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

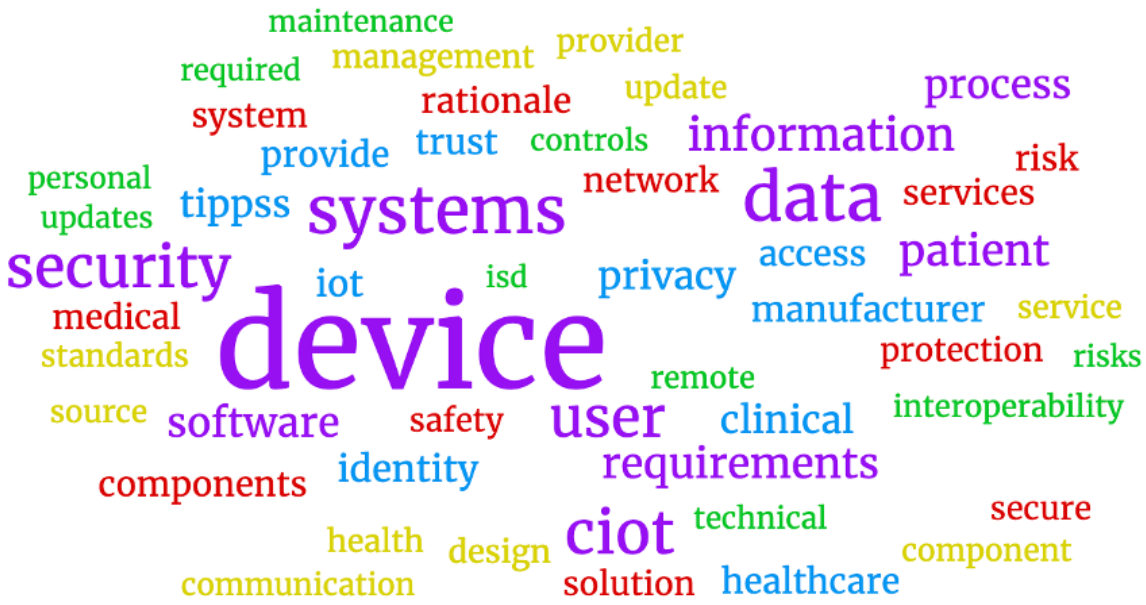
Copyright © 2024 by The Institute of Electrical and Electronics Engineers, Inc.
Three Park Avenue
New York, New York 10016-5997, USA

All rights reserved.

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

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

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



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

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

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

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

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

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

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

Commitments for amendments

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

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

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

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

Copyrights

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

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

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

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

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

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

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

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

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

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

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

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

Translations

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

Official statements

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

Comments on standards

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

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

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

Laws and regulations

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

Data privacy

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

Copyrights

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

Photocopies

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

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

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.

Copyright © 2024 IEEE and ULSE. All rights reserved.

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

IMPORTANT NOTICE

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

Participants

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

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

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

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

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

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

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

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

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

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

*Member Emeritus

Copyright © 2024 IEEE and ULSE. All rights reserved.

Introduction

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

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

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

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

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

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

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

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

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



Figure 1—TIPPSS

Copyright © 2024 IEEE and ULSE. All rights reserved.

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

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

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

Copyright © 2024 IEEE and ULSE. All rights reserved.

Contents

1. Overview 18
1.1 Scope 18
1.2 Purpose 18
1.3 Word usage 19

2. Normative references 19

3. Definitions, acronyms, and abbreviations 19
3.1 Definitions 19
3.1.1 IoT definitions 20
3.1.2 Clinical-related definitions 20
3.1.3 Clinical IoT (CIoT) related definitions 21
3.1.4 General definitions 21
3.2 Acronyms and abbreviations 32

4. Trust and identity 37
4.1 Introduction 37
4.2 Overview 38
4.3 Micro view 40
4.3.1 Discrete components 41
4.3.2 Subassembly 43
4.3.3 Device software 45
4.3.4 Final product 46
4.3.5 Manufacturer device registry 47
4.3.6 Decommissioning 49
4.4 Macro view—Inter-device and systems 50
4.4.1 User-managed software 53
4.4.2 Authentication 56
4.4.3 Identity 56
4.4.4 Context 56
4.4.5 Authorization 57
4.4.6 Accounting/Audit 57
4.4.7 Device onboarding 58
4.4.8 Provisioning 63
4.4.9 Deprovisioning 65

5. Privacy 66
5.1 Overview 66
5.2 Privacy requirements identification 67
5.2.1 Privacy requirements 68
5.2.2 Privacy requirements for Clinical IoT data and device interoperability 69
5.3 Privacy Impact Assessment 69
5.4 Premarket and postmarket privacy requirements 71
5.4.1 Premarket privacy requirements 71
5.4.2 Postmarket privacy requirements 73
5.5 Summary 74

6. Protection 74
6.1 Protection overview 74
6.2 Device pairing 75
6.3 Authentication 75
6.4 Access control 75

Copyright © 2024 IEEE and ULSE. All rights reserved.

6.5 Communication between components 76
6.5.1 Communications between device and sensor 76
6.5.2 Communications between device and aggregator/gateway 76
6.5.3 Communications between aggregator/gateway and backend 78
6.5.4 End-to-end encryption 78
6.6 Updates 78
6.6.1 Third-party and open-source components 79
6.6.2 Sensor 79
6.6.3 Smart device application 79
6.6.4 Backend/Gateway 79
6.6.5 Requirement for update independence 80
6.7 Backup 80
6.8 Requirements for replacements 80
6.9 Tamper-proofing and integrity 80
6.10 Resilience and fail-safe mode 81
6.10.1 Updates and alerts to trouble 81
6.10.2 Signal jamming and interference 82
6.10.3 Backup and restore capabilities 82
6.10.4 Data integrity and quality 83
6.11 Documentation and labeling 83
6.12 Decommissioning 84
6.12.1 Decommissioning legal and regulatory background 85
6.12.2 Decommissioning processes and practices 86

7. Safety 88
7.1 Safety overview 88
7.2 Mitigating safety risks 88
7.3 Quality assurance processes 89
7.4 Other safety risk considerations 90

8. Security 90
8.1 Security overview 90
8.2 Organizational cybersecurity foundation 91
8.2.1 Cybersecurity governance 92
8.2.2 Security as part of the quality management system 92
8.2.3 Secure Development Lifecycle 92
8.2.4 Risk-based approach 93
8.2.5 Establishing security requirements 94
8.2.6 Identified security requirements 94
8.3 Basic security principles 95
8.3.1 Developing a security baseline 96
8.3.2 Meeting a security baseline 96
8.3.3 Maintaining a security baseline 99
8.3.4 Software Bill of Materials (SBOM) 101
8.4 Communication security 102
8.4.1 Interoperability and security 102
8.4.2 Communicate securely 104
8.4.3 Communicate about security 105
8.4.4 Communication as a security risk 106
8.5 Processes, practices, principles, and controls 106
8.5.1 CIA triad 106
8.5.2 Confidentiality 107
8.5.3 Integrity 107
8.5.4 Availability 108
8.5.5 Preservation of authenticity 108

Copyright © 2024 IEEE and ULSE. All rights reserved.

8.6 Security assurance 108
8.7 Risk management and security 109
8.7.1 Risk management overview 109
8.7.2 Asset classification....111
8.7.3 Data classification 112
8.7.4 Vulnerabilities....112
8.7.5 Threats 113
8.7.6 Risk management cycle 113

9. Human factors and usability 114
9.1 Overview 114
9.2 Summary process for Usability Engineering 114
9.2.1 Prepare the technical use specification....114
9.2.2 Prepare hazard analysis related to technical user interface use cases and scenarios 115
9.2.3 Establish a technical user interface specification 115
9.2.4 Establish a technical user interface verification plan 115
9.2.5 Establish a technical user interface validation plan....116
9.2.6 Perform a technical user interface design, implementation, verification, and formative validation 116
9.2.7 Perform technical user interface summative evaluation/validation....116
9.3 Requirements for the technical aspects of the Clinical IoT device user interface 116
9.3.1 General—Human factors requirements....116
9.3.2 Accompanying documentation—Human factors requirements 117
9.3.3 Trust—Human factors requirements....118
9.3.4 Identity—Human factors requirements....118
9.3.5 Privacy—Human factors requirements 118
9.3.6 Safety—Human factors requirements 119
9.3.7 Security—Human factors requirements 120
9.3.8 Interoperability—Human factors requirements....120
9.3.9 Verification and validation—Human factors requirements 120

10. Integrated systems design (ISD)....121
10.1 ISD attributes and characteristics requirements....121
10.2 Documentation requirements....122
10.3 Research and development (R&D) and pre-production requirements 123
10.4 Postmarket requirements 124

11. CIoT reference architecture (RA)....124
11.1 Context Layer requirements 127
11.2 Technology Layer requirements 127
11.2.1 System software requirements 128
11.2.2 Technology Layer general requirements....128
11.2.3 Requirements associated with CIoT system hardware and firmware....129
11.3 Application Services Layer requirements 130
11.4 Healthcare Workflow Services (HWS) Layer requirements....131
11.5 End-User Services (EUS) Layer requirements 132
11.5.1 Patient 133
11.5.2 Home healthcare team....133
11.5.3 Healthcare provider....133
11.5.4 End User Services (EUS) Manager....133
11.6 Services quality and integration/reconciliation of TIPPSS (SQIRT) Layer requirements....136
11.6.1 SQIRT Manager requirements 136
11.6.2 Availability Manager requirements....137
11.6.3 TIPPSS Managers 138
11.6.4 Privacy Manager requirements 138

Copyright © 2024 IEEE and ULSE. All rights reserved.

11.6.5 Protection and Safety Manager requirements 138
11.6.6 Security Manager requirements 138
11.7 Information Architecture Layer requirements 139
11.8 Governance & Policies (G & P) Layer requirements 139
11.8.1 Requirements associated with interoperability and integration plans 140
11.8.2 Requirements associated with TIPPSS policies and plans 140
11.8.3 Requirements associated with system logs 140
11.9 Lifecycle design and management 141
11.9.1 CIoT device manufacturer lifecycle 142
11.9.2 CIoT device supply chain management 142
11.9.3 CIoT device maintenance lifecycle 143
11.9.4 CIoT device deployment organization lifecycle 143

Annex A (informative) Bibliography 145

Annex B (informative) Detailed sample use cases and derived functional needs 148
B.1 Introduction 148
B.2 Overview of the sample use cases 148
B.2.1 Connected monitoring device—Use Case 1 148
B.2.2 Connected therapy device—Use Case 2 149
B.2.3 Hospital @Home use case—Use Case 3 149
B.2.4 Home-to-Hospital use case—Use Case 4 149
B.3 Use case process 149
B.4 TIPPSS stakeholder roles 151
B.5 Use Case 1—Connected monitoring device 151
B.5.1 Use case description 151
B.5.2 Use case narrative 152
B.5.3 Use case actions 153
B.5.4 Actors and stakeholders 153
B.5.5 Use Case 1—Details 153
B.6 Use Case 2—Connected therapy device 163
B.6.1 Use Case 2a—Connected automated implanted cardioverter defibrillator (AICD) 164
B.6.2 Use Case 2b—Connected automated insulin delivery (AID) system 165
B.6.3 Use case actions 166
B.6.4 Actors and stakeholders 167
B.6.5 Use Case 2—Details 167
B.7 Use Case 3—Hospital @Home 178
B.7.1 Use case description 178
B.7.2 Use case narrative 178
B.7.3 Pre-conditions 179
B.7.4 Use case actions 179
B.7.5 Actors and stakeholders 179
B.7.6 Use Case 3—Details 180
B.8 Use Case 4—Home to Hospital 187
B.8.1 Use case description 187
B.8.2 Use case narrative 187
B.8.3 Pre-conditions 188
B.8.4 Use case actions 189
B.8.5 Actors and stakeholders 189
B.8.6 Use Case 4—Details 189
B.9 Other CIoT use cases 198
B.9.1 Use cases from AAMI 2700-1:2019 ICE (Integrated Clinical Environment) 198
B.9.2 Use cases from NITRD 198
B.9.3 Use cases from ONC/AHIC Common Device Connectivity 199
B.9.4 Remote surveillance (minutes to treat) 199

Copyright © 2024 IEEE and ULSE. All rights reserved.

B.9.5 Remote monitoring (seconds to treat) 200
B.9.6 Automated documentation of CIoT data 200
B.9.7 Other use cases 200

Annex C (informative) Lead/Support/Consult (L/S/C) table 202

Annex D (informative) Integrated systems design and the conceptual reference architecture 214
D.1 Introduction 214
D.2 Context for integrated systems design for Clinical IoT with TIPPSS 214
D.3 Purpose and goal of integrated systems design 215
D.4 Extensible and inclusive integrated systems design 215
D.5 Overview of the reference architecture (RA) 216
D.6 Application of the RA to the Hospital@Home Example use case 220

Annex E (informative) Overview of Privacy Frameworks 224
E.1 OECD—Fair Information Practices (FIPs) 224
E.2 EU—General Data Protection Regulation (GDPR) Privacy Principles 225
E.3 U.S. NIST—Privacy Framework 225
E.4 U.S. HIPAA—Privacy Rule 227
E.5 U.S. California—Consumer Privacy Act (CCPA) privacy principles 228
E.6 Australia—Privacy Principles (APP) 229
E.7 Canada—Personal Information Protection and Electronic Documents Act (PIPEDA) 230
E.8 International—ISO/IEC 29100 Privacy Principles 230
E.9 OECD—Council of Europe Convention, EU Data Protection Directive, and the Asia-Pacific Economic Cooperation (APEC) 231

Annex F (informative) Comparison of privacy regulations/guidance 232

Annex G (informative) Direct and indirect patient safety impact 234
G.1 Direct safety impact 234
G.1.1 Disruption of the clinical data flow 234
G.1.2 Disruption of patient engagement 234
G.1.3 Inability to use the clinical devices 235
G.1.4 Regulated devices 237
G.2 Indirect safety impact 237
G.2.1 Device monitoring systems (environmental) 237
G.2.2 Device monitoring systems (clinical) 238
G.2.3 DICOM data flows and interpretation 238
G.2.4 Clinical orders and e-prescribing 239
G.2.5 Device lifecycle management 239
G.3 Operational and business impact 240
G.3.1 Environmental monitoring 240
G.3.2 Disruption to workflow automation 241

Annex H (informative) Examples and rationale for ISD-derived requirements 243
H.1 Overview 243
H.2 Documentation requirements 243
H.3 Research and development (R&D) and pre-production requirements 248
H.4 Postmarket requirements 249
H.5 Context Layer requirements 250
H.6 Technology Layer requirements 250
H.6.1 System software requirements 250
H.6.2 Technology Layer general requirements 251
H.6.3 Requirements associated with CIoT system hardware & firmware 254
H.7 Application Services Layer requirements 257

Copyright © 2024 IEEE and ULSE. All rights reserved.

H.8 Healthcare Workflow Services (HWS) Layer requirements....258
H.9 End-User Services (EUS) Layer requirements....258
H.9.1 End-User Services (EUS) Manager requirements....258
H.9.2 End-User Services requirements....263
H.10 Services Quality and Integration/Reconciliation of TIPPSS (SQIRT) Layer requirements....265
H.10.1 SQIRT Manager requirements....265
H.10.2 Availability Manager requirements....268
H.10.3 TIPPSS Managers....268
H.10.4 Privacy Manager requirements....269
H.10.5 Protection and Safety Manager requirements....269
H.10.6 Security Manager requirements....269
H.11 Information Architecture Layer requirements....270
H.12 Governance & Policies (G & P) Layer requirements....270
H.12.1 Requirements associated with interoperability and integration plans....270
H.12.2 Requirements associated with TIPPSS policies and plans....271
H.12.3 Requirements associated with system logs....271

Copyright © 2024 IEEE and ULSE. All rights reserved.

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

1. Overview

1.1 Scope

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

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

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

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

1.2 Purpose

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

[8] Published by HL7 International.

Copyright © 2024 IEEE and ULSE. All rights reserved.

1.3 Word usage

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

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

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

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

2. Normative references

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

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

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

3. Definitions, acronyms, and abbreviations

3.1 Definitions

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

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

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

Copyright © 2024 IEEE and ULSE. All rights reserved.