as required; establish continual postmarket surveillance and management.
- EOL phase: Communicate with customers; provide final software updates; engage with customers on risk transfer if required; transfer licenses to customer.

11.9.2 CIoT device supply chain management

To reduce and manage security risks because of the software supply chain, TIPPSS manufacturers shall perform the following activities:

- Establish preferred suppliers list: Contractually agreed security practices verifiable through evidence and audits; established vulnerability, incident, and breach notification processes; secure development and design practices; providing of security documentation, including SBOMs and sub-dependencies; secure production and distribution.
- Manage approved supplier list: Continual supplier management and input to future purchasing decisions, closed loop response to vulnerabilities, incidents, and breaches.
- Maintain supplier list: Audits; postmarket surveillance; monitor for timely response to vulnerabilities, incidents, and breaches; monitor suppliers' compliance with defined security requirements.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

11.9.3 CIoT device maintenance lifecycle

The manufacturer shall provide the following so that the deployment organization can maintain the device security over its useful life as follows:

- Postmarket surveillance: Collect and monitor cybersecurity signals; perform postmarket vulnerability surveillance; collect threat intelligence and vulnerability information; communicate to customers in a timely fashion.
- Vulnerability management and incident response: Assess risk when the manufacturer identifies a new cybersecurity signal, assesses impact, and determines risk treatment.
- Engage in coordinated disclosure process: Reporting of newly discovered. cybersecurity issues (threats, vulnerabilities, design weaknesses, security events and incidents, breaches, etc.); engage with reporters (e.g., security researchers); if needed, collaborate with government agencies.
- Mitigation: Provide patching and software updates or other remediation as determined appropriate.
- SBOM maintenance and monitoring: Maintain software composition information via SBOM; maintain up-to-date third-party software list; assess the severity of cybersecurity vulnerability [e.g., via Common Vulnerability Scoring System (CVSS) score].

11.9.4 CIoT device deployment organization lifecycle

Typical lifecycle phases for the role of a TIPPSS deployment organization (such as a healthcare provider/healthcare delivery organization) are as follows:

- Pre-Procurement:
  1) Shall establish security governance
  2) Shall develop risk management process and establish risk criteria
  3) Shall define roles and responsibilities
  4) Shall define device and security scope
  5) Shall establish budgets, staffing, and training
  6) Shall identify key processes, documentation, and tools
  7) Shall establish TIPPSS-aware replacement planning processes
- Procurement:
  1) Shall define TIPPSS requirements
  2) Select vendors and devices
  3) Shall perform initial risk assessment; shall establish contract terms
- Pre-Deployment:
  1) Shall record devices in asset management systems and inventory
  2) Shall perform initial network and identity configurations
  3) Shall update device firmware and software
  4) Shall update digital certificates
- Deployment:
  1) Shall conduct pre-deployment testing—installation, configuration, and integration

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

2) Shall conduct and log user and operator training

— Operation:

1) Shall include, update, and track devices in inventory, risk, and security management systems
2) Shall monitor operational performance criteria
3) Shall perform regular maintenance activities
4) Shall deploy mitigations, updates, and patches
5) Shall manage change and maintain approved configuration
6) Shall monitor for and manage security incidents, and report as needed

— Decommissioning:

1) Shall sanitize and remove any sensitive data (user, customer, PII, credentials, accounts, etc.)
2) Should remove parts for the purpose of servicing other devices

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Annex A

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] 45 CFR Part 164—Security and Privacy, https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164?toc=1.

[B2] AAMI TIR57:2016 (R2023), Principles for medical device security—Risk management.[25]

[B3] ANSI/AAMI/UL 2800-1:2022, Standard for Medical Device Interoperability, includes requirements for human factors analysis with a specific focus on interoperability.

[B4] ANSI/NEMA HN 1-2019, Manufacturer Disclosure Statement for Medical Device Security.

[B5] California Consumer Privacy Act (CCPA), 2018, https://oag.ca.gov/privacy/ccpa.

[B6] Decentralized Identifiers (DIDs) V1.0, https://www.w3.org/TR/did-core/.

[B7] Gellman, Robert, *Fair Information Practices: A Basic History*. Version 2.30, April 9, 2024.

[B8] General Data Protection Regulations (GDPR), 2016, https://gdpr-info.eu/.

[B9] Hartzog, Woodrow, *Privacy Blueprint—The Battle to Control the Design of New Technologies.* Harvard University Press, 2018.

[B10] H-ISAC, Medical Device Cybersecurity Lifecycle Management, Oct. 2019, https://h-isac.org/medical-device-cybersecurity-lifecycle-management/.

[B11] IETF RFC 8995, Bootstrapping Remote Secure Key Infrastructure (BRSKI).

[B12] IEC 60449-2:2004, Sound system equipment—Part 2: Measurement methods of electro acoustical characteristics of professional loudspeakers for general purpose.

[B13] IEC 60601-1, Medical electrical equipment—Part 1: General requirements for basic safety and essential performance.

[B14] IEC 62366-1:2015 Medical devices—Part 1: Application of usability engineering to medical devices.

[B15] IEC 62443-1:2009, Industrial communication networks—Network and system security—Part 1: Terminology, concepts, and models.

[B16] IEC/TR 80001-2-2, Application of risk management for IT-networks incorporating medical devices—Part 2-2: Guidance for the communication of medical device security needs, risks and controls.

[B17] IEEE Std 802.1AR-2018, IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity.

[B18] International Certificate of Origin Guidelines—Facilitating trade through global origin procedures | ICC Knowledge 2 Go.

[B19] IPC-1782, Standard for Manufacturing and Supply Chain Traceability of Electronic Products.

[B20] ISO 14971:2019, Medical devices—Application of risk management to medical devices.

[25] This Association for the Advancement of Medical Instrumentation technical information report is available from ANSI at https://webstore.ansi.org/standards/.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

[B21] ISO/TR 24971:2020, Medical devices—Guidance on the Application of ISO 14971.

[B22] ISO 81001-1:2021, Health software and health IT systems safety, security, and effectiveness—Part 1: Fundamental concepts, principles and requirements.

[B23] ISO/IEC 17788:2014, Information technology—Metadata registry (MDR)—Part 1: Framework.

[B24] ISO/IEC 19678:2015, Information technology—BIOS Protection Guidelines.

[B25] ISO/IEC 19790:2012, Information technology—Open Systems Interconnection—Security frameworks for open systems: Threats, vulnerabilities and controls.

[B26] ISO/IEC 20547-3:2020, Information technology—Learning, education and training—Quality, sustainability, social responsibility and interoperability—Part 3: Competency guidelines for digital competence.

[B27] ISO/IEC 20924:2021, Information technology—Cloud computing—Interoperability and data protection for data and application portability.

[B28] ISO/IEC 24759:2014, Information technology—Open Systems Interconnection—Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the ASN.1 object identifier tree.

[B29] ISO/IEC 27032, Information technology—Security techniques—Guidelines for cybersecurity.

[B30] ISO/IEC 27701, Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines.

[B31] ISO/IEC 29100:2011, Information technology—Security techniques—Privacy framework. [26]

[B32] ISO/IEC 29147, Information technology—Security techniques—Vulnerability disclosure.

[B33] ISO/IEC 30111, Information technology—Security techniques—Vulnerability handling processes.

[B34] ISO/IEC/IEEE 11073-10201, International Standard—Health informatics—Device interoperability—Part 10201: Point-of-care medical device communication—Domain information model.

[B35] ISO/IEEE 11073-10101, Health informatics—Device interoperability—Part 10101: Point-of-care medical device communication—Nomenclature.

[B36] ISO/IEEE 11073-10207, Health informatics—Personal health device communication—Part 10207: Domain information and service model for service-oriented point-of-care medical device communication.

[B37] ISO/IEEE 11073-20601, Health informatics—Device interoperability—Part 20601: Personal health device communication—Application profile—Optimized exchange protocol.

[B38] Joseph, J. and S. Madhukumar, A Novel Approach to Data Driven Preventive Maintenance Scheduling of medical instruments. 2010. DOI: 10.1109/ICSMB.2010.5735370

[B39] NIST SP 800-53-5, Security and Privacy Controls for Information Systems and Organizations.

[B40] NIST SP 800-57, Part 1 Rev. 5, Recommendation for Key Management: Part 1—General.

[B41] NIST SP 800-63-3, Digital Identity Guidelines.

[B42] NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.

[B43] NIST SP 800-130, A Framework for Designing Cryptographic Key Management Systems.

[B44] NIST SP 800-131A Rev.2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

[B45] NIST SP 800-193, Platform Firmware Resiliency Guidelines.

[B46] NIST SP 800-207, Zero Trust Architecture.

[26] All 11073 documents are available from the Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

[B47] NIST SP 800-1800-16, Guideline for Identifying and Managing IoT Cybersecurity Risks.

[B48] OECD Member countries, "Our global reach—OECD," https://www.oecd.org/about/members-and-partners/.

[B49] Office of the Privacy Commissioner of Canada, PIPEDA requirements in brief.[27]

[B50] Rothenburg, Jeff, *Preserving Authentic Digital Information*, The Council on Library and Information Resources. Washington, D.C.: Council on Library and Information Resources. Available from https://www.clir.org/pubs/reports/pub92/rothenberg/.

[B51] SEMI T20, Specification for Authentication of Semiconductors and Related Products.[28]

[B52] SEMI T22, Specification for Traceability by Self Authentication Service Body and Authentication Service Body.

[B53] The HIPAA Privacy Rule, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html.

[B54] The Minimum Elements for a Software Bill of Materials (SBOM), https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

[B55] Using Digital Certificates for IoT Root of Trust, https://www.keyfactor.com/blog/how-secure-boot-and-pki-enable-iot-device-security/.

[B56] W3C Verifiable Credentials Data Model v1.1, https://www.w3.org/TR/vc-data-model/.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

[27] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/
[28] SEMI publications are available at https://www.semi.org/en.

Copyright © 2024 IEEE and ULSE. All rights reserved.

Annex B

(informative)

Detailed sample use cases and derived functional needs

B.1 Introduction

The primary goal of developing use cases is to establish a set of user functional needs/requirements that guide the development of the technical requirements of the standard. The development of use cases for this standard involved the development of several exemplary use cases, from which the user functional needs/requirements were established. Annex C presents these requirements, as well as additional requirements, in a tabular format, allocating their relevance to the various topics of the standard using a Lead/Support/Consult (L/S/C) approach.

NOTE—Though the word "shall" is used in the needs analysis, these are informative functional needs/requirements that drive the technical requirements detailed in the normative content of this standard. The needs identified in Annex B are not requirements for implementation to conform to this standard.

B.2 Overview of the sample use cases

The world of CIoT is vast. Four sample use cases were selected to illustrate the application of the standard and cover most needs from a user perspective. Additional use cases are listed in B.9.

a) Connected monitoring device, using a continuous glucose monitor (CGM) as an example.

b) Connected therapy device, using an automated insulin delivery (AID) system as an example.

c) Hospital @Home, using several devices for a single patient.

d) Home-to-hospital, exploring the integration of devices the patient may bring with them to a hospital and the hospital devices.

It is believed that the user needs/requirements extracted from these four use cases provide a high degree of coverage for many CIoT use cases.

It is strongly recommended that use cases be developed by users of this standard for their specific CIoT scenarios as part of their development process. The approach outlined in this standard can be used to guide this effort.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

B.2.1 Connected monitoring device—Use Case 1

There are many connected monitoring device-based use cases. The clinical use case of a CGM was chosen, which has a simple sensor connected to a data acquisition system. This system may connect to remote server(s). Other use cases build on this initial scenario.

Use Case 1: In this use case, the diabetic uses a CGM to monitor blood sugar without assistance from anyone. The user can connect their CGM to a device management server for the purposes of updating device hardware and firmware.

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.2.2 Connected therapy device—Use Case 2

Use Case 2 consists of two use cases that are clinically dissimilar but technically have very similar requirements and challenges:

- *Use Case 2a:* A person with cardiac issues has an automated implantable cardioverter defibrillator (AICD). The patient goes home where the AICD communicates with an internet-based portal via an intermediate gateway such as an app in a smartphone or a separate standalone device. The clinician can use the portal to view the data provided by the patient's AICD as well as adjust certain settings on the device.
- *Use Case 2b:* In this use case the diabetic manages their blood sugar using an AID system (aka as an artificial pancreas) consisting of a CGM sensor, insulin pump, and "controller." Their physician and family can remotely monitor this data.

B.2.3 Hospital @Home use case—Use Case 3

Use Case 3: In this use case the patient is at home (or another non-traditional remote care environment). The healthcare institution, due to a lack of available beds, decides to monitor the patient remotely. It manages equipment procurement, deployment, and remote monitoring of the patient.

B.2.4 Home-to-Hospital use case—Use Case 4

Use Case 4: In this use case, the patient is at home (or in another non-traditional remote care environment) where the healthcare institution(s) actively monitors them (see B.2.3). The patient's condition deteriorates, which requires transference back to the hospital for more intensive care and therapy. The patient brings with them the medical devices used in the home environment that the hospital may use for monitoring or other purposes.

B.3 Use case process

There are different use case methodologies that use different terminology and approaches. Organizations should choose and apply a use case methodology during the development of a CIoT device and/or system that works well for them. This standard uses the following structured approach (please refer to Figure B.1 and Figure B.2), which starts with the scope:

- Scope: In this case it would be the scope as stated in the standard's project authorization (PAR) and further described in 1.1.
  - *Use case:* Is the general real-life situation within the discussed scope of this standard. The use case has a short name and description that describes the use case. The use case is further decomposed into one or more:
    - *Narratives:* A text description from the actor's standpoint about their involvement in the use case. It can also include the following:
      1) User diagrams that visualize the narrative from the user/actor point of view as well as one or more technical diagrams that visualize the narrative with high level technical implementation assumptions.
      2) List of actors and stakeholders that are interested parties that the use case may affect.
        - *Actions:* Major decomposed episodes in each narrative:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

- *Scenarios:* Variations of the actions that can be *happy paths* (when things go as planned) or *unhappy paths* (i.e., when something does not go as planned). Each scenario is further organized as

  1) *Steps:* Breakdown of the scenario into a sequence of steps

     — *User needs/requirements:* These are informative requirements from the user's perspective that drive the creation of the normative (shall/should) technical requirements that form the bulk of this document.

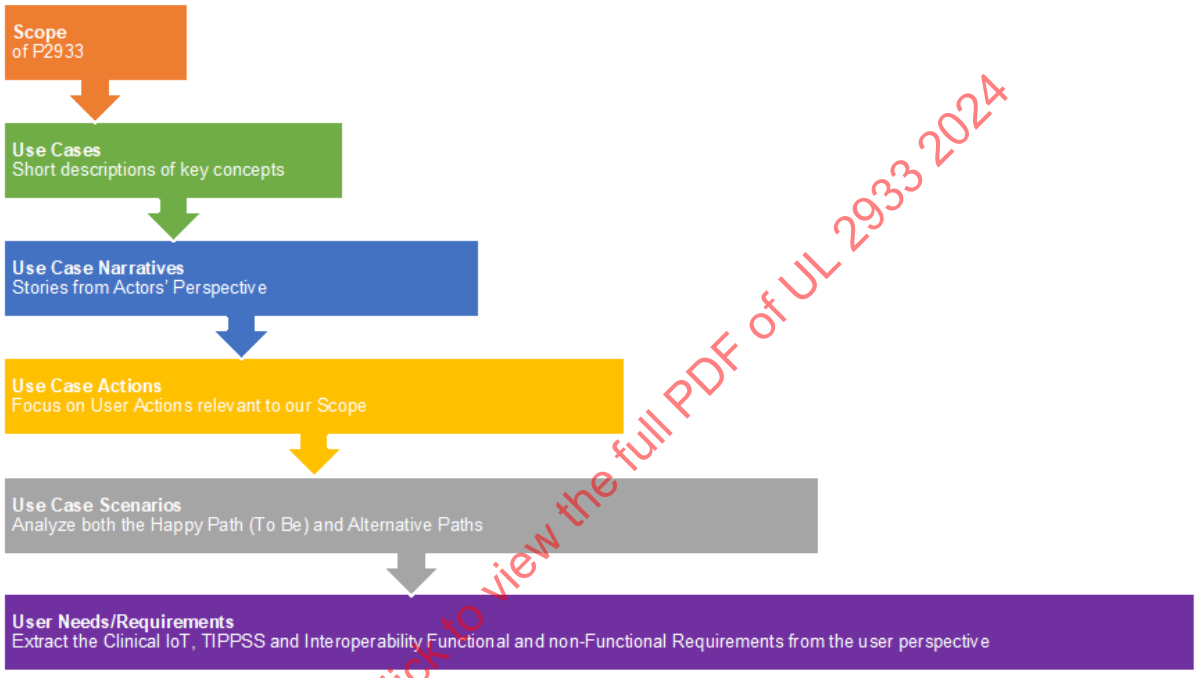

Figure B.1—Use case analysis: Flow from scope to non-technical requirements

Typically, there is only one overall scope, in this case it is CIoT data and device interoperability with TIPPSS. However, there are usually multiple use cases that explore the scope, and potentially multiple narratives that describe the use case from the user's perspective. Each narrative decomposes into actions, each action deconstructs into scenarios, and each scenario generates multiple non-technical user needs/requirements (requirements from the user perspective).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

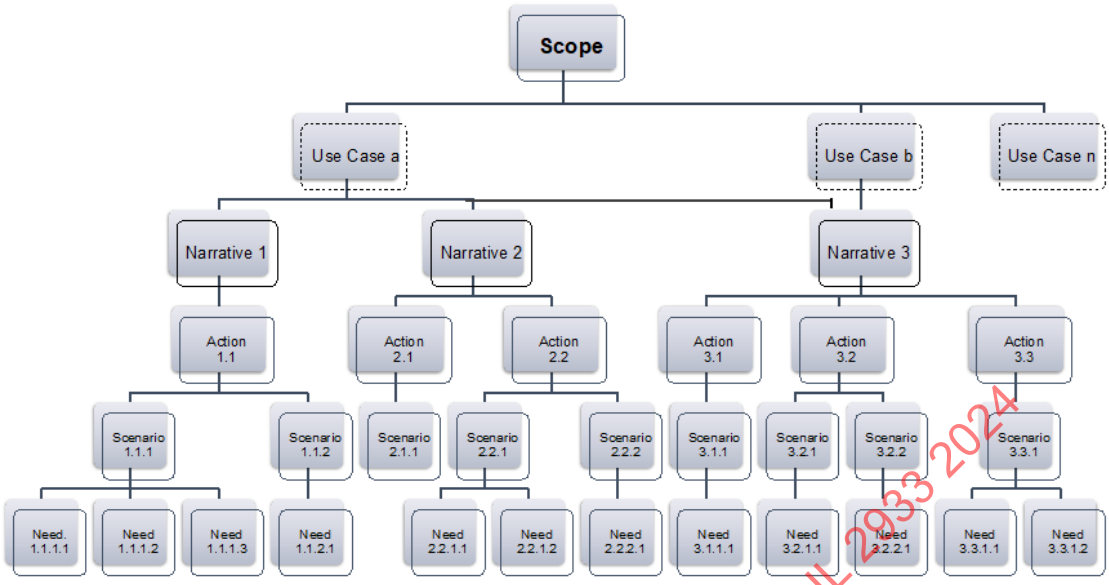

Figure B.2—Breakdown and organization of a typical use case

B.4 TIPPSS stakeholder roles

The following is a list of key CIoT stakeholder roles as referred to in this standard:

- Solution provider
- Patient
- Caregiver
- User
- Operator
- Maintainer
- Payor
- Regulator

NOTE—Subclause 3.1 contains definitions for these terms.

B.5 Use Case 1—Connected monitoring device

B.5.1 Use case description

The diabetic, at the request of their doctor, switched to a CGM system. He/she starts monitoring blood sugar without any assistance.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.5.2 Use case narrative

Caroline is a diabetic who lives on her own in Princeton, New Jersey. Her endocrinologist recommended that she should use a continuous glucose monitoring (CGM) system consisting of a body attached continuous glucose sensor and an accompanying CGM controller or a smartphone with a CGM app. The care provider provides Caroline with the system, has the system set up and gets trained at the doctor's office. If the controller uses a cellular connection, or it uses a phone app, this also addresses this aspect of the setup. She is also provided with a prescription to order additional sensors. Once home, if the controller does not use cellular, Caroline also connects the controller to her home Wi-Fi and starts monitoring her blood sugar. (See Figure B.3, Figure B.4, and Figure B.5.)

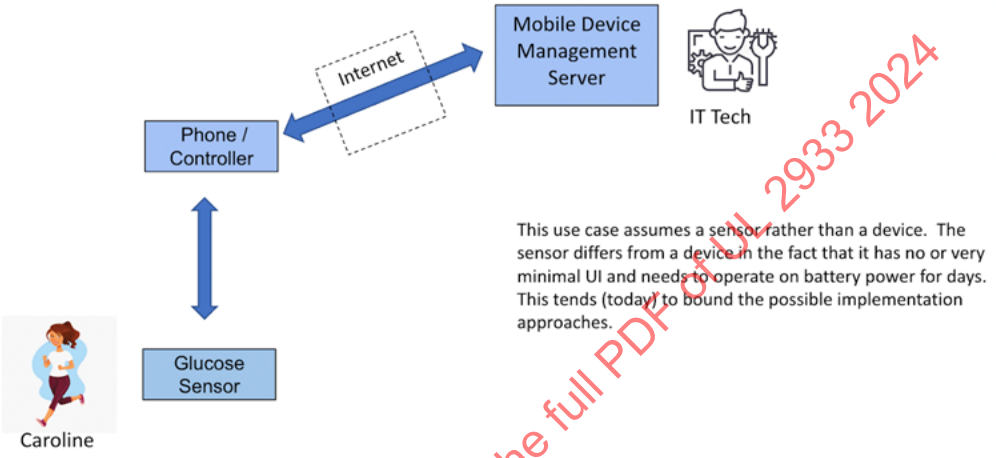

Figure B.3—Use Case 1—Simple continuous glucose monitor (CGM)—User view

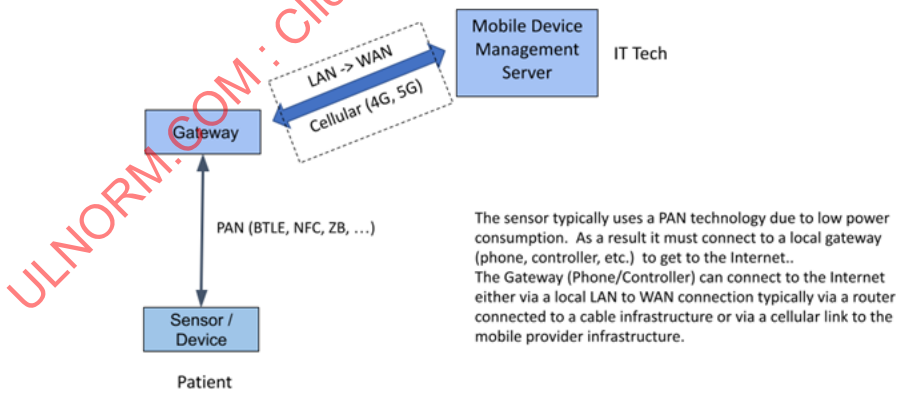

Figure B.4—Use Case 1—Connected monitoring device—Technical view 1

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

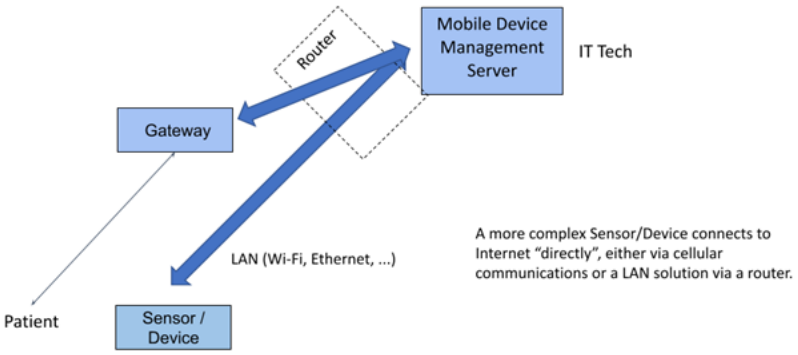

Figure B.5—Use Case 1—Connected monitoring device—Technical view 2

B.5.3 Use case actions

Use Case 1 actions are as follows:

- Acquire and prepare the CGM device
- Attach the CGM to the patient
- Manage glucose level
- Manage the CGM system

B.5.4 Actors and stakeholders

Use Case 1 actors and stakeholders are as follows:

Actors:

- Caroline (patient)

Stakeholders:

- Payor
- Clinician
- Technician (who sets the system up)
- Manufacturer

ULNORM.COM : Click to view the full PDF of UL 2933 2024

B.5.5 Use Case 1—Details

B.5.5.1 Use Case 1—Action #1

Acquire and prepare the CGM system.

Scenario 1.1.1: Happy path

Steps:

Copyright © 2024 IEEE and ULSE. All rights reserved.

a) The care provider provides Caroline with a sensor and controller/app at the endocrinologist office.

b) TECHNICIAN/assistant helps with setting up the controller.

c) Configure CGM controller/CGM app to associate with the CGM sensor.

d) Verify connectivity between CGM sensor and controller.

e) Controller acquires device demographics (device id, model, serial number, etc.)

   1) Controller scans a bar-code on the sensor for device demographics, or

   2) Controller uses NFC or RFID on the sensor for device demographics, or

   3) User enters device demographics into the controller.

f) Calibrates the CGM sensor (if necessary).

g) Configure CGM controller/app with alert levels, etc.

User needs/requirements:

— 1.1.1.01: Instructions for handling the CIoT physical device shall be readily available to the user.

— 1.1.1.02: Instructions for clinical setup and use of the CIoT physical device system shall be readily available.

— 1.1.1.03: CIoT physical devices shall be able to assess whether the device can “trust” other CIoT devices in the CIoT system.

— 1.1.1.04: Communication between the controller/CIoT virtual device and CIoT physical device shall use open standards-based methods for calibration.

— 1.1.1.05: Protocol for synchronizing the CIoT physical devices shall be open and standards-based.

— 1.1.1.06: Communication between the CIoT physical device and controller/CIoT virtual devices shall use a secure communication scheme.

— 1.1.1.07: ePHI and other data at rest shall be de-identified, pseudonymized, or anonymized wherever possible.

— 1.1.1.08: CIoT physical device shall communicate its globally unique verifiable device identifier.

— 1.1.1.09: CIoT physical device shall support NFC or RFID or Bar-Code or label with device “attributes”/identity on the CIoT physical device.

— 1.1.1.10: Controller/CIoT virtual device should support NFC or RFID or Bar-Code or label to enter device demographics/ID.

— 1.1.1.11: User shall be able to validate CIoT physical device to controller/CIoT virtual device connectivity.

— 1.1.1.12: Instructions for the technical setup and use of the CIoT physical device system shall be readily available.

— 1.1.1.13: Demographic data and other data at rest shall be “secure.”

Scenario 1.1.2: CGM sensor does not connect/communicate with CGM controller/app.

Steps:

a) Get alert on controller or smart device.

b) Replace with different sensor (current manufacturer or other manufacturer)

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

c) Bring CGM sensor closer to CGM controller/app.

d) (Imagine John Doe cannot get his normal sensor.)

e) Use wired link or alternative wireless link.

f) Continue to use old glucometer (stick finger to get blood sample)

User needs/requirements:

— 1.1.2.01: System shall support the ability for a user to exchange CIoT physical devices from different manufacturers.

— 1.1.2.02: System should support wired connections for transmission of data as a backup.

— 1.1.2.03: Controller/CIoT virtual device shall continuously monitor quality of communications link with CIoT physical device.

— 1.1.2.04: Controller/CIoT virtual device shall notify user of communications connectivity issues.

— 1.1.2.05: Controller/CIoT virtual device shall support discernable technical alerts for blind users.

— 1.1.2.06: Controller/CIoT virtual device shall support discernable technical alerts for hearing impaired users.

— 1.1.2.07: Controller/CIoT virtual device shall alert if it detects an CIoT physical device with an incompatible protocol version.

— 1.1.2.08: Controller/CIoT virtual device shall alert if it detects a CIoT physical device that does not meet its functional needs (e.g., inadequate accuracy).

— 1.1.2.09: Controller/CIoT virtual device shall alert and reject a CIoT physical device that does not support the same implemented security controls.

— 1.1.2.10: Controller/CIoT virtual device shall alert and reject a CIoT physical device that it does not "trust."

Scenario 1.1.3: User cannot enter user setup information (demographics, configuration, etc.) on CGM controller/smart device app.

Steps:

a) Use without setup information temporarily (if possible).

b) Continue to use old glucometer.

User needs/requirements:

— 1.1.3.01: System shall support limited but safe operation without complete setup of patient information.

Scenario 1.1.4: CGM sensor fails to calibrate.

Steps:

a) Receive CIoT physical device calibration failure message.

b) Replace with different CIoT physical device (current manufacturer or other manufacturer).

c) If failure continues, then return to using the old glucometer.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

— 1.1.4.01: Controller/CIoT virtual device shall detect CIoT physical device calibration failure and notify user.

— 1.1.2.01: System shall support the ability for a user to exchange CIoT physical devices from different manufacturers.

Scenario 1.1.5: Counterfeit CIoT sensor.

Steps:

a) Obtain “new” sensor from pharmacy.

b) Controller/CIoT virtual device detects that CIoT sensor ID is not properly registered.

c) Controller/CIoT virtual device does not operate with potentially counterfeit CIoT sensor.

d) Controller/CIoT virtual device alerts user that CIoT sensor may be counterfeit.

User needs/requirements:

— 1.1.5.01: Controller/CIoT virtual device shall check that CIoT physical device can properly authenticate and authorizes for usage.

— 1.1.5.02: Controller/CIoT virtual device shall alert user if it suspects a counterfeit CIoT physical device.

Scenario 1.1.6: Refurbished CIoT sensor.

Steps:

a) Obtain “new” CIoT sensor from pharmacy.

b) Controller/application (app) detects that a solution provider has not appropriately refurbished the CIoT sensor.

c) Controller/application (app) does not operate with potentially refurbished CIoT sensor.

d) Controller/application (app) alerts user that CIoT sensor is not properly refurbished.

User needs/requirements:

— 1.1.5.01: Controller/CIoT virtual device shall check that CIoT physical device can properly authenticate and authorizes for usage.

— 1.1.6.01: Controller/CIoT virtual device shall alert user if it suspects CIoT physical device is an unauthorized refurbished CIoT physical device.

B.5.5.2 Use Case 1—Action #2

Attach the CGM sensor (to the patient).

Scenario 1.2.1: Happy path

Steps:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

a) Caroline picks a location on her upper left arm.

b) Clean the location with an alcohol swab.

c) Place the sensor in that location.

d) Once she is ready, she switches the glucose sensor on.

e) The controller and sensor connect to each other.

f) The controller verifies the demographics data from the sensor is the same as configured.

g) The sensor continuously reports the glucose readings to the CGM controller/CGM app.

User needs/requirements:

— 1.2.1.01: The CIoT physical device shall encrypt data in motion.

— 1.2.1.02: CIoT physical device should authenticate controller/CIoT virtual device.

— 1.1.1.08: CIoT physical device shall communicate its globally unique device demographics/ID.

— 1.2.1.03: Communication between controller/CIoT virtual device and CIoT physical device shall use seamless open interoperability.

— 1.2.1.04: The user documentation shall disclose data communication capabilities of the CIoT physical device.

— 1.2.1.05: CIoT physical device shall communicate all its measurements, status, settings, and related meta-data.

— 1.2.1.06: To improve effectiveness and performance, the CIoT physical device shall communicate all information that can be used to improve those.

Scenario 1.2.2: CIoT sensor does not connect or communicate with CGM controller or smartphone.

Same as Scenario 1.1.2 plus the following:

— 1.2.2.01: If a communication disruption occurs, the CIoT physical device shall attempt to store all data until connection reestablishment.

— 1.2.2.02: The CIoT physical device shall secure any data stored on it.

— 1.2.2.03: If there is a communication disruption, the CIoT physical device shall upload stored data to controller/CIoT virtual device when connection is reestablished.

— 1.2.2.04: The CIoT physical device shall delete any stored data after transmission to controller/CIoT virtual device unless otherwise needed by the CIoT physical device.

— 1.2.2.05: The manufacturer shall disclose the size and clinically relevant capacity of the CIoT physical device data stored in the user documentation.

Scenario 1.2.3: Glucose reading out of set range.

Steps:

a) User sets upper and lower limits for glucose levels.

b) Controller/application (app) alerts user that glucose level is out of range.

c) User acknowledges alert.

d) User adjusts glucose level by injecting insulin or eating.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

e) User adjusts alert limits if necessary.

The requirements are as follows:

— 1.2.3.01: Controller/CIoT virtual device shall support the adjustment of alert limits.

— 1.2.3.02: Controller/CIoT virtual device shall signal (visual, audible, or haptic) clinical out-of-range conditions.

— 1.2.3.03: Controller/CIoT virtual device shall allow the user to disable clinical alerts.

Scenario 1.2.4: Sensor sends inaccurate readings.

Steps:

a) Patient believes readings are inaccurate:
   1) Patients receive alert for out-of-range readings.
   2) Patients receive alert that data may be inaccurate.
   3) Patient recognizes readings are not “normal” for him/her.
b) Recalibrate sensor.
c) If the sensor continues to send inaccurate readings, then replace the sensor.
d) If inaccurate readings continue use a manual glucometer.

User needs/requirements:

— 1.2.4.01: Controller/CIoT virtual device shall detect out-of-range clinical results and notify user.

— 1.2.4.02: Controller/CIoT virtual device shall flag questionable clinical readings (potentially using an AI-based application).

— 1.1.2.01: System shall support the ability for a user to exchange CIoT physical devices from different manufacturers.

Scenario 1.2.5: Sensor communicates intermittently.

Same as Scenario 1.2.2.

B.5.5.3 Use Case 1—Action #3

Manage glucose level.

Scenario 1.3.1: Happy path

Steps:

a) Obtain readings from CGM.
b) Adjust food intake daily based on reading.
c) Administer medication/insulin as needed.
d) React to alerts as appropriate.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

— 1.2.3.01: Controller shall support the adjustment of alert limits.

— 1.2.4.01: Controller/CIoT virtual device shall detect out-of-range results and notify user.

Scenario 1.3.2: System generates inaccurate readings.

Same as Scenario 1.2.4.

Scenario 1.3.3: User follows improper diet.

Same as Scenario 1.3.1.

Scenario 1.3.4: User administers improper insulin doses.

Same as Scenario 1.3.1.

Scenario 1.3.5: User has an allergic reaction to sensor.

Steps:

— Read the instruction manual (IFU)

User needs/requirements:

— 1.3.5.01: The CIoT physical device shall provide allergy and irritation notification if available.

— 1.3.5.02: The manufacturer shall disclose disclaimers and warnings for the CIoT physical device and/or CIoT virtual device in the accompanying documentation.

Scenario 1.3.6: User ignores alerts and CGM readings.

Steps:

— Out of scope

User needs/requirements:

— None

Scenario 1.3.7: User loses CGM controller.

Steps:

a) If using CGM app on phone, try to find phone.

b) Borrow CGM controller/app from “friend.”

c) Connect to personal sensor (see Scenario 1.1.1).

d) Get reading.

e) Return to “friend.”

User needs/requirements:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— 1.3.7.01: Return Instructions shall be accessible on the controller/app.

— 1.3.7.02: CIoT physical devices should support geo-location reporting.

— 1.3.7.03: CIoT physical device should support remote wipe/lock.

Scenario 1.3.8: Unintentional abuse (water damage, arc welder, MRI, etc.).

Steps:

a) User unintentionally subjects the sensor to environmental abuse.

b) Sensor may seem to work normally.

User needs/requirements:

— 1.3.8.01: The manufacturer shall provide clear instructions concerning proper environments of use for CIoT physical device.

Scenario 1.3.9: Intentional malicious access.

Steps:

a) Bad actor intentionally compromises the sensor, or

b) Bad actor intentionally hacks the sensor to controller data stream, or

c) Bad actor intentionally compromises the controller/app.

User needs/requirements:

— 1.3.9.01: The link between the CIoT sensor and controller/app shall use secure communications.

— 1.3.9.02: The communications link between CIoT sensor and controller/CIoT virtual device shall protect against person-in-the-middle attacks.

— 1.3.9.03: The controller/CIoT virtual device should detect erratic CIoT sensor behavior.

— 1.3.9.04: The controller/CIoT virtual device and sensor shall support secure remote software and firmware updates.

— 1.3.9.05: The controller/CIoT virtual device and sensor shall support human intervention to control software and firmware updates.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

B.5.5.4 Use Case 1—Action #4

Manage the CGM sensor.

Scenario 1.4.1: Happy path

Steps:

a) User receives notification from the controller to replace the sensor.

b) Replace sensor assembly.

c) Synchronize new sensor to CGM monitor or smartphone.

d) Receive notification to replace the battery.

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

— 1.4.1.01: CIoT sensor shall communicate expiration date to controller/CIoT virtual device.

— 1.4.1.02: Controller shall alert user when the controller needs to exchange the CIoT sensor.

— 1.4.1.03: CIoT sensor shall communicate battery status to app/controller.

— 1.4.1.04: Controller/CIoT virtual device shall alert when it is time to charge or replace CIoT sensor battery.

— 1.4.1.05: CIoT physical device shall communicate its “attributes”/identity (ID, SW/FW version, etc.)

— 1.4.1.06: CIoT physical device shall communicate internal error conditions to controller/CIoT virtual device and indicate whether the device requires replacement.

— 1.4.1.07: Controller/CIoT virtual device shall communicate its “attributes”/identity (ID, SW/FW version, etc.).

Scenario 1.4.2: User ignores sensor replacement advisory.

Steps:

a) User receives notification from controller/application (app) to replace sensor.

b) User ignores notification and continues to use CGM system.

c) Controller continues to display glucose reading marked as questionable.

d) If sensor stops operating, the controller/application (app) will display an appropriate error condition.

User needs/requirements:

— 1.4.2.01: Controller/CIoT virtual device shall indicate data from an expired CIoT sensor as questionable on its display.

— 1.4.2.02: Controller/CIoT virtual device shall indicate data from an expired CIoT sensor as questionable during communication.

— 1.4.2.03: Controller/CIoT virtual device shall indicate data from a CIoT sensor requiring battery replacement as questionable on its display.

— 1.4.2.04: Controller/CIoT virtual device shall indicate data from a CIoT physical device requiring battery replacement as questionable during communication.

B.5.5.5 Use Case 1—Action #5

Manage the CGM system.

Scenario 1.5.1: Happy path

Steps:

a) User connects CGM controller with device maintenance server.

b) User receives notification to update controller software (SW).

c) Update controller SW.

d) Receive notification to update sensor firmware (FW).

e) Update sensor FW.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

- 1.5.1.01: Controller/CIoT virtual device should connect to a device maintenance server.
- 1.5.1.02: Controller/CIoT virtual device shall communicate securely with device maintenance server.
- 1.5.1.03: Controller/CIoT virtual device shall obtain CIoT physical device “attributes”/identity (ID, SW/FW version, etc.).
- 1.5.1.04: Controller/CIoT virtual device shall communicate controller/CIoT virtual device and CIoT physical device “attributes”/identity to server.
- 1.5.1.05: Maintenance server shall detect out-of-date SW and FW.
- 1.5.1.06: Maintenance server shall download SW and FW updates to controller.
- 1.5.1.07: Controller/CIoT virtual device shall check authenticity and integrity of downloaded SW and FW.
- 1.5.1.08: Controller/CIoT virtual device shall communicate need for SW and/or FW update to user.
- 1.5.1.09: Controller/CIoT virtual device shall update its SW/FW, on user acknowledgement.
- 1.5.1.10: Controller/CIoT virtual device shall update the CIoT physical device SW and FW, on user acknowledgement.
- 1.5.1.11: Upon completion, controller/CIoT virtual device shall provide SW/FW update message (success or failure).

Scenario 1.5.2: User ignores controller SW update advisory.

Steps:

a) User connects CGM controller with device maintenance server.
b) User receives notification to update controller SW.
c) User ignores notification.

User needs/requirements:

- 1.5.2.01: Controller shall continue to remind user to update SW/FW if required.

Scenario 1.5.3: Sensor SW/FW update failure.

Steps:

a) Receive notification to update sensor SW/FW and initiate SW/FW update.
b) Sensor SW/FW fails to update, and sensor stops working.

User needs/requirements:

- 1.5.1.08: Controller/CIoT virtual device shall communicate need for SW and/or FW update to user.
- 1.5.3.01: CIoT physical device shall notify controller/CIoT virtual device of any SW and/or FW update failures.
- 1.5.3.02: CIoT physical device shall detect potential FW or SW compromises and notify controller/CIoT virtual device.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 1.5.4: Controller battery failure (or full discharge).

Steps:

a) Controller stops operating.

b) Obtain/borrow a different controller (potentially different manufacturer).

c) Use old finger stick glucometer.

User needs/requirements:

— 1.5.4.01: Controller/CIoT virtual device shall alert when it is time to charge or replace its battery.

Scenario 1.5.5: Controller SW/FW update failure.

Steps:

a) User receives notification to update controller SW/FW.

b) User initiates controller SW/FW update.

c) Controller SW/FW fails to update, and controller stops working.

User needs/requirements:

— 1.5.1.08: Controller/CIoT virtual device shall communicate need for SW and/or FW update to user.

— 1.5.5.01: Controller/CIoT virtual device shall notify user of any SW and/or FW update failures.

— 1.5.5.02: Controller/CIoT virtual device CIoT virtual device notify device management server of any SW and/or FW update failures.

— 1.5.5.03: Controller/CIoT virtual device shall detect potential FW or SW compromises.

— 1.5.5.04: Controller/CIoT virtual device should maintain a device log that captures all messages exchanged with device management server

— 1.5.5.05: Device management server should maintain a device log that captures all messages exchanged with the controller/CIoT virtual device.

— 1.5.5.06: Device log should not include any ePHI.

— 1.5.5.07: If the device log contains ePHI, then the device shall restrict access to it.

— 1.5.5.08: If the device log contains ePHI, the CIoT device should give the patient the opportunity to consent.

— 1.5.5.09: The manufacturer shall disclose the size of the CIoT physical device log.

— 1.5.5.10: If the SW and/or FW update fails, the CIoT device shall continue to operate with the previous SW and/or FW version.

B.6 Use Case 2—Connected therapy device

Figure B.6 and Figure B.7 cover the general case of a therapy device, which can be remotely adjusted. Two different use case variants are analyzed, which on the surface look quite different but are closely related to each other.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.6.1 Use Case 2a—Connected automated implanted cardioverter defibrillator (AICD)

B.6.1.1 Use Case 2a description

A person with an AICD is experiencing false discharges. The defibrillator settings need to be adjusted.

B.6.1.2 Use Case 2a narrative

Emily is an 85 y/o female who has been experiencing fainting spells. After evaluation by her cardiologist, it was determined that she was experiencing runs of ventricular tachycardia (VT) which caused the fainting. Her cardiologist decided that she was a suitable candidate for an AICD to manage the VT and she had surgery to insert the AICD. After her physician adjusted the device settings, Emily went home with a box that communicates information from the AICD to a portal and that allows her physician to monitor her status and adjust, as necessary. (See Figure B.8 and Figure B.9.)

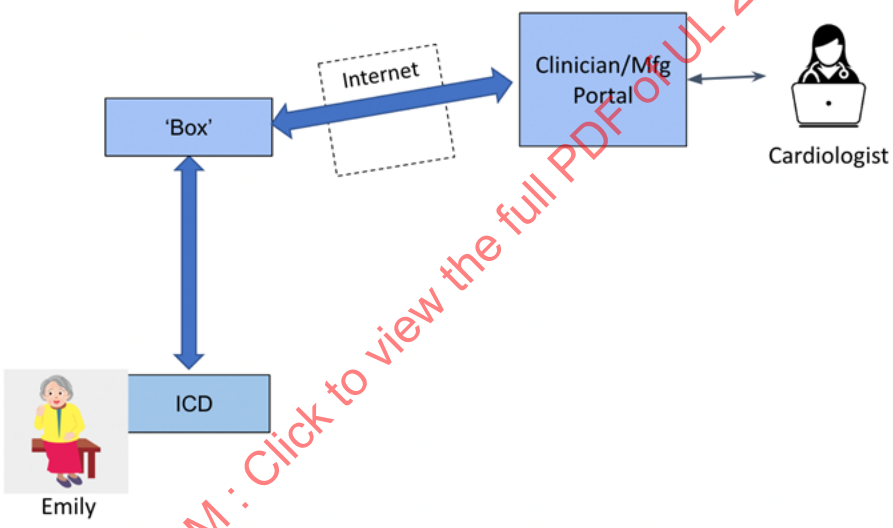

Figure B.6—Use Case 2a—Connected Therapy Device—Implanted cardioverter-defibrillator (ICD) —User view

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

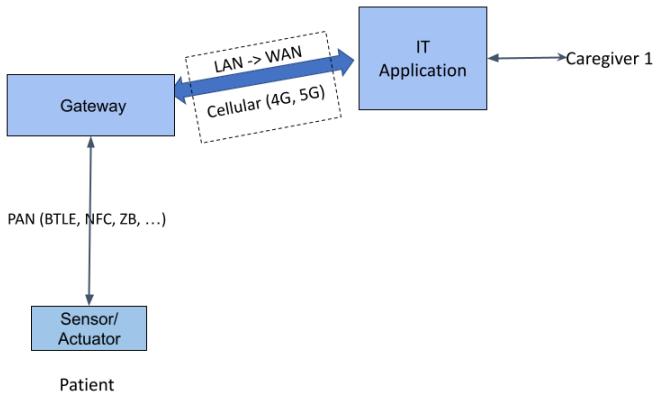

Figure B.7—Use Case 2a—Connected Therapy Device—Technical view

B.6.2 Use Case 2b—Connected automated insulin delivery (AID) system

B.6.2.1 Use Case 2b description

A diabetic is living in a healthcare facility (e.g., assisted living home, clinic). The patient has an automated insulin delivery system which a physician remotely monitors.

B.6.2.2 Use Case 2b narrative

John is a diabetic, living in an assisted living facility in Florida. Recently he has been having trouble managing his glucose. His endocrinologist has evaluated his situation and recommended that he use an AID system. The AID is provided by the physician office and is also set up there: connecting the sensor and pump to the controller, the controller to the facility Wi-Fi and/or cellular system, registering the device with the patient portal and attaching the sensor to John. The doctor, and anyone John authorizes can also monitor his blood sugar via the portal. (See Figure B.8 and Figure B.9.)

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

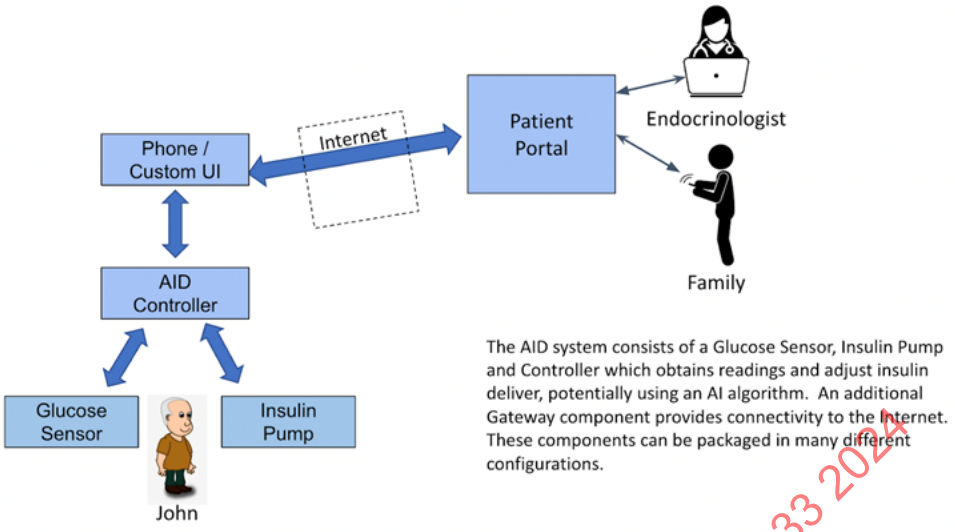

Figure B.8—Use Case 2b—Connected Therapy Device—Automated Insulin Delivery (AID) —User view

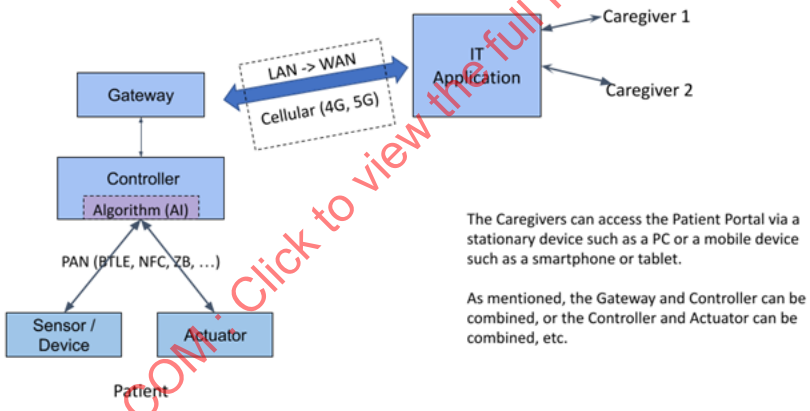

Figure B.9—Use Case 2b—Connected Therapy Device—Technical View

ULNORM.COM : Click to view the full PDF of UL 2933 2024

B.6.3 Use case actions

The use case actions are as follows:

a) Acquire and prepare the AID system—not applicable to UC 2b.
b) Connect Sensor and Pump (to the patient)—not applicable to UC 2b.
c) Connect AICD/AID controller to the facility or cellular infrastructure.
d) Register AICD/AID controller to portal.
e) Connect AICD/AID to the portal.
f) Collect data and transmit it to the portal.

Copyright © 2024 IEEE and ULSE. All rights reserved.

g) Physician/caregiver remotely monitors results.

h) Physician remotely adjusts ICD/AID settings.

B.6.4 Actors and stakeholders

Actors are as follows:

— Patient (John/Emily)

— Clinician (Endocrinologist/Cardiologist)

— Caregivers (parent, spouse, son/daughter, etc.)

Stakeholders are as follows:

— Payor

— Manufacturer

— Assisted-living home

NOTE—User needs/requirements are in *italics* if the previous scenario or use case stated them.

B.6.5 Use Case 2—Details

B.6.5.1 Use Case 2—Action #1

Acquire and prepare the AID system.

Scenario 2.1.1: Happy path

Steps:

a) A physician's office provides and sets up an AID system.

b) Physician staff charge the AID controller and the CGM sensor and Insulin Pump

c) Configure AID controller to associate with the CGM sensor.

d) Verify connectivity between CGM sensor and controller.

e) Controller acquires pump demographics (Device ID, Model, Serial Number, etc.)

   1) Controller scans a bar-code on the sensor for device demographics, or

   2) Controller uses NFC or RFID on the sensor for device demographics, or

   3) User enters device demographics into the controller.

f) Calibrate the CGM sensor.

g) Configure the AID controller to associate with the Insulin Pump

h) Verify connectivity between Insulin Pump and controller.

i) Controller acquires pump demographics (Device ID, Model, Serial Number, etc.)

   1) Controller scans a bar-code on the sensor for device demographics, or

   2) Controller uses NFC or RFID on the sensor for device demographics, or

   3) User enters device demographics into the controller.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

j) Configure AID controller with alert levels, patient specific settings, etc.

k) Validate the proper operation of the AID system.

User needs/requirements:

- 1.1.1.01: Instructions for proper device handling shall be readily available to the user.
- 1.1.1.02: Instructions for setup and use of the CIoT sensor system shall be readily available.
- 1.1.1.03: Devices shall be able to assess whether the device can "trust" other devices and CIoT virtual devices.
- 1.1.1.04: Communication between the controller/CIoT virtual device and CIoT physical device shall use open standards-based methods for calibration.
- 1.1.1.05: Protocol for synchronizing the devices shall be open and standards-based.
- 1.1.1.06: Synchronization scheme shall be "secure."
- 1.1.1.07: CIoT sensor shall encrypt demographics data and other data at rest.
- 1.1.1.08: CIoT sensor shall communicate its globally unique device demographics/ID.
- 1.1.1.09: CIoT sensor shall support NFC or RFID or Bar-Code or label with device demographics/ID on CIoT sensor.
- 1.1.1.10: Controller/CIoT virtual device shall support NFC or RFID or Bar-Code or label to enter device demographics/ID.
- 1.1.1.11: User shall be able to verify CIoT sensor to controller/CIoT virtual device connectivity.
- 2.1.1.01: User shall be able to validate proper system clinical operation.

Scenario 2.1.2: CGM Sensor does not connect/communicate with AID controller.

- Same as Scenario 1.1.2

Scenario 2.1.3: Cannot enter setup information (demographics, configuration, etc.) on AID controller.

- Same as Scenario 1.1.3

Scenario 2.1.4: Sensor fails to calibrate.

- Same as Scenario 1.1.4

Scenario 2.1.5: Insulin Pump does not connect/communicate with AID controller.

- Same as Scenario 1.1.2

ULNORM.COM : Click to view the full PDF of UL 2933 2024

B.6.5.2 Use Case 2—Action #2

Attach the sensor and pump (to the patient)

Scenario 2.2.1: Happy path

Steps:

a) User picks a location for the sensor.
   1) Clean the location with an alcohol swab.
   2) Place the sensor in that location.

Copyright © 2024 IEEE and ULSE. All rights reserved.

b) User picks a location for the insulin pump.

   1) Staff prepare and insert catheter.

   2) Staff attach pump to catheter.

c) Once ready, staff switches the glucose sensor and insulin pump on

d) The controller and sensor connect to each other.

e) The controller verifies the device's demographics data from the sensor and pump are the same as configured.

f) The controller gets a reading from the sensor.

   1) The sensor continuously reports the reading, or

   2) The controller queries the sensor for a reading.

g) The controller runs an AI/ML based algorithm to determine when and the amount of insulin that should be administered.

h) Based on the algorithm, the controller periodically tells the insulin pump to infuse a certain dose

User needs/requirements:

- 1.1.1.08: CIoT sensor shall communicate its globally unique device demographics/ID.
- 1.2.1.01: The CIoT sensor shall encrypt data in motion.
- 1.2.1.03: Controller/CIoT virtual device shall authenticate CIoT physical device.
- 1.2.1.04: CIoT sensor should authenticate controller/app.
- 1.2.1.05: Seamless open interoperability between controller/CIoT virtual device and CIoT physical device.
- 1.2.1.06: Communication between controller/CIoT virtual device and CIoT physical device shall be secure.
- 2.2.1.01: Controller/CIoT virtual device shall check that the actuator properly authenticates.
- 2.2.1.02: Controller/CIoT virtual device shall alert user if it suspects a counterfeit actuator.
- 2.2.1.03: Seamless open interoperability between controller/CIoT virtual device and actuator
- 2.2.1.04: Secure communication between controller/CIoT virtual device and actuator
- 2.2.1.05: Exchanged data shall include its provenance.
- 2.2.1.06: Manufacturers shall provide guidelines concerning data availability.
- 2.2.1.07: Manufacturers shall provide guidelines concerning data usability.
- 2.2.1.08: Manufacturers shall provide guidelines concerning data integrity.

Scenario 2.2.2: Sensor does not connect or communicate with controller.

- Same as Scenario 1.1.2

Scenario 2.2.3: Sensor communicates intermittently with controller.

- Same as Scenario 1.1.3

Scenario 2.2.4: Sensor sends inaccurate readings.

- Same as Scenario 1.1.4

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 2.2.5: Pump does not connect or communicate with controller.

Steps:

a) Get alert on controller or smart device.

b) Potential options:

1) Bring the controller closer to the pump.

2) Replace with different pump (current manufacturer).

3) Replace with different pump (other manufacturer).

4) Use wired link or alternative wireless link.

5) Inject insulin manually based on CGM readings.

User needs/requirements:

— 2.2.5.01: User shall have the ability to exchange actuators from different manufacturers.

— 1.1.2.02: Wired connections for transmission of data as a backup.

— 1.1.2.03: Continuously monitor quality of link between controller/CIoT virtual device and CIoT physical device.

— 1.1.2.04: Notify user of connectivity issues.

— 2.2.5.02: Actuators shall store data during periods of non-connectivity.

— 2.2.5.03: Actuators shall communicate stored data to the controller/CIoT virtual device on connection.

— 2.2.5.04: The actuator shall secure any data stored on it.

— 2.2.5.05: The actuator shall delete any data stored on it as soon as possible.

— 2.2.5.06: System shall operate safely without internet connectivity.

Scenario 2.2.6: Pump communicates intermittently with controller.

— Same as Scenario 2.2.5

Scenario 2.2.7: Pump administers inaccurate doses.

— Same as Scenario 2.2.5

Scenario 2.2.8: AI/ML algorithm failure.

Steps:

a) AI/ML algorithm acquiring the glucose level and controlling the pump fails.

User needs/requirements:

— 2.2.8.01: Guardrails/limits shall be inherent in any algorithms to limit actuator actions.

— 2.2.8.02: The device shall alert users to any clinical algorithm failure.

B.6.5.3 Use Case 2—Action #3

Connect controller to the home/facility or cellular infrastructure.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 2.3.1: Happy path

Steps:

a) If the controller uses IEEE 802.11, configure it with appropriate SSID and password

b) If the controller uses cellular, insert SIM card (or configure eSIM)

User needs/requirements:

— 2.3.1.01: Controller shall support IEEE 802.11g/n/ac, if applicable.

— 2.3.1.02: Controller shall support WPA2 or greater authentication/encryption.

— 2.3.1.03: Controller shall support x.509 security certificates.

— 2.3.1.04: Controller shall support 4G/5G if applicable.

Scenario 2.3.2: Cannot connect to IEEE 802.11 network.

Steps:

a) Verify the IEEE 802.11 network access point and SSID is available and has adequate signal strength.

b) Verify the IEEE 802.11 network access point and SSID support WPA2 or greater authentication/encryption.

c) Verify Wi-Fi password.

User needs/requirements:

— 2.3.2.01: The manufacturer shall disclose the IEEE 802.11 network troubleshooting information in the accompanying documentation, if applicable.

— 2.3.3.01: The manufacturer shall disclose cellular troubleshooting information in the accompanying documentation, if applicable

Scenario 2.3.3: Cannot connect to 4G/5G networks.

Steps:

a) Verify 4G/5G adequate signal strength.

b) Verify data availability according to user's contract.

c) Verify device enables and turned-on data mode.

User needs/requirements:

— 2.3.3.01: The manufacturer shall disclose cellular troubleshooting information in the accompanying documentation, if applicable.

B.6.5.4 Use Case 2—Action #4

Register controller to patient portal.

Scenario 2.4.1: Happy path

Steps:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

a) Patient logs into the patient portal with credentials

b) Patient registers device at the portal using Unique Device Identity

c) Patient registers device at portal using Unique Device Manufacturer Identity

d) Patient registers device at portal using manufacturer-assigned model and serial number

e) Patient registers device at portal using Device MAC address

f) Device initiates communication with the portal

User needs/requirements:

— 2.4.1.01: The portal shall authenticate Patient to use it.

— 2.4.1.02: The portal shall authorize Patient to use specific aspects of it.

— 2.4.1.03: Patient shall communicate securely with the portal.

— 2.4.1.04: Patient shall have a system-wide unique ID at a minimum.

— 2.4.1.05: Patient shall be able to associate CIoT physical devices with themselves.

— 2.4.1.06: Controller/CIoT virtual device has and shall communicate its globally unique verifiable device identity.

— 2.4.1.07: Controller/CIoT virtual device shall communicate its Manufacturer Model and Serial Number.

— 2.4.1.08: Controller/CIoT virtual device shall communicate its MAC Address.

— 2.4.1.09: Controller/CIoT virtual device shall communicate securely with patient portal.

— 2.4.1.10: The device shall only communicate necessary information to the portal.

— 2.4.1.11: The device shall delete any unnecessary patient data after communication with the portal.

— 2.4.1.12: Patient shall be able to associate controller/CIoT virtual device with themselves.

Scenario 2.4.2: Cannot connect to the IEEE 802.11 network.

Steps:

a) Verify that the IEEE 802.11 network access point and SSID are available and have adequate signal strength.

b) Verify The IEEE 802.11 network password.

User needs/requirements:

— 2.3.2.01: The IEEE 802.11 network troubleshooting information shall be provided in user guides if applicable.

Scenario 2.4.3: Cannot connect to 4G/5G networks.

Steps:

a) Verify 4G/5G adequate signal strength.

b) Verify data availability according to user’s contract.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

c) Verify the device has enabled data mode.

d) Verify the SIM (or eSIM) activates properly.

User needs/requirements:

— 2.3.3.01: If applicable, user guides shall provide cellular troubleshooting information.

B.6.5.5 Use Case 2—Action #5

Connect controller to patient portal.

Scenario 2.5.1: Happy path

Steps:

a) Controller/gateway initiates communication with the portal

b) Controller/gateway and portal mutually authenticate.

c) Controller/gateway provides and installs security certificates.

User needs/requirements:

— 2.5.1.01: Controller/gateway shall only communicate with a trusted portal.

— 2.5.1.02: Portal shall only communicate with a trusted controller/gateway.

— 2.5.1.03: Device shall accept and install x.509 security certificates.

Scenario 2.5.2: Portal does not "trust" device/sensor since it is counterfeit.

Steps:

a) Controller/application (app) detects that one or more CIoT physical devices are not properly registered.

b) Controller/application (app) does not operate with potentially counterfeit sensors.

c) Controller/application (app) alerts the user that the sensor may be counterfeit.

User needs/requirements:

— Same as Scenario 1.1.5

Scenario 2.5.3: Portal does not "trust" device/sensor since it has been used.

Steps:

a) Controller/application (app) detects inappropriate refurbishment of one or more CIoT physical devices.

b) Controller/application (app) does not operate with potentially improperly refurbished sensors.

c) Controller/application (app) alerts user of an inappropriately refurbished sensor.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

— Same as Scenario 1.1.6

Scenario 2.5.4: Portal does not "trust" device/sensor since it does not meet requirements.

Steps:

a) Controller/application (app) detects that one or more CIoT physical devices does not meet requirements.

b) Controller/application (app) does not operate with the CIoT physical devices.

c) Controller/application (app) alerts user that the CIoT physical device cannot operate.

User needs/requirements:

— 2.5.4.01: Controller/CIoT virtual device shall check that the CIoT physical device meets the requirements for its intended use.

— 2.5.4.02: Controller/CIoT virtual device shall notify the user if the CIoT physical device does not meet the requirements for its intended use and will not operate.

B.6.5.6 Use Case 2—Action #6

Collect data and transmit it to the portal.

Scenario 2.6.1: Happy path

Steps:

a) Sensor communicates with AID controller.

b) Pump communicates with the AID controller.

c) Controller manages dosage based on sensor readings.

d) Controller communicates with patient portal, uploading data every 15 minutes.

   1) Sensor readings

   2) Dosage administered.

   3) Error conditions

   4) Other appropriate data.

User needs/requirements:

— 2.6.1.01: CIoT physical device and controller shall communicate securely and reliably.

— 2.6.1.02: Controller/CIoT virtual device and cloud/portal shall communicate securely and reliably.

— 2.6.1.03: CIoT physical device and controller shall support "Continuous" reporting (as often as every minute) of data from system to cloud/portal.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 2.6.2: Intermittent connection to the IEEE 802.11 network.

— Same as Scenario 1.2.2

Scenario 2.6.3: Intermittent connection to patient portal using cellular connection.

— Same as Scenario 1.2.2

Scenario 2.6.4: The AID becomes compromised.

Steps:

a) AID operation becomes unstable, slow, or stops operating.

User needs/requirements:

— 2.6.4.01: The manufacturer shall incorporate malware protection.
— 2.6.4.02: The manufacturer shall incorporate safe coding practices.
— 2.6.4.03: The manufacturer shall conduct a complete threat analysis of the system.
— 2.6.4.04: The manufacturer shall conduct vulnerability testing.
— 2.6.4.05: The manufacturer shall provide information to the user regarding the safe and secure use of its products.

Scenario 2.6.5: Friend loses AID controller/app.

Steps:

a) Lend AID controller/app to friend.
b) Disable communication between AID controller/app to portal.
c) Connect AID controller/app to personal sensor.
d) Get reading.
e) Retrieve from friend.
f) Re-enable communication between AID controller/app to portal.

User needs/requirements:

— 2.6.5.01: The user shall be able to temporarily disable controller/CIoT virtual device communication to portal.
— 2.6.5.02: The controller/CIoT virtual device shall alert user if it has not been communicating to portal after a defined time.

B.6.5.7 Use Case 2—Action #7

Endocrinologist/caregiver monitor the results.

Scenario 2.7.1: Happy path

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Steps:

a) Doctor/caregiver establishes an account in the portal.
b) Patient provides permission for doctor/caregiver to view results in portal.
c) Doctor/caregiver logs into the patient portal with credentials
d) Portal allows doctor/caregiver to view the patient's results.

User needs/requirements:

— 2.7.1.01: Authenticated caregivers shall be able to establish accounts in the portal application.
— 2.7.1.02: Patients shall be able to authorize one or more caregivers to view results.
— 2.7.1.03: Authenticated caregivers shall be able to only view the results of specific patients once authorized.

Scenario 2.7.2: Doctor/caregiver connection to the portal via the IEEE 802.11 network fails.

Steps:

a) Verify that the IEEE 802.11 network access point and SSID are available and have adequate signal strength.
b) Verify the IEEE 802.11 network password.

User needs/requirements:

— 1.2.2.01: Provide troubleshooting information in user guides.

Scenario 2.7.3: Doctor/caregiver connection to the portal via cellular network fails.

Steps:

a) Verify that the cellular account is active.

User needs/requirements:

— 1.2.2.01: Provide troubleshooting information in user guides.

B.6.5.8 Use Case 2—Action #8

Endocrinologist remotely changes AID Settings

Scenario 2.8.1: Happy path

Steps:

a) The doctor decides to adjust the settings on the AID controller.
b) The doctor accesses the portal and the patient's account.
c) Doctor makes change.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

d) System acknowledges that change was queued.

e) The patient's controller asks the patient to accept the change.

f) Patient accepts the change.

g) The system makes the change to the controller settings.

h) The system sends the change notification back to the doctor.

User needs/requirements:

— 2.8.1.01: The system shall allow the patient to acknowledge any remote change commands.

— 2.8.1.02: The system shall advise the caregiver of the results of remote change commands (on the user interface) they requested in a timely fashion.

Scenario 2.8.2: Physician cannot adjust settings on the controller.

Steps:

a) The doctor decides to adjust settings on the controller.

b) The doctor accesses the portal and the patient's account.

c) Doctor requests change at the portal.

d) Request fails.

User needs/requirements:

— 2.8.2.01: CIoT physical device shall reject commands if it cannot authenticate the source.

— 2.8.2.02: CIoT physical device shall reject commands if the source does not have adequate rights (trust).

— 2.8.2.03: System shall allow portal application to distinguish between failure types and notify user.

Scenario 2.8.3: Hacker breaks into portal and attempts to adjust settings on the patient's CIoT physical device.

Steps:

a) Unauthorized user gains access to the Command Center portal

b) Unauthorized user changes settings on Jan's home monitor

c) The system informs the Command Center technician of any settings changes to their patients.

d) Command Center technician can temporarily lock access to the portal.

User needs/requirements:

— 2.8.3.01: The system shall notify the User of any remote settings changes.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.7 Use Case 3—Hospital @Home

B.7.1 Use case description

The hospital sends home a patient for intense remote monitoring. The data is aggregated locally and sent to a "Command Center" where an AI-based service monitors the status. If the patient develops complications that the system detects, it notifies a human who takes appropriate action.

B.7.2 Use case narrative

Jan Ferguson went to the hospital ER because he had a fever and a cough. The hospital tested them, and the results were that Jan tested positive for COVID-19. Normally, Jan would have been admitted; however, the hospital only currently admits patients who are in serious condition. The hospital sent Jan home for isolation and remote monitoring.

Within hours, a technician arrived and attached them to a Temperature monitor, Non-Invasive Blood Pressure Monitor, SpO2 monitor, and Respiration monitor, as well as a portable point-of-care lab. These devices are all interoperable and communicate with a provided home-based device aggregator (#1), which will communicate real-time results back to the hospital via cellular connection (#2). Before leaving, the technician verified that everything was working locally, registered the system in the hospital Command Center system, and verified the connection to the hospital was working.

In the hospital, the data from the remote monitoring system feeds a "Command Center" where trained technicians can view Jan's results (#3). In parallel, a service (application) using AI continuously analyzes its data. This service has been trained to monitor Jan for any COVID-related worsening of symptoms (#4). If Jan reaches a preset threshold, the service will alert a human in the Command Center (#5). The technician will then review the results with a physician and send an ambulance if necessary. (See Figure B.10 and Figure B.11.)

ULNORM.COM : Click to view the full PDF of UL 2933 2024

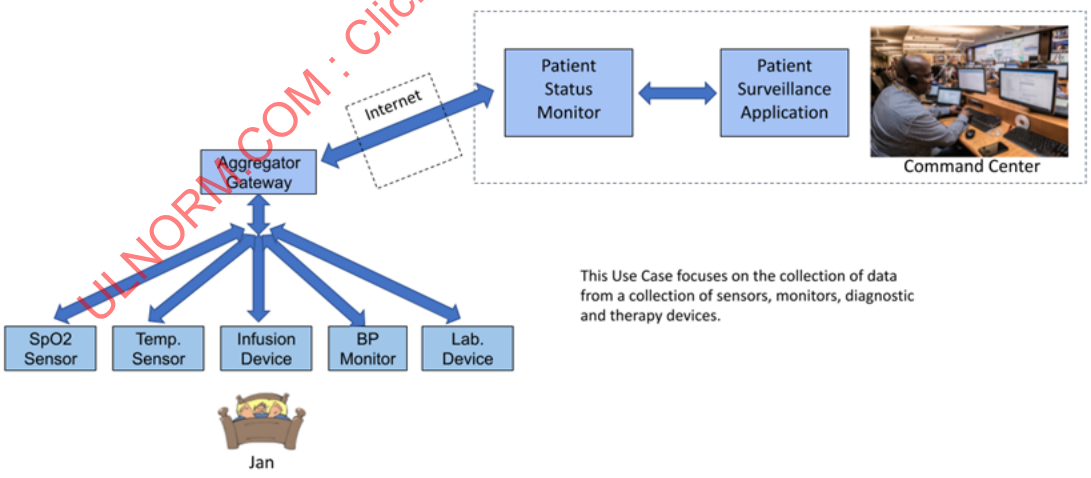

Figure B.10—Use Case 3—Hospital @Home—User View

Copyright © 2024 IEEE and ULSE. All rights reserved.

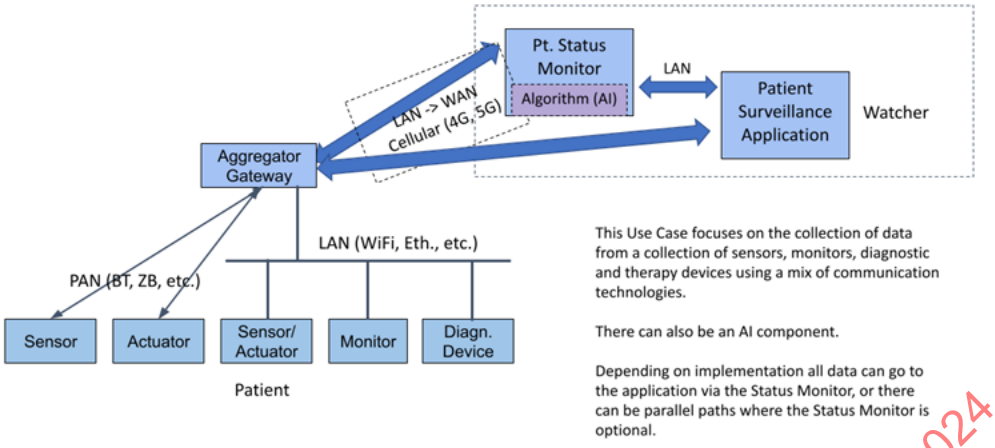

Figure B.11—Use Case 3—Hospital @Home—Technical View

B.7.3 Pre-conditions

- Sensors and actuators have previously connected to the aggregator/gateway.
- Previous use cases related to connection handled connection-related scenarios.

B.7.4 Use case actions

- Connect devices to home aggregator/gateway.
- Connect home aggregator to hospital Command Center portal and AI service.
- Command Center technicians monitor the results.
- Command Center technician receives alerts at the portal from the AI service.
- Command Center technician modifies settings.
- Command Center technician alerts emergency services.
- Provider discharges the patient from home health monitoring.

B.7.5 Actors and stakeholders

Actors:

- Jan, the patient
- Technician (sent to home)
- Technician (in Command Center)

Stakeholders:

- Payor
- Manufacturers
- Hospital

NOTE—User needs/requirements are in *italics* if a previous scenario or use case stated them.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.7.6 Use Case 3—Details

B.7.6.1 Use Case 3—Action #1

Connect devices to home aggregator (sensors and actuators covered in previous use cases).

Scenario 3.1.1: Happy path

Steps:

a) Configure an aggregator to associate with the device.

b) Verify connectivity between device(s) and aggregator.

c) User enters device demographics (device ID, model, serial number, etc.) into aggregator.

d) Hospital @Home CIoT physical devices discover other local CIoT physical devices and connect to them as needed.

User needs/requirements:

— 1.1.1.01: Instructions for proper CIoT physical device handling shall be readily available to the user.

— 1.1.1.02: Instructions for setup and use of the CIoT physical device system shall be readily available.

— 1.1.1.03: CIoT physical devices shall be able to assess whether the device can “trust” other CIoT physical devices and controller/CIoT virtual devices.

— 1.1.1.04: Communication between the controller/CIoT virtual device and CIoT physical device shall use Open standards-based methods for calibration.

— 1.1.1.05: Protocol for synchronizing the CIoT physical devices shall be open and standards-based.

— 1.1.1.06: Communication scheme shall be “secure.”

— 1.1.1.07: The CIoT physical device shall encrypt demographics data and other data at rest.

— 1.1.1.08: CIoT physical device shall communicate its globally unique device demographics/ID.

— 1.1.1.09: CIoT physical device shall support NFC or RFID or bar-code or label with device demographics/ID on CIoT physical device.

— 1.1.1.10: Controller/CIoT virtual device should support NFC or RFID or bar-code or label to enter device demographics/ID.

— 1.1.1.11: User shall be able to validate CIoT physical device to controller/CIoT virtual device connectivity.

— 3.1.1.01: Communication between the controller/gateway and CIoT physical devices shall use Open standards-based communication.

— 3.1.1.02: Communication between CIoT physical devices and other CIoT physical devices shall use Open standards-based communication.

— 3.1.1.03: CIoT physical devices shall be able to discover and connect with other CIoT physical devices.

— 3.1.1.04: Controllers/gateways shall be able to discover and connect with other CIoT physical devices.

— 3.1.1.05: User shall be able to validate CIoT physical device to CIoT physical device connectivity.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— 3.1.1.06: The manufacturer shall provide detailed instructions concerning the provisioning of devices.

— 3.1.1.07: The manufacturer shall provide detailed instructions concerning the provisioning of aggregators/gateways.

— 3.1.1.08: The manufacturer shall provide detailed installation and troubleshooting instructions for system integrators to follow.

— 3.1.1.09: The manufacturer shall provide detailed installation and troubleshooting instructions for intended users (patient, caregiver, service provider, etc.) to follow.

— 3.1.1.10: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines from the manufacturer when provisioning the CIoT physical device.

— 3.1.1.11: System integrators shall follow detailed instructions.

— 3.1.1.12: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines for provisioning of aggregator/gateways.

— 3.1.1.13: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines for deprovisioning of aggregators/gateways.

— 3.1.1.14: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines from the manufacturer when deprovisioning the CIoT physical device.

— 3.1.1.15: Manufacturers shall design the aggregator/gateway to enable remote provisioning, forensic data logging, and software updates.

Scenario 3.1.2: Device does not connect/communicate with controller/gateway.

Steps:

a) Get alert on controller/gateway or smart device.

b) Replace with different device (current manufacturer or other manufacturer).

c) Use wired link or alternative wireless link.

d) Continue to use device without connectivity until the user/operator resolves the issue.

User needs/requirements:

— Same as Scenario 1.1.2

Scenario 3.1.3: Aggregator does not "trust" device/sensor since it is counterfeit.

Steps:

a) Controller/application (app) detects that one or more CIoT physical devices are not properly registered.

b) Controller/application (app) does not operate with potentially counterfeit sensor.

c) Controller/application (app) alerts the user that the sensor may be counterfeit.

User needs/requirements:

— Same as Scenario 1.1.5

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 3.1.4: Aggregator does not "trust" device/sensor since it has been used.

Steps:

a) Controller/application (app) detects that the solution provider has inappropriately refurbished one or more CIoT physical devices.

b) Controller/application (app) does not operate with potentially refurbished sensor.

c) Controller/application (app) alerts the user of an inappropriately refurbished sensor.

User needs/requirements:

— Same as Scenario 1.1.6

Scenario 3.1.4: Aggregator does not "trust" device/sensor since it does not meet requirements.

Steps:

a) Controller/application (app) detects that one or more CIoT physical devices do not meet requirements.

b) Controller/application (app) does not operate with the CIoT physical devices.

c) Controller/application (app) alerts users that the current CIoT physical device cannot be used.

User needs/requirements:

— Same as Scenario 2.5.4

B.7.6.2 Use Case 3—Action #2

Connect home aggregator to hospital Command Center portal and AI service.

Scenario 3.2.1: Happy path

Steps:

a) Admin user logs into the Command Center and AI service with credentials.

b) Admin user registers aggregator at the Command Center and AI service using Unique Device Identity.

c) Patient registers aggregator at Command Center and AI service using Unique Device Manufacturer Identity.

d) Patient registers aggregator at Command Center and AI service using manufacturer-assigned model and serial number.

e) Patient registers aggregator at Command Center and AI service using Device MAC address.

f) Aggregator communicates with the AI service and Command Center.

g) Verify sensors, actuators, and devices connect to and interoperate with the AI service and Command Center.

h) Report results every minute to the AI service and Command Center.

User needs/requirements:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— 3.2.1.01: Monitoring portal/application shall authenticate aggregator/gateway.

— 3.2.1.02: Monitoring portal/application shall authenticate all connected CIoT physical devices.

— 3.2.1.03: The link between the aggregator/gateway and monitoring portal/application shall use secure communications.

— 3.2.1.04: The manufacturer shall limit communications between the aggregator/gateway and the monitoring portal/application to the minimal data set required for the application.

— 3.2.1.05: Communications between aggregator/gateway and monitoring portal/application shall use open standards-based interoperable communications.

— 3.2.1.06: AI service shall authenticate aggregator/gateway.

— 3.2.1.07: AI service shall authenticate all connected CIoT physical devices.

— 3.2.1.08: The manufacturer shall secure communications between aggregator/gateway and the AI service.

— 3.2.1.09: The manufacturer shall limit communications between aggregator/gateway and the AI service to the minimal data set required for the application.

— 3.2.1.10: Communications between aggregator/gateway and AI service shall use open standards-based interoperable communications.

— 3.2.1.11: AI service shall authenticate monitoring portal.

— 3.2.1.12: Monitoring portal/application shall authenticate AI service.

— 3.2.1.13: The manufacturer shall provide for secure communications between the monitoring portal/application and the AI service for all communication.

— 3.2.1.14: The manufacturer shall limit communications between the monitoring portal/application and the AI service to the minimal data set required for the application.

— 3.2.1.15: Communications between monitoring portal/application and AI service shall use open standards-based interoperable communications.

— 3.2.1.16: The manufacturer shall disclose whether the Device contains AI/ML in the accompanying documentation.

— 3.2.1.17: A device shall communicate whether it contains AI/ML.

Scenario 3.2.2: Aggregator/gateway fails.

Steps:

a) User receives an alert from the Command Center that the aggregator/gateway no longer works.

b) User substitutes current aggregator/gateway with another from a different manufacturer.

c) User follows steps from Scenario 3.2.1.

User needs/requirements:

— 3.2.2.01: Application shall detect failure (lack of communication) of aggregator/gateway.

— 3.2.2.02: Application shall alert users of aggregator/gateway failures.

— 3.2.2.03: Application and aggregator/gateway communicate using open standards-based interoperability protocols.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 3.2.3: AI service fails.

Steps:

a) Verify that the IEEE 802.11 network access point and SSID are available and has adequate signal strength.

b) Verify the IEEE 802.11 network password.

User needs/requirements:

— Same as Scenario 2.3.2

Scenario 3.2.4: Command Center fails.

Steps:

a) Verify 4G/5G adequate signal strength.

b) Verify data availability according to user's contract.

c) Verify that the device activated data mode.

User needs/requirements:

— Same as Scenario 2.3.3

B.7.6.3 Use Case 3—Action #3

Command Center technicians monitor Jan's data.

Scenario 3.3.1: Happy path

Steps:

a) Command Center is in a secure restricted access location.

b) Command Center gives the technician access to the restricted location.

c) Command Center assigns the technician to monitor specific patients.

d) Technician monitors those patients.

e) Command Center technician can disable settings changes by home patient.

User needs/requirements:

— 3.3.1.01: The organization shall only authorize authenticated users to establish accounts in the portal application.

— 3.3.1.02: The organization shall only authorize authenticated users to only view results of specific patients.

— 3.3.1.03: Authenticated authorized users shall possess the ability to enable/disable the control panels of the remote devices.

Scenario 3.3.2: Technician connection to portal fails.

Steps:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

a) The Command Center notifies the Command Center technician that there are connection issues for the portal.

User needs/requirements:

— 3.3.2.01: Command Center shall notify remote user/caregiver if connection to a specific patient has failed.

— 3.3.2.02: Command Center shall notify remote user/caregiver if connection to all patients has failed.

— 3.3.2.03: Command Center shall notify remote user/caregiver if connection to any connected service has failed (such as monitoring system, AI service, etc.).

B.7.6.4 Use Case 3—Action #4

Command Center technician receives alerts from AI service.

Scenario 3.4.1: Happy path

Steps:

a) AI service receives data from the patient at home (either directly or via a feed from the Command Center portal).

b) Command Center portal receives status and alert feed from the AI service.

c) AI service receives settings commands from the Command Center portal.

d) Command Center portal advises Technician of an alert from the AI service via the Command Center portal.

User needs/requirements:

— Same as scenario 3.3.1

Scenario 3.4.2: Technician connection to portal fails.

Steps:

a) Verify the IEEE 802.11 network access point and SSID is available and has adequate signal strength.

b) Verify the IEEE 802.11 network password.

User needs/requirements:

— 1.2.2.01: Provide troubleshooting information in user guides.

B.7.6.5 Use Case 3—Action #5

Command Center technician modifies settings on remote devices in Jan's home.

Scenario 3.5.1: **Happy path**

Steps:

a) Command Center technician consults with Jan's physician.

b) The physician makes the decision to adjust the settings on the remote infusion pump.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

c) Command Center technician makes the change.

d) System acknowledges that change was queued.

e) The system makes the change to the settings of the remote infusion pump.

f) The system sends the change notification back to the Command Center technician.

User needs/requirements:

— 3.5.1.01: Controller/CIoT virtual device shall safely adjust the CIoT physical device settings.

— 3.5.1.02: CIoT virtual device shall indicate CIoT physical device change only after confirmation from actual CIoT physical device.

— 3.5.1.03: CIoT physical device shall respond to a command only if it trusts the source of the command.

Scenario 3.5.2: Physician cannot adjust the settings on the controller.

Steps:

a) The doctor decides to adjust settings on the controller.

b) The doctor accesses the portal and the patient's account.

c) Doctor requests change at the portal.

d) Request fails.

User needs/requirements:

— Same as Scenario 2.8.2

Scenario 3.5.3: Hacker breaks into portal and attempts to adjust settings on the patient's CIoT physical device.

Steps:

a) Unauthorized user gains access to the Command Center portal.

b) Unauthorized user changes settings on Jan's home monitor.

c) Command Center informs technician of any settings changes to their patients.

User needs/requirements:

— 3.5.3.01: System shall notify user of any settings changes not made by them.

B.7.6.6 Use Case 3—Action #6

Command Center technician alerts emergency services.

Scenario 3.6.1: Happy path

Steps:

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

a) Command Center alerts technician of a serious condition.

b) Command Center technician consults with physician on duty.

c) The physician decides to notify EMS to transport Jan to the hospital.

d) Command Center technician contacts EMS

User needs/requirements:

— Same as Scenario 2.8.3.

B.7.6.7 Use Case 3—Action #7

Jan is discharged from home health monitoring.

Scenario 3.7.1: Happy path

Steps:

a) Command Center alerts Command Center technician of a serious condition.

b) Command Center technician consults with physician on duty.

c) The physician decides to notify EMS to transport Jan to the hospital.

d) Command Center technician contacts EMS.

User needs/requirements:

— 3.7.1.01: The manufacturer shall provide detailed instructions concerning the deprovisioning of CIoT physical devices.

— 3.7.1.02: The manufacturer shall provide detailed instructions concerning deprovisioning of aggregator/gateways.

B.8 Use Case 4—Home-to-Hospital

B.8.1 Use case description

A patient is at home (or another non-traditional remote care environment) where the hospital actively monitors them (see Hospital @Home Use Case 3). The patient's condition deteriorates, and the hospital needs to transfer them back for more intensive care and therapy. The patient brings with them some of the medical devices that were being used in the home environment.

B.8.2 Use case narrative

Pauline has been at home for isolation and remote monitoring as she recovers from COVID-19. The technician noticed that their SpO2 had dropped below 90% and their glucose levels were climbing, so their care team decided to have them return to the hospital (via ambulance) for more intensive monitoring and therapy.

The hospital admits Pauline to an ICU bed. The hospital staff connects Pauline to a patient monitor that acquires their electrocardiogram (ECG), blood pressure, temperature, and SpO2. This data also appears at the monitoring central station and is forwarded to the hospital EMR system. Pauline has diabetes and wears

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

a CGM, which now connects to the hospital infrastructure. It also appears at the monitoring central station and in the hospital EMR.

Unfortunately, Pauline's condition deteriorates to the point where the hospital places them on a ventilator. The ventilator data will also appear at the Central Station and in the hospital EMR. (See Figure B.12 and Figure B.13.)

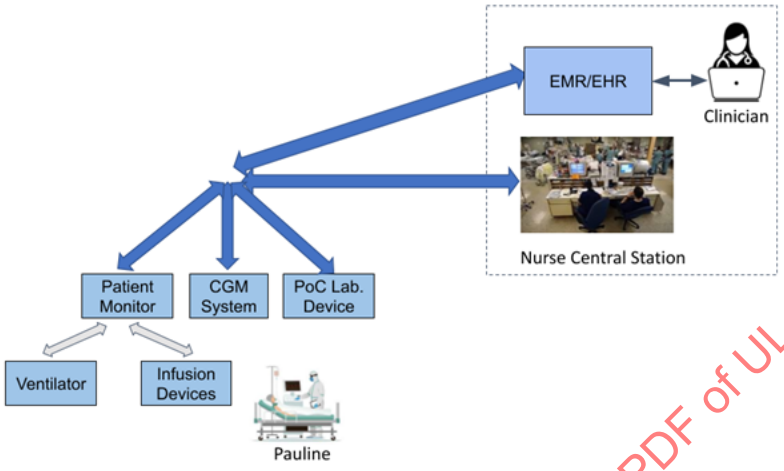

Figure B.12—Use Case 4—Home-to-Hospital—User View

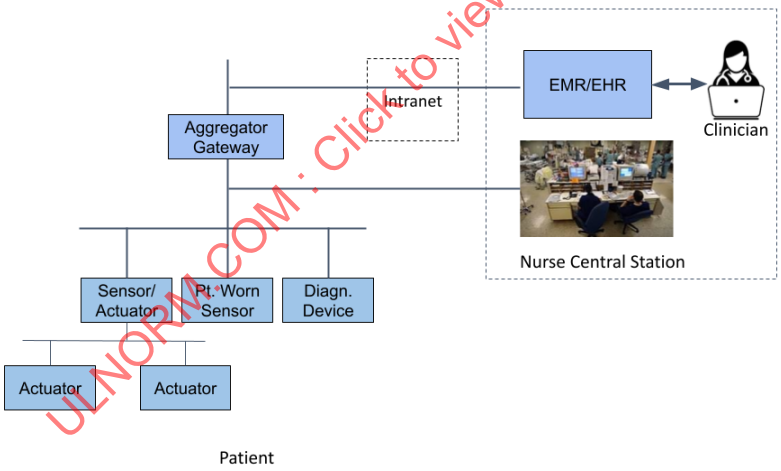

Figure B.13—Use Case 4—Home-to-Hospital—Technical View

B.8.3 Pre-conditions

— None

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.8.4 Use case actions

a) Connect ICU sensors/actuators/devices to Nursing Central Station (Application).
b) Connect patient worn sensor (from home) to Nursing Central Station (Application) directly.
c) Connect patient worn sensor (from home) to Nursing Central Station (Application) indirectly.
d) Nurses at Nursing Central Station monitor Pauline's results.
e) Connect ICU devices to aggregator/gateway.
f) Connect aggregator/gateway to EMR/EHR

B.8.5 Actors and stakeholders

Actors:

— Pauline, the patient
— Nurse (at Central Station)
— Clinician (using EMR)

Stakeholders:

— Payor
— Manufacturers
— Hospital

NOTE—User Needs/Requirements are in italics if stated in a previous scenario or use case.

B.8.6 Use Case 4—Details

B.8.6.1 Use Case 4—Action #1

Connect ICU sensors/actuators/devices to Nursing Central Station (Application).

Scenario 4.1.1: Happy path

Steps:

a) Connect device(s) to the appropriate hospital network (wired or wireless).
b) Enter the device location into the device(s) if possible.
c) Associate device(s) with Nursing Central using device demographics (Device ID, Model, Serial Number, etc.) or device location (Bed, Room, Care Unit) into aggregator.
d) Verify proper connectivity between device(s) and Central Station.
e) Transfer patient demographics from Nursing Station to device(s), if available.

User needs/requirements:

— 1.1.1.01: The solution provider shall make instructions for managing the CIoT physical device available to the user.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

- 1.1.1.02: The solution provider shall make available instructions for setup and use of the CIoT physical device system readily available.
- 1.1.1.03: CIoT physical devices shall assess whether the device can “trust” other CIoT physical devices and controller/CIoT virtual devices.
- 1.1.1.04: Communication between the controller/CIoT virtual device and CIoT physical device shall use Open standards-based communication methods for calibration.
- 1.1.1.05: CIoT physical devices shall use open and standards-based protocols for synchronization.
- 1.1.1.06: Solution providers shall use secure communication schemes.
- 1.1.1.07: Solution providers shall encrypt demographic data and other data at rest and in motion.
- 1.1.1.08: CIoT physical device shall communicate its globally unique device demographics/ID.
- 1.1.1.09: CIoT physical device shall support NFC or RFID or Bar-Code or label with device demographics/ID on CIoT physical device.
- 1.1.1.10: Controller/CIoT virtual device should support NFC or RFID or Bar-Code or label to enter device demographics/ID.
- 1.1.1.11: The CIoT physical device shall allow the user to validate CIoT physical device to controller/CIoT virtual device connectivity.
- 3.1.1.01: Communication between the controller/gateway and CIoT physical devices shall use open standards-based communication methods.
- 3.1.1.02: Communication between CIoT physical devices and other CIoT physical devices shall use open standards-based communication methods.
- 3.1.1.03: CIoT physical devices shall allow discovery and connectivity with other CIoT physical devices.
- 3.1.1.04: Controllers/gateways shall allow discovery and connectivity with other CIoT physical devices.
- 3.1.1.05: The CIoT physical device shall allow the user to validate CIoT physical device to CIoT physical device connectivity.
- 3.1.1.06: Manufacturers shall provide detailed instructions concerning the provisioning of devices.
- 4.1.1.01: CIoT virtual devices shall allow discovery and connectivity with other CIoT virtual devices.
- 4.1.1.02: CIoT virtual devices should allow the population of CIoT physical devices with patient demographics.
- 4.1.1.03: CIoT virtual devices should allow the population of CIoT virtual devices with patient demographics.
- 4.1.1.04: CIoT physical devices should have a mechanism for entering their locations in the hospital such as bed #, room #, care unit, hospital name, etc.
- 4.1.1.05: CIoT virtual devices should allow association with CIoT physical devices using the device ID and/or the device location.

Scenario 4.1.2: Device does not connect/communicate with applications (apps).

Steps:

a) Get an alert on application (app).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

b) Replace with different device (current manufacturer or other manufacturer).

c) Use wired link or alternative wireless link.

d) Continue to use the device without connectivity until resolution of issue.

User needs/requirements:

— Same as Scenario 1.1.2

Scenario 4.1.3: Application (app) does not "trust" device/sensor since it is counterfeit.

Steps:

a) Application (app) detects improper registration of one or more CIoT physical devices.

b) Application (app) does not operate with potentially counterfeit sensor(s).

c) Application (app) alerts user to counterfeit sensor(s).

User needs/requirements:

— Same as Scenario 1.1.5

Scenario 4.1.4: Application (app) does not "trust" a used device/sensor.

Steps:

a) Application (app) detects that the solution provider has not properly refurbished one or more CIoT physical devices.

b) Application (app) does not operate with potentially refurbished sensor(s).

c) Application (app) alerts user to improperly refurbished sensor(s).

User needs/requirements:

— Same as Scenario 1.1.6

Scenario 4.1.5: Application (app) does not "trust" device/sensor since it does not meet requirements.

Steps:

a) Application (app) detects that one or more CIoT physical devices does not meet requirements.

b) Application (app) does not operate with the CIoT physical devices.

c) Application (app) alerts users that the CIoT physical device cannot be used.

User needs/requirements:

— Same as Scenario 2.5.4

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.8.6.2 Use Case 4—Action #2

Connect patient worn sensor (from home) to Nursing Central Station (Application) directly.

Pre-condition—the patient's device can connect directly to the hospital network (typically via an IEEE 802.11 network), or it is connected to a controller (typically via an IEEE 802.15 network) which supports connectivity to the hospital network. Otherwise, see Use Case 4 Action #3.

Scenario 4.2.1: Happy path

Steps:

a) If possible, connect the device(s) to the appropriate hospital network (wired or wireless) directly or via its controller.

b) Enter the device location into the device(s) if possible.

c) Associate device(s) with Nursing Central using device demographics (device ID, model, serial number, etc.) or device location (bed, room, care unit) into aggregator.

d) Verify proper connectivity between device(s) and Central Station.

e) Transfer patient demographics from Nursing Station to device(s), if available.

User needs/requirements:

— Same as Scenario 4.1.1

Scenario 4.2.2: Device does not connect/communicate with applications (apps).

Steps:

a) Get an alert on application (app).

b) Replace with a different device (current manufacturer or other manufacturer).

c) Use wired link or alternative wireless link.

d) Continue to use the device without connectivity until the resolution of issue.

User needs/requirements:

— Same as Scenario 1.1.2

Scenario 4.2.3: Application (app) does not "trust" a counterfeit device/sensor.

Steps:

a) Application (app) detects improper registration of one or more CIoT physical devices.

b) Application (app) does not operate with potentially counterfeit sensor.

c) Application (app) alerts user of the potentially counterfeit sensor.

User needs/requirements:

— Same as Scenario 1.1.5.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 4.2.4: Application (app) does not "trust" a used device/sensor.

Steps:

a) Application (app) detects that the solution provider has not properly refurbished one or more CIoT physical devices.

b) Application (app) does not operate with potentially refurbished sensor(s).

c) Application (app) alerts user to improperly refurbished sensor(s).

User needs/requirements:

— Same as Scenario 1.1.6.

Scenario 4.2.5: Application (app) does not "trust" device/sensor since it does not meet requirements.

Steps:

a) Application (app) detects that one or more CIoT physical devices do not meet requirements.

b) Application (app) does not operate with the CIoT physical device(s).

c) Application (app) alerts users that the user cannot use the CIoT physical device(s).

User needs/requirements:

— Same as Scenario 2.5.4

B.8.6.3 Use Case 4—Action #3

Connect patient-worn sensor (from home) to Nursing Central Station (Application) indirectly.

Pre-condition—the patient's device communicates over a cellular connection to the cloud and via the cloud to a repository such as an EMR, EHR, portal, etc. The Nursing Central Station accesses the data from the portal.

Scenario 4.3.1: Happy path

Steps:

a) The device is already communicating with the portal, which has associated the device with a specific person.

b) Connect the Nursing Central Station to the portal.

c) Associate device(s) with Nursing Central using device demographics (device ID, model, serial number, etc.) and/or person associated with the device.

d) Verify proper connectivity between the portal and Central Station.

User needs/requirements:

— 4.3.1.01: CIoT virtual devices shall allow portal connectivity.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— 4.3.1.02: CIoT virtual devices shall use open standards-based communication to communicate with the portal.

— 4.3.1.03: CIoT virtual devices shall enable association with the correct patient based on patient demographics or device demographics.

Scenario 4.3.2: Portal does not connect/communicate with the application (app).

Steps:

a) Get alert on application (app).

b) Continue to use device without connectivity until resolution of issue.

User needs/requirements:

— Same as Scenario 1.1.2

Scenario 4.3.3: Application (app) does not "trust" portal.

Steps:

a) Application (app) alerts the user that it does not trust the portal due to the following:
   — Potential improper portal registration.
   — Portal does not support the application (app) requirements.
   — Additional steps as needed.

User needs/requirements:

— 4.3.3.01: CIoT virtual device shall verify the portal's identity.

— 4.3.3.02: CIoT virtual device shall verify that the portal meets the CIoT virtual device's requirements.

Scenario 4.3.4: Portal does not "trust" the application (app).

Steps:

a) Portal alerts the user that it does not trust the application (app) due to the following:
   — Potential improper application (app) registration.
   — Portal does not support the applications (apps) requirements.
   — Additional steps as needed.

User needs/requirements:

— 4.3.4.01: Portal shall verify CIoT virtual device's identity.

— 4.3.4.02: Portal shall verify that the CIoT virtual device meets the portal's requirements.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.8.6.4 Use Case 4—Action #4

Nurses at Nursing Central Station monitor Pauline's results.

Scenario 4.4.1: Happy path

Steps:

a) Nursing Central is in a secure restricted access location.
b) Managers give Caregivers access to the restricted location.
c) Managers assign Caregivers to monitor specific patients.
d) Caregivers monitor those patients.
e) Caregivers clear technical alerts, adjust technical alerts, and control device settings remotely as needed.
f) Caregivers go to the patient as needed.

User needs/requirements:

— 3.5.1.01: Controller/CIoT virtual device shall safely adjust the CIoT physical device settings.
— 3.5.1.02: CIoT virtual device shall indicate CIoT physical device change only after confirmation from the actual CIoT physical device.
— 3.5.1.03: CIoT physical device shall respond to a command only if it trusts the source of the command.
— 4.4.1.01: CIoT virtual devices can control settings on CIoT physical devices using open standards-based communication protocols.

Scenario 4.4.2: Caregiver cannot adjust the setting on the device.

Steps:

a) Caregivers decide to adjust settings on the device.
b) Caregiver requests change at the portal.
c) Request fails.

User needs/requirements:

— Same as Scenario 2.8.2.

Scenario 4.4.3: An unauthorized intruder breaks into Nursing Central and attempts to adjust settings on the patient's CIoT physical device.

Steps:

a) Unauthorized user gains access to the Nursing Central.
b) Unauthorized user changes settings on Pauline's monitor.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

— 4.4.3.01: Locate devices that have minimal access controls in restricted areas.

B.8.6.5 Use Case 4—Action #5

Connect ICU sensors/actuators/devices to gateway/aggregator.

NOTE—As depicted in the diagram EMR/EHR systems typically do not interface directly to CIoT physical devices but do it through intermediary gateways or aggregators, which take on the burden of converting protocols and combining and filtering the data streams, which manages the burden on the EMR/EHR. If the interface is direct, then this is like Use Case 4—Action #1.

Scenario 4.5.1: Happy path

Steps:

a) Configure an aggregator to associate with the device.
b) Verify connectivity between device(s) and aggregator.
c) User enters device demographics (device ID, model, serial number, etc.) into the aggregator.
d) IoT physical devices discover other local CIoT physical devices and connect to them as needed.

User needs/requirements:

— Same as Scenario 3.3.1.

Scenario 4.5.2: Devices do not connect/communicate with controller/gateway.

Steps:

a) Get alert on controller/gateway or smart device.
b) Replace with different device (current manufacturer or other manufacturer).
c) Use wired link or alternative wireless link.
d) Continue to use device without connectivity until resolution of issue.

User needs/requirements:

— Same as Scenario 1.1.2.

Scenario 4.5.3: Aggregator does not “trust” device/sensor since it is counterfeit.

Steps:

a) Controller/application (app) detects that one or more CIoT physical devices is not properly registered.
b) Controller/application (app) does not operate with potentially counterfeit sensor.
c) Controller/application (app) alerts the user that the sensor may be counterfeit.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

User needs/requirements:

— Same as Scenario 1.1.5.

Scenario 4.5.4: Aggregator does not "trust" a used device/sensor.

Steps:

a) Controller/application (app) detects inappropriate refurbishment of one or more CIoT physical devices/sensors.

b) Controller/application (app) does not operate with potentially refurbished device(s)/sensor(s).

c) Controller/application (app) alerts user to improperly refurbished device(s)/sensor(s).

User needs/requirements:

— Same as Scenario 1.1.6.

Scenario 4.5.5: Aggregator does not "trust" device/sensor since it does not meet requirements.

Steps:

a) Controller/application (app) detects that one or more CIoT physical devices/sensors does not meet requirements.

b) Controller/application (app) does not operate with the CIoT physical devices/sensors.

c) Controller/application (app) alerts users that the CIoT physical device(s)/sensor(s) cannot be used.

User needs/requirements:

— Same as Scenario 2.5.4

B.8.6.6 Use Case 4—Action #6

Connect aggregator/gateway to EMR/EHR

Scenario 4.6.1: Happy path

Steps:

a) Admin user logs into the EMR/EHR with credentials.

b) Admin user registers aggregator using Globally Unique Verifiable Device Identity.

c) Patient registers aggregator at Command Center and AI service using Device MAC address.

d) Aggregator communicates with the EHR/EMR.

e) Report results as needed to the EMR/HER.

User needs/requirements:

— Same as Scenario 3.2.1.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Scenario 4.6.2: Aggregator/gateway fails.

Steps:

a) User receives an alert from the EMR/EHR that the aggregator/gateway no longer works.

b) User substitutes current aggregator/gateway with another from the same or different manufacturer.

c) User follows steps from Scenario 4.2.1.

User needs/requirements:

— Same as Scenario 3.2.2

Scenario 4.6.4: EMR/EHR fails, or connection fails.

Steps:

a) Troubleshoot failure.

b) Aggregator will buffer data feed to the extent possible.

c) Aggregator will forward buffered data when connectivity resumes.

User needs/requirements:

— 4.6.4.01: Aggregator shall buffer data if it cannot be successfully exchanged with CIoT virtual device.

— 4.6.4.02: Aggregator shall forward buffered data after an interruption.

B.9 Other CIoT use cases

The list of other potential use cases is almost unlimited. The following subclauses list some that were considered. Some originated with other standardization efforts.

B.9.1 Use cases from AAMI 2700-1:2019 ICE (Integrated Clinical Environment)

— Safety interlocks

— Synchronization with safety interlock

— Process control (workflow)

— Smart alarm system

— Decision support

— Physiological Closed Loop Control (PCLC)

— Medical Device Plug-and-Play Interoperability (MD PnP)

B.9.2 Use cases from NITRD

The Networking and Information Technology Research and Development Program (NITRD) proposed some use cases as part of a medical device interoperability workshop.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Seamless changes of medical devices
— Capture of data and settings
— Supervisory control established
— Autonomous patient therapy
— Data flows through the continuum of care
— Capture of equipment configurations
— Black box recorder

B.9.3 Use cases from ONC/AHIC common device connectivity

The U.S. Department of Health and Human Services, Office of the National Coordinator/American Health Information Community (ONC/AHIC) as part of an analysis of needs regarding devices and their interfaces to EHR systems.

— Configure and register a device to communicate with an EHR.
— Associate patient ID and device information within an HER.
— Communicate measurement information to the EHR.
— Communicate device meta-data with each measurement to the EHR.
— Communicate measurement intervals, etc. within the EHR.
— Query the device or device intermediary for additional information.
— Gracefully recover from a lapse in EHR connectivity.
— Communicate standardized alert types to the EHR.
— Set limits and safeguards for device settings from the EHR to a device.
— Wirelessly communicate PoC device information from the device to a device intermediary or HER.

B.9.4 Remote surveillance (minutes to treat)

— “Home” to Physician Remote Consult to EHR (primary care visit, pregnancy visit, COPD evaluation, etc.)
— Remote monitoring/surveillance of vitals, activity status, IVD (in-vitro diagnostics) results, egress/barrier status, medication, device status, device configuration, etc.
— “Home” to Remote Monitoring Service/Command Center
— “Home” to Remote Monitoring and Therapy Control
    1) COPD patient monitoring
    2) Chronic Lymphocytic Leukemia
— Pacemaker remote monitoring/glucometer remote monitoring/implanted sensors/ingested sensors
— Remote device management
    1) Remote software/firmware update/version control
    2) Remote machine technical status monitoring
    3) Security monitoring and notification

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

4) Error logs, audit logs, access logs, etc. (forensics)

B.9.5 Remote monitoring (seconds to treat)

- Hospital device to Central Station/Command Center
- ICU to eICU (Hospital Remote Monitoring and Consulting) to EHR
- Isolation (Infection Control) ICU to "Next Door" Monitoring and Therapy Control
- In-hospital automatic respiratory monitoring and automated opioid infusion interlocks
- During transport (ambulance, helicopter)

B.9.6 Automated documentation of CIoT data

- Device tracking/Trace infected device/UDI
- Trusted systems: Device-to-device trust; device to application (app) trust; application (app) to application (app) trust
- Remote surgery
- Robotic surgery
- Integration of OR devices
- Remote audio/video communication to patient/caregiver (FB Portal, Google Nest, etc.)
- AI analysis of the video stream to assess patient comfort, patient-clinician interactions, patient rotation, and responsiveness of staff to nurse calls
- Robotic assistance; "pet robot;" therapeutic robots (for Autism, dementia, Alzheimer's, etc.)

B.9.7 Other use cases

- Monitoring activities of daily living
- Hospital @Home
  1) Pregnancy, infectious disease care (viral, bacterial, etc.), Rural healthcare, chronic disease care, capsule endoscopy
- Home dialysis
  1) Medtronic Launches the First and Only Pediatric and Neonatal Acute Dialysis Machine in the U.S.
  2) FDA Grants Marketing of New Device for Continuous Dialysis Therapy for use in Pediatric Patients with Certain Kidney Conditions
  3) Italian Nephrologists Invent Renal Replacement Machine for Neonates
  4) The story of the CARPEDIEM Machine
  5) Carpediem, by Claudio Ronco (Author), August 22, 2016
- Implanted CIoT device
  1) Deep brain stimulation
  2) Implanted pacemaker, defibrillator

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— Ingested CIoT device

1) "Ingestible Things are internet connected ingestible medical devices such as smart gut-sensing pills."

2) "The IEM Sensor activates when in contact with stomach fluid and communicates to a wearable sensor, called the MYCITE patch." (Otsuka America Pharmaceutical[29])

3) Internet of Ingestible Things

— Exoskeleton

— Prosthetic, like a patient's or provider's artificial limb or organ.

— Nurse call system using smart home contral devices.

— Failure modes affecting trust and identity systems:

1) Tamper detection: Device detects unauthorized physical tampering (someone not authorized breached its case or one of its modular components). Therefore, its API flags that it is not trustworthy. Is the "I've been tampered with" flag metadata a part of trust protocols?

2) Orphaned device: The manufacturer sets a status of end-of-life for a device, abandons it, or deactivate it, which has the effect of shutting down identity-related services so the device can no longer call "home." This affects the UID (issued to the device by the manufacturer), the ability of identity services to authenticate the device, and the ability of the device to authenticate other stakeholders.

3) Rugged identity: Our identity technologies assume continuous power, continuous local connectivity, continuous internet connectivity, continuous access to stakeholder identity processes. But the real-world needs devices to operate despite long latency, noisy, or interrupted communications (time, reliability, and integrity to the moon or Mars), and low power modes during power outages. This shows the required qualities of tolerance of disruption and recovery from interruption.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

[29] https://otsuka-us.com/discover/articles-1075

Copyright © 2024 IEEE and ULSE. All rights reserved.

Annex C

(informative)

Lead/Support/Consult (L/S/C) table

This annex shows how the user functional needs/requirements derived in the use cases map into various clauses of the standard.

This approach uses a modified RACI (Responsible, Accountable, Consulted, and Informed) table, simplified as a Lead/Support/Consult table. As the use case requirements were developed, it was not always clear which sub-group would address and provide the technical requirements for the issue. In addition, many User Needs/Requirements crossed group boundaries and it was important to identify which group had the responsibility of leading the development of the technical requirements.

NOTE—Though the word "shall" is used in the entries of the L/S/C table since the various functional needs were inherited from the use case analysis in Annex B. These are informative functional needs/requirements that drive the technical requirements detailed in the normative content of this standard in the clause/subclause(s) as specified by the L/S/C table. There are not requirements to conform to this standard.

The following table documents the results.

- Lead: Implies that the specified clause/subclause(s) of the standard will provide the main content for the topic/requirement.
- Support: Implies that the specified clause/subclause(s) of the standard may provide additional content for the topic/requirement.
- Consult: Implies that the specified clause/subclause(s) of the standard may have some minor supporting content.

Note that only one clause/subclause can be the "lead" for a requirement, though there can be multiple Support and/or consult.

The standard clauses were divided into vertical and horizontal groupings. The vertical oriented clauses of the standard can stand on their own and include the following:

- Tr Trust
- Id Identity
- Pri Privacy
- Pro Protection
- Saf Safety
- Sec Security
- AI/ML Artificial intelligence and machine learning

The horizontal oriented clauses of the standard touch all the vertical clauses and include the following:

- ISD Integrated Systems Design
- Int Interoperability

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

— V&V Verification and validation

— HF Human Factors

— OoS Out of Scope

Annex B defines the use cases and numbering:

a) Use Case 1—Connected Monitoring Device (CGM)

b) Use Case 2—Connected Therapy Device

1) Use Case 2a—Connected Therapy Device (AICD)

2) Use Case 2b—Connected Therapy Device (AID)

c) Use Case 3—Hospital @Home

d) Use Case 4—Home-to-Hospital

Line items in the LSC table (Table C.1) beginning with the number 1.x.x.x are correspondingly related to Use Case Number 1.x.x.x.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Table C.1—Lead/support/consult table

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
User Needs/Requirements from Use Case 1																
1.1.1.01: Instructions for handling the CIoT physical device shall be readily available to the user.													X		OoS	1
1.1.1.02: Instructions for clinical setup and use of the CIoT physical device system shall be readily available.													X		OoS	2
1.1.1.03: CIoT physical devices shall be able to assess whether the device can “trust” other CIoT devices in the CIoT system.	L	S	C	C	C	C	S		C	S	S				Tr	3
1.1.1.04: Communication between the controller/CIoT virtual device and CIoT physical device shall use open standards-based methods for calibration.		L			C	C			C	S	S				Id	4
1.1.1.05: Protocol for synchronizing the CIoT physical devices shall be open and standards-based.		C							L	S	S				ISD	5
1.1.1.06: Communication between the CIoT physical device and controller/CIoT virtual devices shall use a secure communications scheme.				C	C	L			C	S	C				Sec	6
1.1.1.07: ePHI and other data at rest shall be de-identified, pseudonymized, or anonymized wherever possible.			L		C	S			C	C	S				Pri	7
1.1.1.08: CIoT physical device shall communicate its globally unique verifiable device identifier.	S	L				C	C			S	S				Id	8
1.1.1.09: CIoT physical device shall support NFC or RFID or bar-code or label with device attributes/identity on the CIoT physical device.		S										L			HF	170
1.1.1.10: Controller/CIoT virtual device should support NFC or demographics/ID.		S					C					L			HF	171
1.1.1.11: User shall be able to validate CIoT physical device to controller/CIoT virtual device connectivity.							C				L	S			V&V	172
1.1.1.12: Instructions for technical setup and use of the CIoT physical device system shall be readily available.									C	C		L			HF	173
1.1.1.13: Demographic and other data at rest shall be “secure.”			L			S			C	C	S				Pri	308
1.1.2.01: System shall support the ability for a user to exchange CIoT physical devices from different manufacturers.		C			C	C			C	L	S				Int	9
1.1.2.02: System should support wired connections for transmission of data as a backup.		C			S	C			L	C	C				ISD	13

Table continues

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
1.1.2.03: Controller/CIoT virtual device shall continuously monitor quality of communications link with CIoT physical device.					L	C			C	S	C				Saf	14
1.1.2.04: Controller/CIoT virtual device shall notify user of communications connectivity issues.			C		L	C				S	S	C			Saf	15
1.1.2.05: Controller/CIoT virtual device shall support discernable technical alerts for blind users.												L			HF	174
1.1.2.06: Controller/CIoT virtual device shall support discernable technical alerts for hearing impaired users.												L			HF	175
1.1.2.07: Controller/CIoT virtual device shall alert if it detects an CIoT physical device/ with an incompatible protocol version.					C		C		C	L	C				Int	176
1.1.2.08: Controller/CIoT virtual device shall alert if it detects a CIoT physical device that does not meet its functional needs (e.g., inadequate accuracy).	L	S			C		C			S	C				Tr	177
1.1.2.09: Controller/CIoT virtual device shall alert and reject a CIoT physical device that does not support the same implemented security controls implemented.	S	S			C	L			C	C	C				Sec	11
1.1.2.10: Controller/CIoT virtual device shall alert and reject a CIoT physical device that it does not "trust."	L	S			C	C			C	S	C				Tr	12
1.1.3.01: System shall support limited but safe operation without complete setup of patient information.					L	C			C	S	S	C			Saf	19
1.1.4.01: Controller/CIoT virtual device shall detect CIoT physical device calibration failure and notify the user.					L				C	S	C	C			Saf	20
1.1.5.01: Controller/CIoT virtual device shall check that CIoT physical device can properly authenticate and authorizes for usage.	L	S		C	S	S			C	S					Tr	180
1.1.5.02: Controller/CIoT virtual device shall alert user if it suspects a counterfeit CIoT physical device.	S	L		C	C	C			C	C	C				Id	181
1.1.6.01: Controller/CIoT virtual device shall alert user if it suspects CIoT physical device is an unauthorized refurbished CIoT physical device.	S	L		C	C				C	C	C				Id	182
1.2.1.01: The CIoT physical device shall encrypt data in motion.			S		C	L			C	C	C				Sec	22
1.2.1.02: CIoT physical device should authenticate controller/CIoT virtual device.	C	S				L			C	S	C				Sec	185
1.2.1.03: Communication between controller/CIoT virtual device and CIoT physical device shall use seamless open interoperability.						C			S	L	C				Int	187
1.2.1.04: The user documentation shall disclose data communication capabilities of the CIoT physical device.						L			S	S					Sec	188
1.2.1.05: CIoT physical device shall communicate all its measurements, status, settings, and related meta-data.			C		S	C				L	S	C			Int	63
1.2.1.06: To improve effectiveness and performance, the CIoT physical device shall communicate all information that can be used to improve those.	S	C	L			C			C						Pri	115
1.2.2.01: If a communication disruption occurs, the CIoT physical device shall attempt to store all data until connection reestablishment.	C	C	S		L				C						Saf	16
1.2.2.02: The CIoT physical device shall secure any data stored on it.			S			L				C	C				Sec	17
1.2.2.03: If there is a communication disruption, the CIoT physical device shall attempt to store all data until connection reestablishment.	C	C	S			C			S	L					Int	189
1.2.2.04: The CIoT physical device shall delete any stored data after transmission to controller/CIoT virtual device unless otherwise needed by the CIoT physical device.			L								C				Pri	18
1.2.2.05: The manufacturer shall disclose the size and clinical capacity of the CIoT physical device data store in the user documentation.	C					C				C	C	L	X		OoS	110
1.2.3.01: Controller/CIoT virtual device shall support the adjustment of alert limits.					C				S	L		C	X		OoS	190

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
1.2.3.02: Controller/CIoT virtual device shall signal (visual, audible, or haptic) clinical out-of-range conditions.					C				C	S		L	X		OoS	191
1.2.3.03: Controller/CIoT virtual device shall allow the user to disable clinical alerts.					C					S		L			HF	192
1.2.4.01: Controller/CIoT virtual device shall detect out-of-range clinical results and notify user.					C				C	S		L	X		OoS	193
1.2.4.02: Controller/CIoT virtual device shall flag questionable clinical readings (via AI?).	C				C		C			S	C	L	X		OoS	194
1.3.5.01: The CIoT physical device shall communicate user allergy and irritation issues if available.					L							S			Saf	23
1.3.5.02: The manufacturer shall disclose disclaimers and warnings for the CIoT physical device and/or CIoT virtual device in the accompanying documentation.												L			HF	24
1.3.7.01: Return Instructions shall be accessible on the controller/app.												L			HF	25
1.3.7.02: CIoT physical devices should support geo-location reporting.									S	L					Int	309
1.3.7.03: CIoT physical device should support remote wipe/lock.					S	L			S	S	C				Sec	310
1.3.8.01: The manufacturer shall provide clear instructions concerning proper environments of use of the CIoT physical device.					C							L			HF	195
1.3.9.01: The link between the CIoT sensor and controller/app shall use secure communications.						L			S	S	C				Sec	196
1.3.9.02: The communications link between CIoT sensor and controller/CIoT virtual device shall protect against person-in-the-middle attacks.					C	L			S	S	C				Sec	197
1.3.9.03: The controller/CIoT virtual device should detect erratic CIoT sensor behavior.					L		S		S	S	C				Saf	198
1.3.9.04: The controller/CIoT virtual device and sensor shall support secure remote software and firmware updates.	C	C			L					S	C	S			Saf	199
1.3.9.05: The controller/CIoT virtual device and sensor shall support human intervention to control software and firmware updates.	C	C			S					S	C	L			HF	200
1.4.1.01: CIoT physical device shall communicate expiration date(s) to controller/CIoT virtual device.		L			C				S			C			Id	201
1.4.1.02: Controller shall alert user when the controller needs to exchange the CIoT sensor.		C			L		C		C	S	C	C			Saf	29
1.4.1.03: CIoT sensor shall communicate battery status to app/controller.		C			L				C	S	C	C			Saf	33
1.4.1.04: Controller/CIoT virtual device shall alert when it is time to charge or replace CIoT sensor battery.		C			L				C	S	C	C			Saf	34
1.4.1.05: CIoT physical device shall communicate its “attributes”/identity (ID, SW/FW version, etc.).		L			C	C			C	S	S				Id	30
1.4.1.06: CIoT physical device shall communicate internal error conditions to controller/CIoT virtual device and indicate whether the devices require replacement.		L			C	C			C	S	S				Id	202
1.4.1.07: Controller/CIoT virtual device shall communicate its “attributes”/identity (ID, SW/FW version, etc.).	C	L			S	C	C			S	C				Id	203
1.4.2.01: Controller/CIoT virtual device shall indicate data from an expired CIoT sensor as questionable on its display.	C										C	L			HF	204
1.4.2.02: Controller/CIoT virtual device shall indicate data from an expired CIoT sensor as questionable during communication.	C									L	C				Int	205
1.4.2.03: Controller/CIoT virtual device shall indicate data from a CIoT sensor requiring battery replacement as questionable on its display.											C	L			HF	208
1.4.2.04: Controller/CIoT virtual device shall indicate data from a CIoT physical device requiring battery replacement as questionable during communication.										L	C	C			Int	207

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
1.5.1.01: Controller/CIoT virtual device should connect to a device maintenance server.						S				L	C				Int	209
1.5.1.02: Controller/CIoT virtual device shall communicate securely with device maintenance server.						L			S	S	C				Sec	210
1.5.1.03: Controller/CIoT virtual device shall obtain CIoT physical device “attributes”/identity (ID, SW, FW, etc.).		L								S					Id	211
1.5.1.04: Controller/CIoT virtual device shall communicate controller/CIoT virtual device and CIoT physical device “attributes”/identity to server.		L				S				S					Id	212
1.5.1.05: Maintenance server shall detect out-of-date SW and FW.	S					L			S	S					Sec	213
1.5.1.06: Maintenance server shall download SW and FW updates to controller.	S				C	L			C	S	R				Sec	37
1.5.1.07: Controller/CIoT virtual device shall check authenticity and integrity of downloaded SW and FW.	S				S	L				S					Sec	214
1.5.1.08: Controller/CIoT virtual device shall communicate need for SW and/or FW update to user.		S				S				S		L			HF	31
1.5.1.09: Controller/CIoT virtual device shall update its SW/FW, on user acknowledgement.		C			C	S			C	L	S	S			Int	37
1.5.1.10: Controller/CIoT virtual device shall update the CIoT physical device SW and FW, on user acknowledgement.	C					C			C	L	S	S			Int	32
1.5.1.11: Upon completion, controller/CIoT virtual device shall provide SW/FW update message (success or failure)	C					C			C	L	S	S			Int	32
1.5.2.01 Controller shall continue to remind user to update SW/FW if required.					L	S				S		C			Int	377
1.5.3.01: CIoT physical device shall notify controller/CIoT virtual device of any SW and/or FW update failures.					L	S				S		C			Saf	216
1.5.3.02: CIoT physical device shall detect potential FW or SW compromises and notify controller/CIoT virtual device.	C				L					S		C			Saf	311
1.5.4.01: Controller/CIoT virtual device shall alert when it is time to charge or replace its battery.					L					S		S			Saf	217
1.5.5.01: Controller/CIoT virtual device shall notify user of any SW and/or FW update failures.	S					S				S		L			HF	319
1.5.5.02: Controller/CIoT virtual device shall notify device management server of any SW and/or FW update failures.	S					S			L	S		C			ISD	320
1.5.5.03: Controller/CIoT virtual device shall detect potential FW or SW compromises.	S					L				S					Sec	321
1.5.5.04: Controller/CIoT virtual device should maintain a device log that captures all messages exchanged with device management server.					S	S				S	L				V&V	322
1.5.5.05: Device management server should maintain a device log that captures all messages exchanged with the controller/CIoT virtual device.										S	L				V&V	323
1.5.5.06: Device log should not include any ePHI.			L			S									Pri	324
1.5.5.07: If the device log contains ePHI, then the device shall restrict access to it.			L			S				S					Pri	325
1.5.5.08: If the device log contains ePHI, the CIoT device should give the patient the opportunity to consent.			S			S						L			HF	326
1.5.5.09: The manufacturer shall disclose the size of the CIoT device log.												L			HF	331
1.5.5.10: If the SW and/or FW update fails, the CIoT device shall continue to operate with the previous SW and/or FW version.					S				L						ISD	377
User Needs/Requirements from Use Case 2																
2.1.1.01: User shall be able to validate proper system clinical operation.					S						S	L	X		OoS	218
2.2.1.01: Controller/CIoT virtual device shall check that the actuator properly authenticates.		L	S			S	S			C	S				Id	219

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
2.2.1.02: Controller/CIoT virtual device shall alert user if it suspects a counterfeit actuator.					S	S				S	C	L			HF	220
2.2.1.03: Seamless open interoperability between controller/CIoT virtual device and actuator.						S				L					Int	221
2.2.1.04: Secure communication between controller/CIoT virtual device and actuator.						L				S					Sec	222
2.2.1.05: Exchanged data shall include its provenance.	L					S				S					Tr	312
2.2.1.06: Manufacturers shall provide guidelines concerning data availability.	L					S				S					Tr	313
2.2.1.07: Manufacturers shall provide guidelines concerning data usability.	L					S				S					Tr	314
2.2.1.08: Manufacturers shall provide guidelines concerning data integrity.	L					S				S					Tr	315
2.2.5.01: User shall have the ability to exchange actuators from different manufacturers.										L	S				Int	224
2.2.5.02: Actuators shall store data during periods of non-connectivity.					L										Saf	225
2.2.5.03: Actuators shall communicate stored data to the controller/CIoT virtual device on connection.					S					L					Int	226
2.2.5.04: The actuator shall secure any data stored on it.			S			S									Sec	227
2.2.5.05: The actuator shall delete any data stored on it as soon as possible.			L			S									Pri	228
2.2.5.06: System shall operate safely without internet connectivity.	S				L	S			S	S					Saf	316
2.2.8.01: Guardrails/limits shall be inherent in any algorithms to limit actuator actions.					L						S	S			Saf	229
2.2.8.02: The device shall alert users to any clinical algorithm failure.						S						L	X		OoS	230
2.3.1.01: Controller shall support IEEE 802.11g/n/ac…if applicable.						S			L						ISD	231
2.3.1.02: Controller shall support WPA2 or greater authentication/encryption.						S			L						ISD	232
2.3.1.03: Controller shall support x.509 security certificates.	S					L				S					Sec	233
2.3.1.04: Controller shall support 4G/5G if applicable.									L						ISD	342
2.3.2.01: The manufacturer shall disclose the IEEE 802.11 network troubleshooting information in the accompanying documentation, if applicable.									S			L			HF	234
2.3.3.01: The manufacturer shall disclose cellular troubleshooting information in the accompanying documentation, if applicable.									S			L			HF	235
2.4.1.01: The portal shall authenticate patient to use it.	S	L				S			S	S					Id	236
2.4.1.02: The portal shall authorize Patient to use specific aspects of it.	L	S				S			S	S					Tr	237
2.4.1.03: Patient shall communicate securely with the portal.						L									Sec	238
2.4.1.04: Patient shall have a system-wide unique ID at minimum.	S	L				S			S	S					Id	239
2.4.1.05: Patient shall be able to associate CIoT physical devices with themselves.	L	S			S	S				S	C				Tr	240
2.4.1.06: Controller/CIoT virtual device has and shall communicate its Globally Unique Verifiable Device Identity.		L				S				S					Id	241
2.4.1.07: Controller/CIoT virtual device shall communicate its manufacturer model and serial number.		L				S				S					Id	243
2.4.1.08: Controller/CIoT virtual device shall communicate its MAC address.		L				S			S	S					Id	244
2.4.1.09: Controller/CIoT virtual device shall communicate securely with patient portal.	S					L				S	S				Sec	245
2.4.1.10: The device shall only communicate necessary information to the portal.			L			S				S					Pri	246
2.4.1.11: The device shall delete any unnecessary patient data after communication with the portal.			L												Pri	247

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
2.4.1.12: Patient shall be able to associate controller/CIoT virtual device with themselves.	L	S								S	S				Tr	158
2.5.1.01: Controller/gateway shall only communicate with a trusted portal.	L														Tr	248
2.5.1.02: Portal shall only communicate with a trusted controller/gateway.	L	S													Tr	249
2.5.1.03: Device shall accept and install x.509 security certificates.						L			S	S					Sec	250
2.5.4.01: Controller/CIoT virtual device shall check that CIoT physical device meets the requirements for its intended use.	L	C		C	S		S								Tr	251
2.5.4.02: Controller/CIoT virtual device shall notify the user if the CIoT physical device does not meet the requirements for its intended use and will not operate.	L	C			S							S			Tr	252
2.6.1.01: CIoT physical device and controller shall communicate securely and reliably.	S	C		C	S	L	S		S	S					Sec	253
2.6.1.02: Controller/CIoT virtual device and cloud/portal shall communicate securely and reliably.	S	C		C	S	L	S		S	S					Sec	255
2.6.1.03: CIoT physical device and controller shall support "Continuous" reporting (as often as every minute) of data from system to cloud/portal.						S				L	C				Int	256
2.6.4.01: The manufacturer shall incorporate malware protection.				C	C	L					C				Sec	257
2.6.4.02: The manufacturer shall incorporate safe coding practices.					S	L					C				Sec	258
2.6.4.03: The manufacturer shall conduct a complete threat analysis of system.					S	L					C				Sec	259
2.6.4.04: The manufacturer shall conduct vulnerability testing.				C	S	L				C	C				Sec	260
2.6.4.05: The manufacturer shall provide information to the user regarding safe and secure use of its products.	S				S	C						L			HF	261
2.6.5.01: The user shall be able to temporarily disable controller/CIoT virtual device communication to portal.				S	C	C				S		L			HF	262
2.6.5.02: The controller/CIoT virtual device shall alert the user if it has not been communicating to portal after a defined time.					S					L		S			Int	263
2.7.1.01: Authenticated caregivers shall be able to establish accounts in the portal application.	C	L	C	C		C						S			Id	264
2.7.1.02: Patients shall be able to authorize one or more caregivers to view results.	L	S	C	C								S			Tr	265
2.7.1.03: Authenticated caregivers shall be able to only view results of specific patients once authorized.	S	S	S	C		S						L			HF	266
2.8.1.01: The system shall allow the patient to acknowledge any remote change commands.	S				C					S		L			HF	267
2.8.1.02: The system shall advise the caregiver of the results of remote change commands (on the user interface) in a timely fashion.				C	C	C	C			L		S			Int	268
2.8.2.01: CIoT physical device shall reject commands if it cannot authenticate source.	L	C		C	C	C				S					Tr	269
2.8.2.02: CIoT physical device shall reject commands if source does not have adequate rights (trust?).	L	C		C	C	C	S			S					Tr	270
2.8.2.03: System shall allow portal application to distinguish between failure types and notify user.				C	C	C				L		S			Int	271
2.8.3.01: The system shall notify the user of any remote settings changes.					C	C				L		S			Int	272
User Needs/Requirements from Use Case 3																
3.1.1.01: Communication between the controller/gateway and CIoT physical devices shall use open standards-based communication.	S	S	S	S	S	S	C			L					Int	273
3.1.1.02: Communication between CIoT physical devices and other CIoT physical devices shall use open standards-based communication.	S	S	S	S	S	S	C			L					Int	274
3.1.1.03: CIoT physical devices shall be able to discover and connect with other CIoT physical devices.	C	C				C	C			L					Int	275

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
3.1.1.04: Controllers/gateways shall be able to discover and connect with other CIoT physical devices.	C	C				C	C			L					Int	276
3.1.1.05: User shall be able to validate CIoT physical device to CIoT physical device connectivity.						C					L				V&V	277
3.1.1.06: Manufacturers shall provide detailed instructions concerning the provisioning of devices.	S	S				C			L			S			ISD	327
3.1.1.07: Manufacturer shall provide detailed instructions concerning the provisioning of aggregators/gateways.																
3.1.1.08: The manufacturer shall provide detailed installation and troubleshooting instructions for system integrators to follow.									L			S			ISD	343
3.1.1.09: The manufacturer shall provide detailed installation and troubleshooting instructions for intended users (patient, caregiver, service provider, etc.) to follow.									L			S			ISD	344
3.1.1.10: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines from the manufacturer when provisioning the CIoT physical device.									L			S			ISD	345
3.1.1.11: System integrators shall follow detailed instructions.									L			S			ISD	346
3.1.1.12: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines for provisioning of aggregators/gateways.									L			S			ISD	347
3.1.1.13: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines for deprovisioning of aggregators/gateways.									S	L					Int	348
3.1.1.14: User (patient, caregiver, service provider, etc.) shall follow explicit guidelines from the manufacturer when deprovisioning the CIoT physical device.									S	L					Int	379
3.1.1.15: Manufacturers shall design the aggregator/gateway to enable remote provisioning, forensic data logging, and software updates.						S			S	L						380
3.2.1.01: Monitoring portal/CIoT virtual device shall authenticate aggregator/gateway.	L	C			C	C			S	S					Tr	278
3.2.1.02: Monitoring portal/CIoT virtual device shall authenticate all connected CIoT physical devices.	L	C			C	C			S	S					Tr	279
3.2.1.03: The link between the aggregator/gateway and monitoring portal/application shall use secure communications.				C	C	L				S					Sec	280
3.2.1.04: The manufacturer shall limit communications between the aggregator/gateway and monitoring portal/application to the minimal data set required for the application.			L			C									Pri	281
3.2.1.05: Communications between aggregator/gateway and monitoring portal/CIoT virtual device shall use open standards-based interoperable communications.						C				L					Int	282
3.2.1.06: AI service shall authenticate aggregator/gateway.	L	C				C	S		S	S					Tr	283
3.2.1.07: AI front-end shall authenticate all connected CIoT physical devices.	L	C				C	S		S	S					Tr	284
3.2.1.08: The manufacturer shall secure communications between aggregator/gateway and the AI service.						L	S			S					Sec	285
3.2.1.09: The manufacturer shall limit communications between aggregator/gateway and the AI service to the minimal data set required for the application.			L	C	C		S								Pri	286
3.2.1.10: Communications between aggregator/gateway and AI front-end shall use open standards-based interoperable communications.							S			L					Int	287
3.2.1.11: AI service shall authenticate monitoring portal.	L	C				S			S	S					Tr	288
3.2.1.12: Monitoring portal shall authenticate AI service.	L	C				S	S		S	S					Tr	289
3.2.1.13: The manufacturer shall provide for secure communications between monitoring portal/application and the AI service for all communication.				C	C	L	S			S					Sec	290

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
3.2.1.14: The manufacturer shall limit communications between the monitoring portal/application and the AI service to the minimal data set required for the application.			L			C	S								Pri	291
3.2.1.15: Communications between monitoring portal/CIoT virtual device and AI front-end shall use open standards-based interoperable communications.						C	S			L					Int	292
3.2.1.16: The manufacturer shall disclose whether the device contains AI/ML in the accompanying documentation.							L		C			S			AI	332
3.2.1.17: A device shall communicate whether it contains AI/ML	C						L		C	S					AI	333
3.2.2.01: Application shall detect failure (lack of communication) of aggregator/gateway.										L					Int	293
3.2.2.02: Application shall alert users of aggregator/gateway failures.										L		S			Int	294
3.2.2.03: Application and aggregator/gateway communicate using open standards-based interoperability protocols.										L					Int	295
3.3.1.01: The organization shall only authorize authenticated users to establish accounts in the portal application.	L	S													Tr	302
3.3.1.02: The organization shall only authorize authenticated users to only view results of specific patients.	S	S										L			HF	297
3.3.1.03: Authenticated authorized users shall possess the ability to enable/disable the control panels of the remote devices.										L		S			Int	298
3.3.2.01: Command Center shall notify remote user/caregiver if connection to a specific patient has failed.										L		S			Int	299
3.3.2.02: Command Center shall notify remote user/caregiver if connection to all patients has failed.										L		S			Int	300
3.3.2.03: Command Center shall notify remote user/caregiver if connection to any connected service has failed (such as monitoring system, AI service, etc.).										L		S			Int	301
3.5.1.01: Controller/CIoT virtual device shall safely adjust the CIoT physical device settings.	S	C			L					S					Saf	304
3.5.1.02: Controller/CIoT virtual device shall indicate CIoT physical device change only after confirmation from actual CIoT physical device.	S	C								L		S			Int	305
3.5.1.03: CIoT physical device shall only respond to a command only if it trusts the source of the command.	L	C								S					Tr	306
3.5.3.01: System shall notify user shall be notified of any settings changes not made by them.		S								L		S			Int	307
3.7.1.01: Manufacturer shall provide detailed instructions concerning deprovisioning of CIoT physical devices.	S	C		C	C	C			L			S			ISD	329
3.7.1.02: Manufacturer shall provide detailed instructions concerning deprovisioning of aggregator/gateways.	S	C		C	C	C			L			S			ISD	330
User Needs/Requirements from Use Case 4																
4.1.1.01: CIoT virtual devices shall allow discovery and connectivity with other CIoT virtual devices.									S	L					Int	352
4.1.1.02: CIoT virtual devices should allow population of CIoT physical devices with patient demographics.									S	L					Int	353
4.1.1.03: CIoT virtual devices should allow population of CIoT virtual devices with patient demographics.									S	L					Int	354
4.1.1.04: CIoT physical devices should have a mechanism for entering their locations in the hospital such as bed #, room #, care unit, hospital name, etc.			C						S	S		L			HF	355
4.1.1.05: CIoT virtual devices should allow association with CIoT physical devices using the device ID and/or the device location.		S							S	L					Int	356
4.3.1.01: CIoT virtual devices shall allow portal connectivity.									S	L					Int	357
4.3.1.02: CIoT virtual devices shall use open standards-based communication to communicate with the portal.									S	L					Int	358

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
4.3.1.03: CIoT virtual devices shall enable association with the correct patient based on patient demographics or device demographics.		S	S						S	L					Int	359
4.3.3.01: CIoT virtual device shall verify the portal's identity.		L							S	S					Id	360
4.3.3.02: CIoT virtual device shall verify that the portal meets the CIoT virtual device's requirements.	L								S	S					Tr	361
4.3.4.01: Portal shall verify CIoT virtual device's identity.		L							S	S					Id	362
4.3.4.02: Portal shall verify that CIoT virtual device meets the portal's requirements.									S	L					Int	363
4.4.1.01: CIoT virtual devices can control settings on CIoT physical devices using open standards-based communication protocols.									S	L					Int	364
4.4.3.01: Locate devices that have minimal access controls in restricted areas.					S	L									Sec	378
4.6.4.01: Aggregator shall buffer data if it cannot be successfully exchanged with CIoT virtual device.									S	L					Int	365
4.6.4.02: Aggregator shall forward buffered data after an interruption.									S	L					Int	366
User Needs/Requirements from other sources																
A.001 All CIoT devices should consider accommodations for individuals with disabling (visual, auditory, cognitive, mobility, etc.) conditions.			S							S		L			HF	167
A.002 All CIoT devices shall disclose their accommodations for individuals with disabling (visual, auditory, cognitive, mobility, etc.) conditions in the accompanying material.			S									L			HF	334
A.003 All CIoT devices should communicate known user disabling (visual, auditory, cognitive, mobility, etc.) conditions to consuming "trusted" CIoT devices.			C							S		L			HF	335
Authorized processes—safe listing.	C					L					C				Sec	336
A.004 A CIoT device shall disclose with which jurisdictional regulatory requirements it complies in the accompanying materials.	S											L			HF	337
A.005 A CIoT device should communicate with which jurisdictional regulatory requirements it complies to consuming CIoT devices.	S									L					Int	338
A.006 All CIoT devices should consider accommodations for regional cultural norms.												L			HF	339
A.007 All CIoT devices shall disclose their accommodations for regional cultural norms in the accompanying material.												L			HF	340
A.008 All CIoT devices should communicate user culture-based accommodations to data consumers.										L		S			Int	341
A.010 Shall disclose "all" personal information entered, captured, and generated in accompanying material.			L												Pri	349
A.011 Generate a plan to protect personal health information (PHI) based on the PHI assessment.			L			S									Pri	350
A.012 Conduct an assessment to establish lists of "all" personal health information (PHI) processing activities (GDPR).			L			S	S		S						Pri	139
A.013 Privacy notice shall be easily accessible via the user interface of the CIoT physical device and/or CIoT virtual device.			L									S			Pri	367
A.014 User should be able to disable part or all the results reporting from their CIoT physical device and/or CIoT virtual device.			L									S			Pri	368
A.015 Applications shall only acquire the minimal amount of data required to meet their intended use.			L							S		S			Pri	369
A.016 IoT physical devices shall limit the data exchanged to that requested by an CIoT virtual device or controller/gateway.			S							L					Int	370
A.017 Applications shall support management of data acquired via user consent.			S									L			HF	371
A.018 IoT physical devices shall not trust controller/gateway unless it provides proof of authorization (consent provided).	L	S							S						Tr	372

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
A.019 Manufacturer shall disclose the data communicated by the CIoT physical device and/or CIoT virtual device.												L			HF	373
A.020 Compliance with national safeguards—Ethics.	C		L	C											Pri	117
A.021 Data and device protection.				C		L				C	C				Sec	121
A.022 Data confidentiality.	C	C	L			C				C	C				Pri	82
A.023 Data minimization: Shall help ensure the personal data you are processing is adequate, relevant, and limited to the minimum data necessary to achieve the stated purpose.			L	C							C				Pri	112
A.024 Data ownership/controller: Who owns private health information? Who has the right to protect the data?			L	C		C				C	C				Pri	119
A.025 Data Processing Impact Assessment: A Data Protection Impact Assessment (DPIA) is a process to help identify and reduce the data protection risks of a project.			L			C					C				Pri	118
A.026 Data quality and accuracy: as it impacts privacy, i.e., if Patient A's medical results are accidentally stored to Patient B's record, Patient A's privacy may be compromised when Patient B sees the results.	C	C	L			S			C	C					Pri	123
A.027 Data Subject Notification about incidents affecting their data.		C	L			S									Pri	131
A.028 Defense in depth or multi step process shall be defined for verifying the identity of the device.	C	L	C	C	C	S			C	S	S				Id	56
A.029 Device and ecosystem access control in terms of hardware and software.		C	C			L	C		C	S					Sec	122
A.030 Efficacy of predictive analysis.	C				C		L			C	C				AI	87
A.031 The organization shall establish and implement a process to evaluate privacy risks when starting a new IT project or changing a business process—Define what "high risk" or "risk" means for the organization.			L			C				C	C	S			Pri	144
A.032 The organization shall establish a process to identify, prioritize and report for data incidents within 72 hours.		C	L			S	C		C			S			Pri	148
A.033 The organization shall establish technical measures to implement secure deletion of data upon the request of the data subject.			L			S			C	C	C	S			Pri	143
A.034 Exception mechanism, such as HITRUST for requesting exceptions to policy.	C	L	C	C	C	C			C	C	C				Id	53
A.035 Assurance identity of data (governance) coming from devices.	L	S			S					C	C				Tr	157
A.036 Human oversight—Algorithms.	S	S			C		L			C	C	C			AI	92
A.037 Identify appropriate organizational "measures" to mitigate risks and limit exposure.			L		S	C				C	C				Pri	146
A.038 Identify appropriate technical "measures" to mitigate risks and limit exposure.	S				L	C			C	C	C				Saf	145
A.039 Identify instances where personal information is stored for longer than necessary and delete unnecessary files.	C	S	L		C	S	C		C	C	C				Pri	142
A.040 Integrity and confidentiality: Shall establish reasonable safeguards to protect data CIA and protect security data.	S	C	L	S	C	S				C	C				Pri	113
A.041 Limitation of use—State intended use of data; Limit data collection to the minimum required.			L	C		S			S	S	S	S			Pri	165
A.042 Multiple layers of identity	C	L				C			C	C	C				Id	160
A.043 Privacy in health safety by default: Consider preserving privacy in health safety by default scenarios in devices. Failing Safely: what does fail safely concerning privacy look like? What is the most important? How to balance conflicting constraints. For example, if the device is in a state of failure with limited resources and it can either destroy the data and maintain privacy or maintain the data and risk privacy exposure. Which is best?			L	C	C				C	C	C				Pri	138
A.044 Privilege delegation shall be supported.	C	L	C	C	C	C	C			C	C				Id	57
A.045 Privileged Identity Management and Privileged Access Management.	S	L	C			C			S	S	C				Id	69

Table continues

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

L/S/C—Lead/Support/Consult	Tru	Id	Pri	Pro	Saf	Sec	AI		ISD	Int	V&V	HF	OoS		Lead	Req #
A.046 Purpose limitation—primary and secondary data usage.	C	C	C			L			C	C	C				Sec	111
A.047 Shall establish data subjects' rights—data access, amendment, erasure of inaccurate data, correction, completion, control over disclosure, sharing, etc.	C	C	L	C	C	S	S			C	C				Pri	114
A.048 There shall be a process for patients to register consumer-grade devices.	S	L		C	S	C				C	C				Id	47
A.049 System capabilities address professional users, and client users with disabling conditions.	C		C		C		C			S	S	L			HF	168
A.050 System components shall support Asset Tracking/Management.		L				C			C	C	C				Id	75
A.051 System objectives, assertions of trustworthiness, and corresponding zones of trust.	L			C					C	C	C				Tr	68
A.052 Systems/devices have been tested using mock data prior to making it available to real end-users.			C		C					S	L				V&V	129
A.053 Technical and data workflow.			C		C				C	L	S				Int	102
A.054 The need for independent system security audits has been considered.			C			L									Sec	127
A.055 TIPPSS labeling is transparent about the capabilities and purposes of any device.									L	C	C				ISD	51
A.056 Transmitting data about adverse reactions to devices or components for postmarket surveillance.					S				C	L	C				Int	72
A.057 Transparency—Be clear about the following: 1) Data collection practices 2) What data is being collected 3) How each data type/element will be used 4) With whom the data will be shared			L						C	C	C				Pri	164
A.058 Trusted Network—Endpoints.	C	C	C			C			C	S	S				Tr	103
A.059 User boundaries	S	C	L	C		C				C	C				Pri	108
A.060 Vendors can be rated on different elements such as: storage, security, etc.	C		C						L	C	C				ISD	162
A.061 Critical functionality/primary operating functions of the Device should be preserved as justified by risk management in the presence of SECURITY controls.	C				S	L									Sec	374
A.062 The device should support emergency override ("Break the Glass") provisioning (i.e., safety considerations override SECURITY considerations in certain cases that are rare and exceptional by definition).					S	L			C						Sec	375
A.063 The device shall have a well-defined method for managing potentially conflicting commands.					S	L			C						Sec	376

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Annex D

(informative)

Integrated systems design and the conceptual reference architecture

D.1 Introduction

The integrated systems design (ISD) approach provides meaningful guidance for the design, development, and deployment of connected healthcare solutions that function and safeguard human interests. The delivered value from CIoT devices and systems has the greatest potential when CIoT-based solutions facilitate companies of all sizes and all types of stakeholders, including clinical/medical service providers, patients, and researchers, to leverage CIoT devices and integrated systems safely and securely through independent as well as collaborative efforts. The CIoT healthcare ecosystem can benefit from this standard to enable integrated, collaborative, and complex systems that can more easily address many diverse health disparities and serve many more patients with important clinical functions and services. This can potentially increase the positive impact on public health and individual health beyond what individual companies, services, or technologies can achieve alone while delivering high-quality and high-reliability services.

Applications access and use the data transmitted by CIoT devices, components/elements, and systems in a growing number of ways with high variety. Data can be accessed in real time and might be episodic, periodic, continuous, or on-demand. These can include, and are not limited to, system processes such as recognition of device, patient, and provider for multiple purposes such as monitoring, diagnosis, and treatment. At another level, these include maintaining history, learning from the data at different scales, inferring causation, and predicting the future for various elements of the system. Other processes include alerting and ensuring non-functional requirements for improved quality of services. Monitoring, status, and prediction apply to devices, patients, and providers with the potential to be far-reaching in scope and scale. Likewise, with exponential data growth, the need exists for architectures and frameworks, such as TIPPSS, that can adapt to such a scale.

ULNORM.COM : Click to view the full PDF of UL 2933 2024

D.2 Context for integrated systems design for Clinical IoT with TIPPSS

Standards regarding ISD for CIoT systems that achieve TIPPSS attributes have the potential to unify globally connected healthcare and provide guidance related to simplifying devices and components, as well as interactions among components, while protecting humans, data, and devices. The ISD elements aim to provide tools and techniques for CIoT device and system manufacturers and deployment organizations to follow data, device, software, and interoperability processes, which can enable a safer and more secure, cohesive, and comprehensive system of systems. The goal is to enable the design and production of connected healthcare systems with TIPPSS built in, with ongoing monitoring for TIPPSS compliance. TIPPSS ISD can simplify the configuration of technologies into a CIoT system of systems (SoS) and ecosystem, enabling secure data sharing, transfer, interoperability, and improved relevant clinical communications, which can help improve medical treatment and healthcare outcomes from connected healthcare systems while protecting patient interests from which the TIPPSS attributes originated. ISD operates as a scaffold upon which stakeholders may construct the next generations of TIPPSS-compliant CIoT devices and systems and build in new desirable features.

ISD includes considerations for the integration of device and clinical observation, including determination of device and system status, safer transfer of data between CIoT systems, devices, and components, and processing of data at the appropriate point and location at a variety of scales and scopes. For an individual in a Hospital @Home situation, such as in Use Case 3 for example, detection of patient status or condition, critical vital signs and values, environmental conditions, and response to patient status locally and remotely,

Copyright © 2024 IEEE and ULSE. All rights reserved.

provides a means to incorporate the clinical dialog and performance into modeling for the standard to inform patient care. Conversely, for home-to-hospital situations, such as in Use Case 4, the patient brings some of the medical devices used in the home environment. Thus, home-to-hospital situations involve controlling and operating devices remotely, transferring and administering them in multiple settings, predicting and forecasting healthcare resource availability at multiple locations, scheduling needed services to be coordinated in multiple locations, predicting and forecasting the status of devices and systems, human status during the handoffs between care teams and/or facilities, and more.

D.3 Purpose and goal of integrated systems design

The purpose of this ISD subclause is to provide requirements and recommendations for the design, development, and deployment of integrated CIoT systems that are interoperable and adhere to the TIPPSS attributes, including the requirements that shall be satisfied for a CIoT device, system, or system-of-systems to conform to this standard. As the healthcare ecosystem continues to evolve and expand beyond traditional clinical settings utilizing advances in IoT technology, the human values associated with TIPPSS attributes are becoming increasingly important.

Table C.1 highlights thirty-nine interdependencies and overlaps between ISD requirements and individual TIPPSS requirements from the use cases and Human Factors perspectives.

Complementing the ISD approach, this annex (Annex D) provides a MVRA. The MVRA enables us to envision a robust, adaptive, reusable, and flexible architecture for the connected healthcare sector with a scaffold for hardware, software, services, and connectivity that facilitate the incorporation of TIPPSS attributes at the concept and design stage of connected healthcare systems and over the system lifecycle. The MVRA provides a theoretical vision for the overall CIoT system of systems, guiding device and data interoperability, device and data verification and validation, validation of identities of system devices, and validation of identities of humans, all while adhering to TIPPSS attributes. This system-of-systems approach strives to strike the best balance between individual best practices and federated optimization within the CIoT ecosystem. The ISD-MVRA illustrates how to view the standard in the presence of interoperable elements of the system of systems to apply all the TIPPSS requirements, ensuring each of the TIPPSS attributes is met. The ISD-MVRA mediates all TIPPSS requirements; when an interaction or conflict exists between multiple elements of the system of systems or between the TIPPSS requirements, the MVRA seeks to reconcile the conflict and find the best compromise.

D.4 Extensible and inclusive integrated systems design

The ISD approach is intended to be extensible. The suggestions and requirements put forth are only a starting point for the incorporation and implementation of burgeoning and future technologies, systems, and data requirements while maintaining TIPPSS attributes.

The CIoT ecosystem is fundamental in the expanding era of connected healthcare, involving enormous amounts of data, the usage of which can change over time. Since it is difficult for people to individually monitor, track, analyze, and interpret all the vast amounts of information in the connected healthcare ecosystem, the ISD of CIoT becomes truly relevant. The benefits of ISD for CIoT with TIPPSS include harmonization and interoperability of elements of the system, data, and human factors to provide the most value in a wide and diverse clinical ecosystem. Safer and effective leveraging of data, in large volumes and across populations, can improve insights to enable improved quality of healthcare.

ISD defines a wider set of user and stakeholder requirements to meet the needs of diversity and inclusion. Clinical ecosystems involve individuals with varying needs, including not only healthy athletes, but also people with temporary or chronic frailty or health challenges. People might have different abilities related to hearing, vision, mobility, cognition, and other attributes. It is challenging to be entirely inclusive, accommodate all needs, and reach all audiences. There is also a need to address cultural, linguistic, and other

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

facets of diversity. Envisioning CIoT systems that accommodate inclusion, diversity, and multimodal human factors at inception and into the future, enabled by an extensible TIPPSS standard, is part of the ISD approach.

D.5 Overview of the reference architecture (RA)

The CIoT reference architecture for ISD was developed considering a number of existing Reference Architectures (RAs) from related fields. The Open Group Architecture Framework (TOGAF), S3 Reference Architecture for business-driven service-oriented architecture (SOA), and Homecare Architecture for health smart homes laid the foundation. Additional complementary factors/layers were included to address interoperability, TIPPSS attributes, healthcare information architectures, data-driven healthcare and system failure predictions, and international healthcare policies and regulations. ArchiMate reference framework was used to develop the MVRA depicted in Figure D.1 and described herein.

A simple 2D projection of the MVRA presents the requirements in alignment with the functional layers of a conceptual RA (repeated as Figure D.2) for CIoT with TIPPSS, comprised of five key layers, the SQIRT Layer, and two upper-level, system-wide layers, Information Architecture Layer and Governance & Policies Layer, that interact with all other layers of the MVRA.

The five key layers, some corresponding to similar layers in the TOGAF Framework, include the following:

a) Context Layer
b) Technology Layer, as in TOGAF
c) Application Services Layer, as in TOGAF
d) Healthcare Workflow Services Layer, similar to Business Services in TOGAF
e) End-user Services (EUS) Layer

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

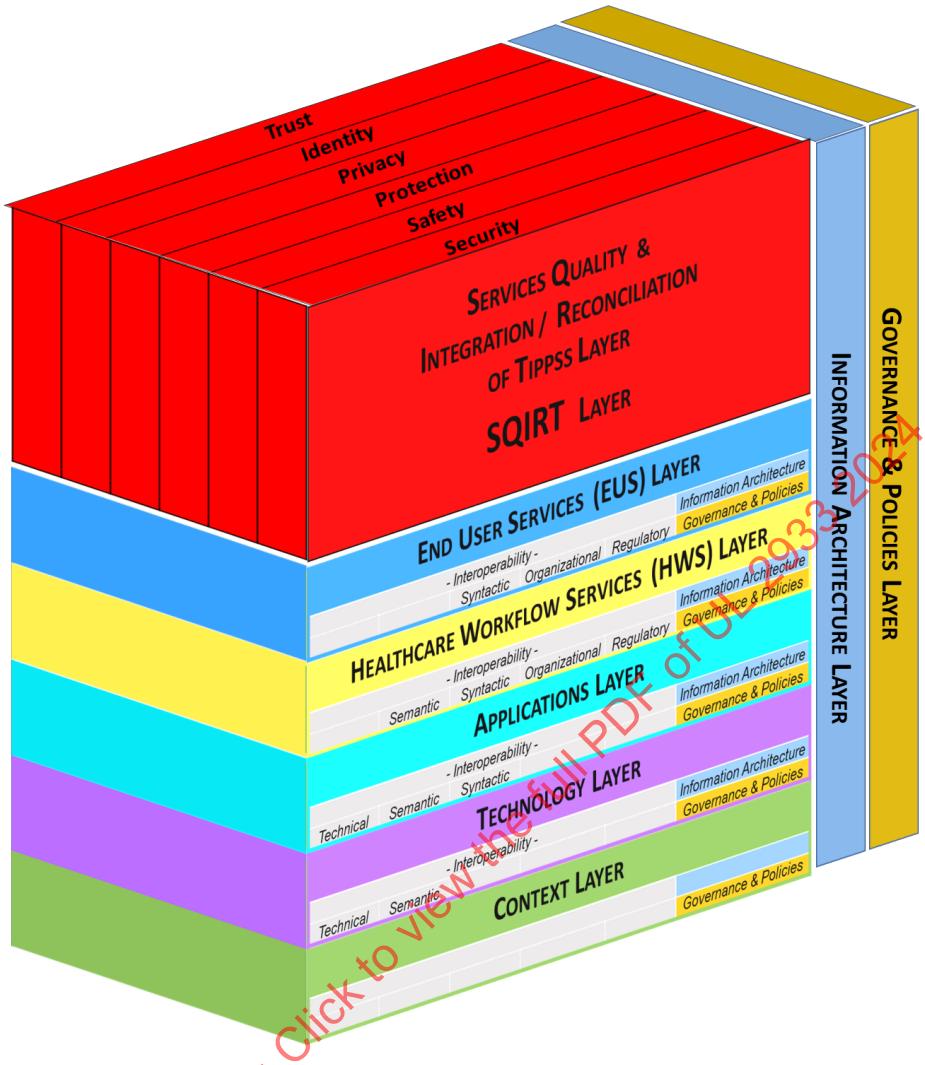

Figure D.1—3D conceptual view of MVRA for integrated CIoT System with TIPPSS

A SQIRT Layer (shown in the upper left section of Figure D.1) contains six sub-layers corresponding to each of the TIPPSS attributes to be achieved. Each TIPPSS attribute interacts with and operates on the five key layers, each of which contains one or more of the seven operational design requirements. The SQIRT Layer also interacts with and obtains information and instructions from two system-wide layers—the Information Architecture Layer and the Governance & Policies Layer. The SQIRT Layer helps ensure that all non-functional requirements, the TIPPSS attributes, are satisfied across all RA layers representing the integrated system. The SQIRT Layer manages all interoperability and data/device TIPPSS attributes to be achieved, and coordinates processes and communication between the five key layers and the Information Architecture Layer and Governance & Policies Layer. It also helps ensure the optimization of TIPPSS when conflicts exist between one or more TIPPSS attributes or requirements.

In addition, as shown in the right section of Figure D.1, an Information Architecture Layer (as in TOGAF) and a Governance & Policies Layer (as in S3) wrap the entire system and interact with all layers at the system level (back end) providing standards, healthcare plans, and governing policies and plans for operational integration of the Integrated CIoT System. These two system-wide layers also act on devices, applications, and services (within each of the five key layers).

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.

Finally, as shown in Figure D.2, the five key layers of the RA integrate operational design requirements related to interoperability, information architecture, and governance and policies. Each of the five key layers contains at least one of the operational design requirements listed in Figure D.3. Table D.1 defines each operational requirement.

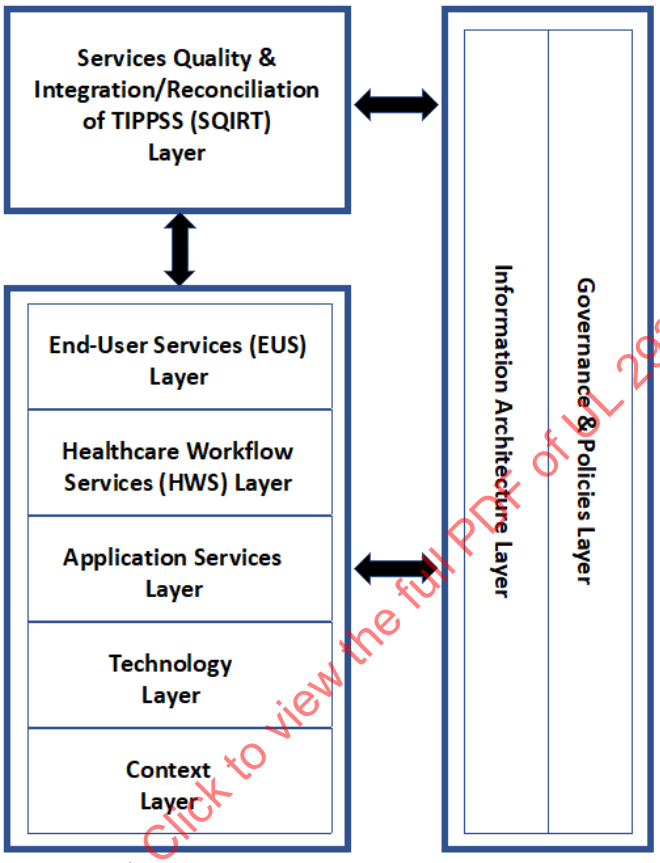

Figure D.2—Conceptual view of MVRA for integrated CIoT system with TIPPSS

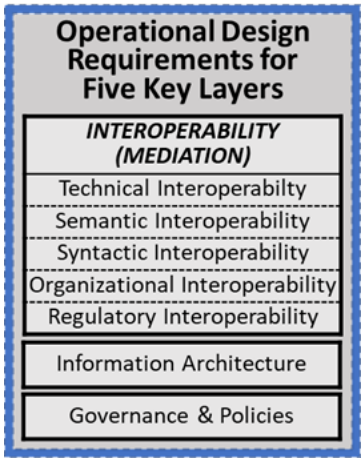

Figure D.3—Interoperability, information architecture, and governance and policies operational design requirements for five key layers

ULNORM.COM : Click to view the full PDF of UL 2933 2024

Copyright © 2024 IEEE and ULSE. All rights reserved.