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

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

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

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:

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

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

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

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

[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.

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.

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).

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/.

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.

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.

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

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

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.

Figure 1—TIPPSS

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.

Contents

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

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.

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.

[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.

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]

[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.

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

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.

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.

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.

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)

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

— 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.

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

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.

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.

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]

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

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

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

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

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

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

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.

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.

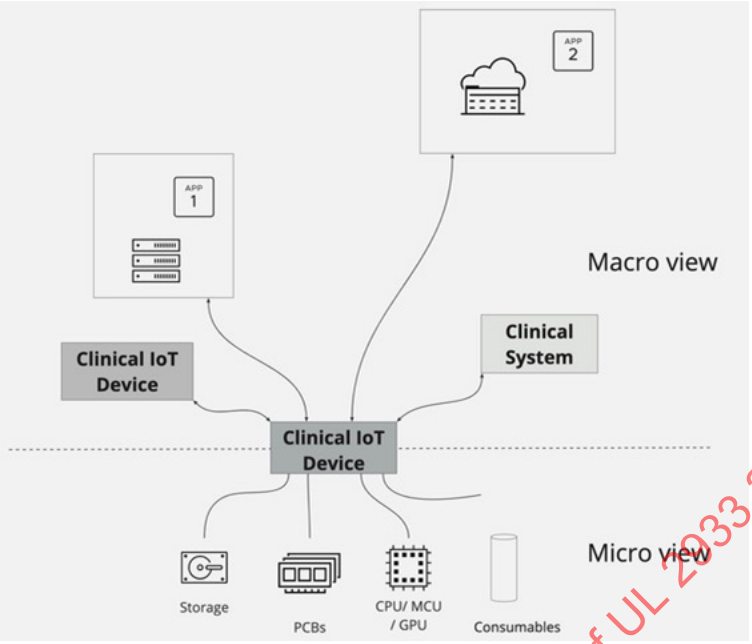

Figure 2—CIoT device in context

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.

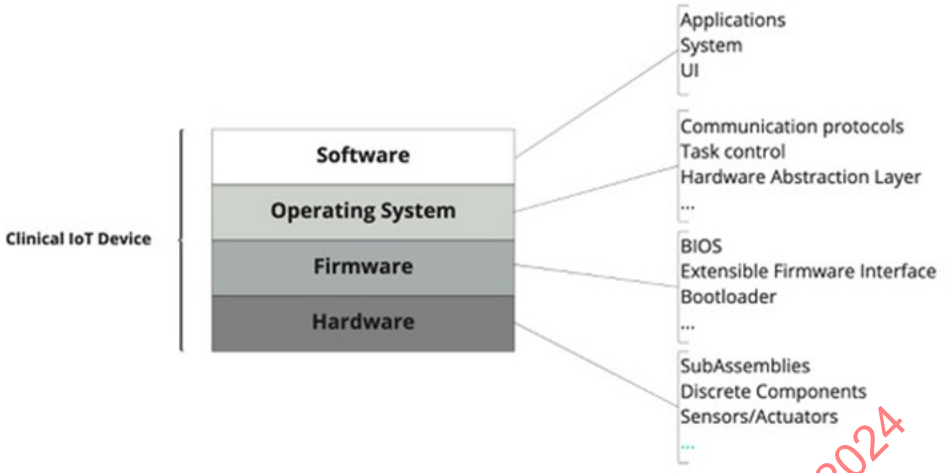

Figure 3—Logical CIoT device layers

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.

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.

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.

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.

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.

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.

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].

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.

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.

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)

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:

— 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.

— 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.

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).

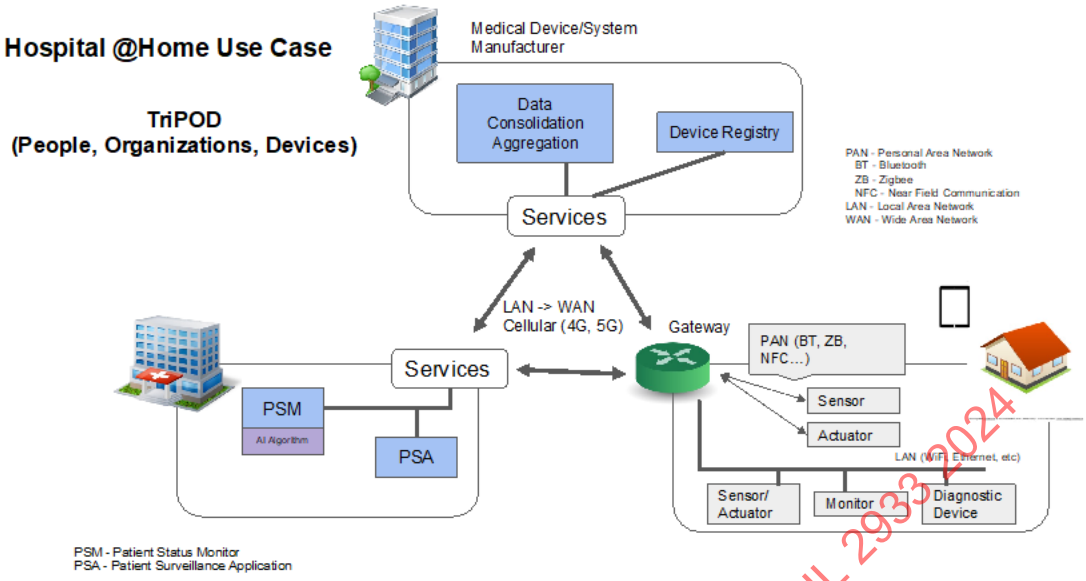

Figure 4—Trust and identity interactions of people, organizations, and devices in the CIoT Hospital @Home use case

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.

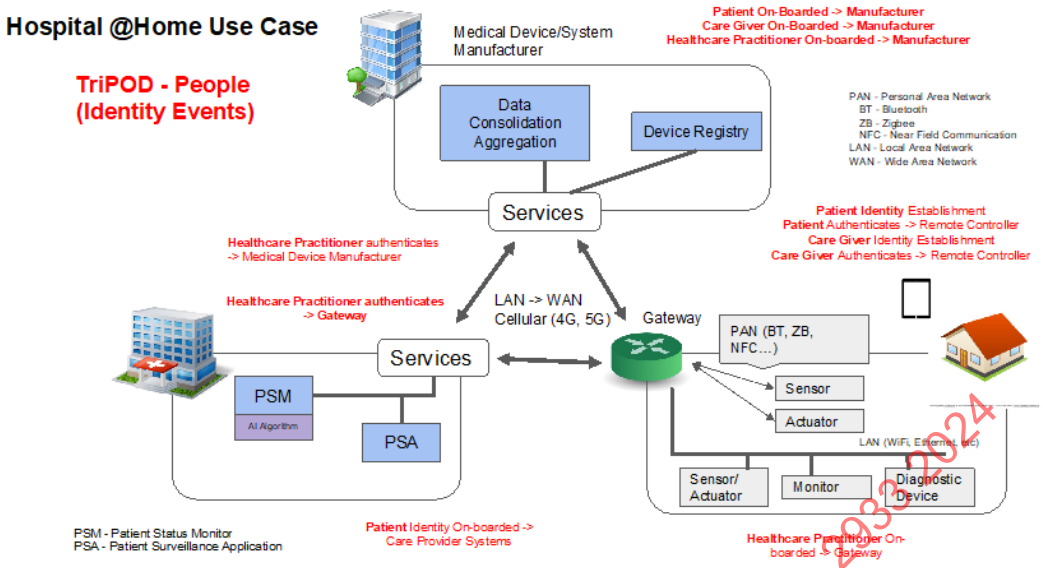

Figure 5—Trust and identity events of people in the "Hospital @Home" use case

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.

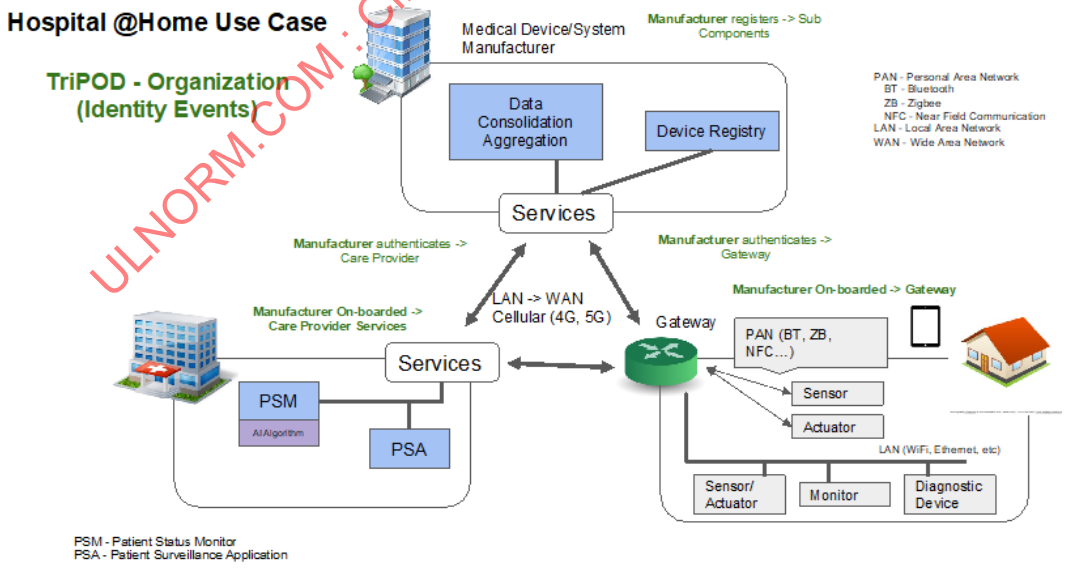

Figure 6—Trust and identity events of organizations in the "Hospital @Home" use case

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.

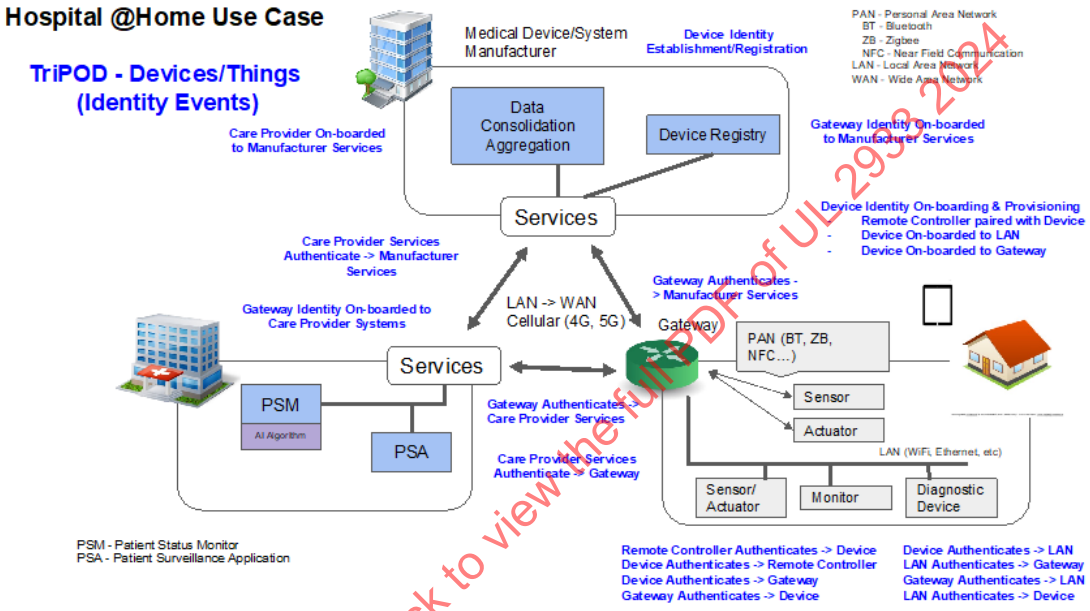

Figure 7—Trust and identity events of devices in the "Hospital @Home" use case

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.