Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain

Trademarks and Disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

The Institute of Electrical and Electronics Engineers, Inc.

3 Park Avenue, New York, NY 10016-5997, USA

Notice and Disclaimer of Liability
Concerning the Use of IEEE-SA Documents

This publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of this activity that produced this Work. IEEE-SA expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE-SA disclaim any and all conditions relating to: results; and workmanlike effort. This document is supplied "AS IS" and "WITH ALL FAULTS."

Although the members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE-SA OR THE AUTHORS OF THIS REPORT BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF 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 USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder.

This Work is published with the understanding that IEEE and the authors of this report are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain

Authored by

IEEE-Standards Association Pre-Standards Workstream Team for Clinical IoT Data Validation and Interoperability with Blockchain, 2018-2019

Keywords: blockchain, clinical IoT, connected Healthcare, cybersecurity, identity, IEEE, Internet of Medical Things, Internet of Things, IoMT, IoT, P2733, privacy, protection, safety, security, standards, TIPPSS, trust

ABSTRACT

The IEEE-Standards Association (IEEE-SA) pre-standards workstream for Clinical Internet of Things (IoT) data validation and interoperability with blockchain was initiated to determine if a viable standards framework could be established to enable the validation of data generated from a clinical-grade IoT device and shared through the interoperability of blockchain technology. Participants in the workstream were gathered from an IEEE-SA workshop held at Johns Hopkins University in Rockville, Maryland in April 2018, and grew to include their network of healthcare and HealthIT ecosystem players, as well as participants in prior IEEE-SA efforts in related areas. The workstream commenced in August 2018 and completed in February 2019. Participants in this pre-standards workstream who are the authors of this paper are listed in Appendix A.

The pre-standards workstream led to the recommendation of the development of an IEEE-SA Standards effort on Clinical IoT data and device interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety and Security—in connected healthcare to improve data sharing and healthcare outcomes. The pre-standards workstream team decided that blockchain is not necessary for clinical IoT data and device interoperability and validation, nor does it necessarily meet the robust TIPPSS needs in connected healthcare. The workstream recommendation includes a draft TIPPSS Architectural Framework for Clinical IoT data validation & interoperability, which could include digital ledger technology but does not need to do so. The resulting IEEE Standards Association P2733 working group to develop a standard for Clinical IoT Data and Device Interoperability with TIPPSS kick off meeting is scheduled for July 17, 2019, sponsored by the IEEE-SA Engineering in Medicine and Biology Society (EMBS).

The contents of this report are listed in Table 1.

Table 1. Topical outline of information covered in this report

Section	***Topic***
I	Executive Overview and Recommendations
II	Definitions related to Clinical IoT and blockchain
III	Related standards efforts for collaboration
IV	TIPPSS—Trust, Identity, Privacy, Protection, Safety, and Security
	a. TIPPSS Architectural Framework
	b. Potential Ecosystem partnerships to enable TIPPSS, including standards
V	Data Validation
VI	Data Interoperability
VII	Identity
VIII	Conclusion
Appendix A	Pre-standards workstream participants
Appendix B	References
Appendix C	Glossary of Abbreviations

I. EXECUTIVE OVERVIEW AND RECOMMENDATIONS

The need for trusted, secure data sharing in connected healthcare, leveraging the Internet of Things, is increasing. [1], [2][1] There are many data sharing mechanisms, but the advent of blockchain and distributed ledger technology (DLT) is increasing the interest in how technology can enable data sharing between databases without a central authority, as is needed in connected healthcare toward the goal of precision medicine and improved health outcomes. The availability of DLT and blockchain technology is increasing the focus on the opportunity and need for process and cultural transformations to allow increased data sharing.

Current architected deployments of blockchain create concerns for clinical IoT use cases. While blockchain can enable data sharing, current blockchain deployments, primarily for cryptocurrencies, have heavy computing burdens including the proof of work, which creates a very high latency implementation. This is not useful, nor practical in a real-time connected, healthcare IoT scenario. Therefore, standards of compute efficiency are needed for Clinical IoT and blockchain. Also of concern is, if 51% of the nodes in a blockchain using current consensus algorithms agree to an addition to the chain and they are in collusion, the provenance of the data and transactions could be compromised. This could create financial loss in a cryptocurrency situation, but in a healthcare or Clinical IoT situation could cause loss of life.

The IEEE-SA pre-standards workstream team began this project focused on blockchain, but evolved to realize and recommend that it is the broader aspects of Trust, Identity, Privacy, Protection, Safety, and

[1] Information on references can be found in Appendix B.

Security (TIPPSS) in clinical IoT data and device interoperability that is of the utmost importance. While blockchain could be one of the technologies utilized, it is not necessary. Data sharing technologies have existed for many years. Blockchain is yet another technology and architecture that enables data sharing, in this case across data bases without a central authority, but it is not the only technology to support data sharing. Therefore, newstandards are needed to help ensure Clinical IoT data and device validation and interoperability, and provenance, enabled by a framework providing Trust, Identity, Privacy, Protection, Safety, and Security of the data and devices.

The elements of data validation, data and device interoperability, and validating identities of humans and devices are critical points in connected healthcare. These all are connected to an overall framework that IEEE has been developing for TIPPSS for IoT (Trust, Identity, Privacy, Protection, Safety and Security for the Internet of Things) (Figure 1). This framework was originally developed in February 2016 at an IEEE End-to-End trust and security for IoT workshop at George Washington University,[3] and further communicated in *IEEE Computer*, September 2018 in the article "Wearables and Medical Interoperability: The Evolving Frontier."[4]

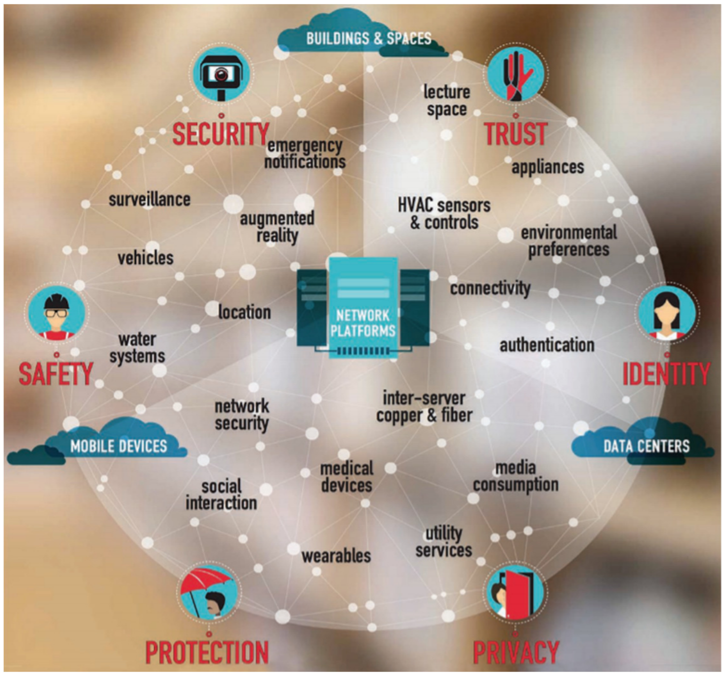
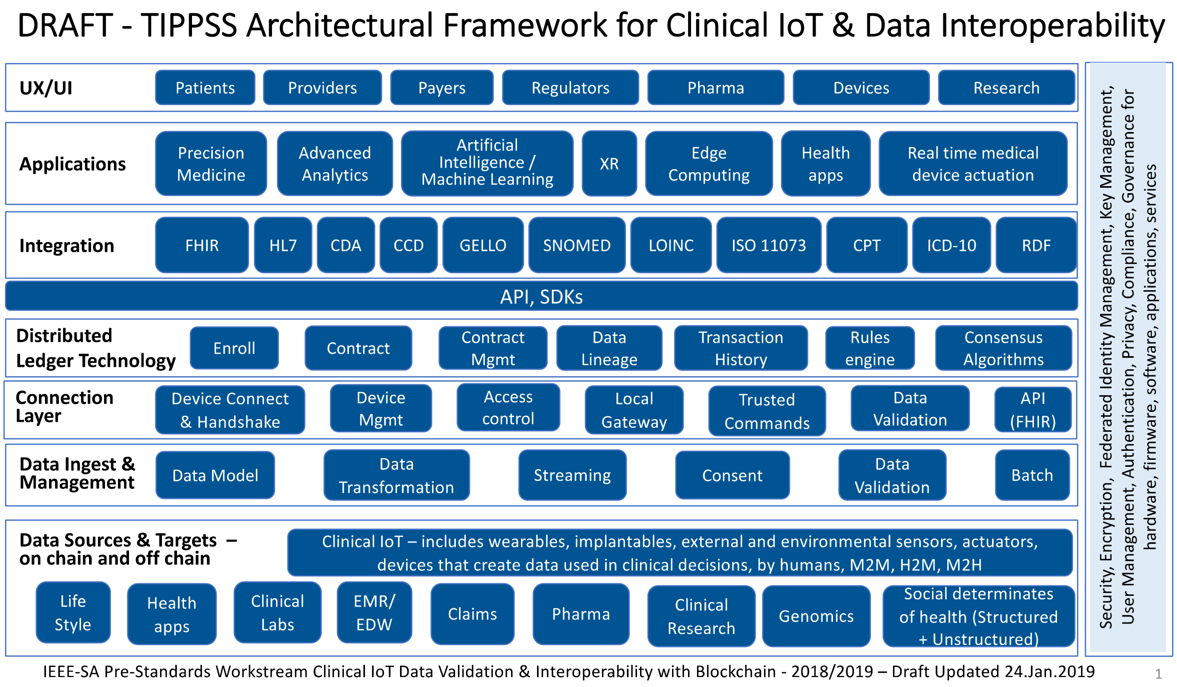


Figure 1. TIPPSS for IoT: Trust, Identity, Privacy, Protection, Safety and Security for the Internet of Things, © 2018 IEEE [4]

The IEEE-SA Clinical IoT data validation and interoperability with blockchain workstream team developed a "DRAFT—TIPPSS architectural framework for Clinical IoT data validation & interoperability with blockchain" (Figure 2) to enunciate the elements of an Information and Communications Technology (ICT) architecture and future standard, which need to be considered for a safe, secure, efficient, privacy-preserving clinical data sharing environment leveraging clinical IoT and blockchain. The recommended standards efforts should leverage this draft TIPPSS framework to ensure we architect around the world for Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) in Clinical IoT data and device interoperability, related to patients, providers, and devices. This is to help ensure end-to-end trust and security to keep patients safe, devices secure, data private and secure, and ensure healthcare providers and device manufacturers provide TIPPSS for their patients and systems.

Data are increasingly created, shared, and leveraged to improve healthcare outcomes. The accuracy and consistency of the data needs to be ensured by validating the devices and users, patients and providers, including credentialing. Visualizing this need in the field of Clinical IoT has been the inspiration to develop a feasible base for a standard framework and set of guidelines that enable validation of data from clinically-graded IoT devices and their interoperability with healthcare systems and potentially Distributed Ledger Technology such as blockchain.



DRAFT - TIPPSS Architectural Framework for Clinical IoT & Data Interoperability

UX/UI	Patients Providers Payers Regulators Pharma Devices Research
Applications	Precision Medicine Advanced Analytics Artificial Intelligence / Machine Learning XR Edge Computing Health apps Real time medical device actuation
Integration	FHIR HL7 CDA CCD GELLO SNOMED LOINC ISO 11073 CPT ICD-10 RDF
API, SDKs	
Distributed Ledger Technology	Enroll Contract Contract Mgmt Data Lineage Transaction History Rules engine Consensus Algorithms
Connection Layer	Device Connect & Handshake Device Mgmt Access control Local Gateway Trusted Commands Data Validation API (FHIR)
Data Ingest & Management	Data Model Data Transformation Streaming Consent Data Validation Batch
Data Sources & Targets – on chain and off chain	Clinical IoT – includes wearables, implantables, external and environmental sensors, actuators, devices that create data used in clinical decisions, by humans, M2M, H2M, M2H Life Style Health apps Clinical Labs EMR/ EDW Claims Pharma Clinical Research Genomics Social determinates of health (Structured + Unstructured)

Security, Encryption, Federated Identity Management, Key Management, User Management, Authentication, Privacy, Compliance, Governance for hardware, firmware, software, applications, services

IEEE-SA Pre-Standards Workstream Clinical IoT Data Validation & Interoperability with Blockchain - 2018/2019 – Draft Updated 24.Jan.2019

1

Figure 2: DRAFT—TIPPSS architectural framework for Clinical IoT data validation & interoperability with blockchain

The standard developed should be rigorous in terms of consistency, granularity, reliability, methods, processes, defined users, and concepts for the validation of data generated. This includes ensuring adherence from device manufacturers when it comes to integrating Clinical IoT data streams and distributed data repositories with other operational and analytical data streams and repositories, across enterprises and extended networks. The standard will govern the what, where, who, and how of the dimensions surrounding the Clinical IoT and data usage. The importance of the data being generated or utilized by the medical devices demands a sense of responsibility on our part to repeatedly ensure it is legitimate for purpose. Storing the data on and off the device and even off-blockchain will require cryptographic hashing and adherence to standards such as Health Insurance Portability and Accountability Act (HIPAA), extending it further to the transmission of data over communication methods. In order to strengthen the validation, the technical and functional validation may be augmented by automated standards alignment. Implementing the validation with acceptable minimum error tolerances will require calibration, formatting and cleansing for effective disposal. The use of artificial intelligence and machine learning algorithms could be fruitful here.

The broader picture focuses on creating the industry standard as a reference in the healthcare industry. One opportunity is to learn from blockchain efforts deployed in other industries for related examples, such as supply chain. There are blockchain solutions successfully deployed, for instance in shipping and transportation, which leverage blockchain as a foundation for digital management of supply chains, with several trading partners working together by forming a single shared view of a transaction without compromising details, privacy or confidentiality. Similarly, leveraging blockchain in the field of Clinical IoT is a potential advancement in terms of security and consistency, scrutinizing data manipulation and creating immutable records. It allows for the implementation of new standards in managing devices, data sharing, insurance claims, Personal Health Information (PHI), and medical records.

II. DEFINITIONS RELATED TO CLINICAL IOT AND BLOCKCHAIN

There are various definitions in play in the blockchain ecosystem that must be considered.

As a team, we have agreed that Distributed Ledger Technology (DLT) is a more appropriate term than blockchain as the market evolves and matures. It could be that blockchain becomes the ubiquitous term in the future; however, at a pure technology level, Digital Distributed Ledger Technology is the base. We have defined DLT and other pertinent terms used in this recommendation for a standards effort for Clinical IoT data and device validation and interoperability as follows:

Clinical Internet of Things, aka Clinical IoT

Clinical IoT comprises instrumented, connected, networked, interoperable and/or intelligent devices, equipment, instruments, apparatuses, implements, machines, contrivances, implants, in vitro reagents, or other similar or related articles, including component parts or accessories, which output their data to a clinical system of record (e.g., Electronic Patient Record), and which are recognized in the official National Formulary or the United States Pharmacopoeia, or any supplement to them. Clinical IoT devices are intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals.

In the interest of future-proofing the standards, it is important that the standards be developed bearing in mind promised and promising evolution of Clinical IoT. Consideration should include potential advancements such as synthetic skin patches, which will be able to record a variety of body signals and measurements, as well as the Biological Internet of Things (BIoT), which may include such concepts as brain interfaces that could tap directly into signals produced by the human brain or other tissues in the body. While not widely available today, these advancements must be taken into account over time.

A distinction must be drawn between Clinical IoT, as compared to Consumer IoT and Consumer Wearables. The differentiation is that Consumer IoT devices or wearables output their data to a consumer, whereas Clinical IoT devices output their data to clinical professional(s) and potentially allow for secondary sharing with the patient.

Blockchain, the colloquial term for Digital Distributed Ledger Technology

Digital Distributed Ledger Technology enables data sharing, verification, and validation services between mutually exclusive and independent participants where there is no central authority (Table 2).

Table 2. Ways in which DLT provides verification and validation services

	Services
i.	A synchronized shared digital distributed ledger, replicated and distributed across participants
ii.	Mutually agreeable record and transaction formats that can be verified and validated by source systems
iii.	Strong cryptographic verification and cross-validation of record entries to ensure immutability and prevent tampering or double-entries
iv.	Processes for ensuring consensus and consistency of the ledger view by all participants utilizing strong cryptography, appropriate consensus mechanisms, and cryptographic hashing algorithms to link entries together
v.	Technologies that allow participants to utilize Application Programming Interfaces (APIs) or utilities to enable reading or writing to the distributed ledger and enable records and transactions to be transferred between the Distributed Ledger and authoritative data sources and/or systems

See Glossary in Appendix C for defined acronyms.

Identity

Clinical IoT includes multiple forms of identity (Table 3). These are further developed in healthcare and clinical trial use cases in Section VII.

Table 3. Clinical IoT includes multiple forms of identity

	Identity
i.	Patient identity
ii.	Patient identity related to the Clinical IoT device and software
iii.	Clinical IoT device identity and data transfer
iv.	Physician/Clinician/Organization identity related to patient data
v.	Patient and their data identity
vi.	Publisher-subscriber identity

Virtual identity companies, both for profit and not for profit, provide identity validation and authentication. Examples of virtual identity solutions to consider as part of the TIPPSS framework, and to collaborate with, include the following:

- Sovrin (https://sovrin.org/#row_2)
- Evernym (https://www.evernym.com/)
- Thinktecture (https://www.thinktecture.com/identityAndAccessControl)

Decentralized Identifiers

Decentralized Identifiers (DIDs) are a type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject. See https://w3c-ccg.github.io/did-spec/.

Technical Interoperability

The ability of two or more information and communication technology applications to accept data from each other and perform a given task in an appropriate and satisfactory manner without the need for extra operator intervention is referred to as Technical Interoperability (EHealth Governance Initiative, 2017 [6]).

Harmonization

In terms of Distributed Ledger Technologies (DLT), *harmonization* is defined as the ability of the system and data maintained within it to be provably reconciled both forward and backward with other systems with which it exchanges data using DLT technologies, and with source and destination systems that may not utilize DLT.

TIPPSS

As previously stated, the acronym TIPPSS stands for Trust, Identity, Privacy, Protection, Safety, and Security. There are many commercial and personal devices being created without the due diligence to ensure these TIPPSS elements. Engineers need to ensure that the "things" that make up the IoT and the systems to which they connect are secure; that the devices or services connecting to a device can be trusted; that the identity of the incoming service request or person can be validated by a trusted authority; that the privacy of the data and the individual is maintained; that the humans and the infrastructure using the device are protected; and that safety and security are maintained. This is called TIPPSS for IoT (Table 4).

Table 4. TIPPSS for IoT elements

Elements	Service
Trust	Allow only designated people or services to have device or data access
Identity	Validate the identity of people, services and "things"
Privacy	Ensure device, personal, and sensitive data are kept private
Protection	Protect devices and users from physical, financial and reputational harm
Safety	Provide safety for devices, infrastructure, and people
Security	Maintain security of data, devices, people, systems

There are multiple publications on the topic of TIPPSS for IoT, including the following:

- IEEE Trust and Security Workshop for the Internet of Things. IEEE Standards Association. 4 February 2016. © 2016 IEEE [3]
- IEEE Computer Society, Computer Magazine. "Wearables and Medical Interoperability: The Evolving Frontier." September 2018. © 2018 IEEE [4]
- IEEE Computer Society. IT Professional Magazine, Technology Solutions for the Enterprise, "Enabling Trust and Security: TIPPSS for IoT." March/April 2018. © 2018 IEEE [7]
- "Women Securing the Future with TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things," © 2019 Springer Nature Switzerland AG [8]

III. RELATED STANDARDS EFFORTS FOR COLLABORATION

The standards efforts that are potentially valuable as sources against which to validate Clinical IoT data, and for collaboration as new standards are developed, are described in Table 5 and Table 6.

Table 5 includes standards efforts the team believes are valuable for technical and semantic validation. The standards efforts listed in Table 6 may or may not be directly useful for clinical IoT data and device interoperability at this time, as they may be redundant to other standards cited in Table 5, or their value is inconclusive. They are included in this report because some of them may prove valuable in the future, as more and more devices become more intelligent, and potentially capable and approved to offer diagnoses and recommend specific procedures. The standards developed should be extensible into the future.

(See the Glossary in Appendix C for defined acronyms and terms.)

Table 5. Standards efforts for technical validation (i.e., format, structure, data types, etc.) and semantic validation (i.e., content, meaning, values, etc.)

Standards	Descriptions and Notes
CDA	Clinical Document Architecture (CDA) is a base standard that provides a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents. CDA defines the structure of building blocks that can be used to contain a multitude of healthcare data elements that can be captured, stored, accessed, displayed and transmitted electronically for use and reuse in many formats.
C-CDA	Consolidated Clinical Document Architecture (C-CDA) was created in response to conflicting CDAs in use by the healthcare industry, to streamline commonly used templates for the exchange of medical summaries and documentation.
CIMI	The Clinical Information Modelling Initiative (CIMI) is an international collaboration that is dedicated to providing a common format for detailed specifications for the representation of health information content so that semantically interoperable information may be created and shared in health records, messages and documents.
CQL	Clinical Quality Language (CQL) is a Health Level Seven International (HL7) authoring language standard that is intended to be human readable. It is part of the effort to harmonize standards used for electronic clinical quality measures (eCQMs) and clinical decision support (CDS). CQL provides the ability to express logic that is human readable yet structured enough for processing a query electronically. CQL is the expression logic used in Health Quality Measure Format (HQMF) and eCQMs.
eCQM	electronic Clinical Quality Measure (eCQM) is a clinical quality measure that is expressed and formatted to use data from electronic health records (EHRs) and/or health information technology systems to measure healthcare quality, specifically data captured in structured form during the process of patient care.
FHIR	Fast Healthcare Interoperability Resources (FHIR) is s a standard for exchanging healthcare information electronically.
HQMF	Health Quality Measure Format (HQMF) is an HL7 standards-based representation of a quality measure as an electronic document. A quality measure expressed in this way is also referred to as an electronic clinical quality measure (eCQM).
HL7 IPS	Health Level Seven International Patient Summary (HL7 IPS) is a minimal and non-exhaustive Patient Summary, specialty-agnostic, condition-independent, but readily usable by all clinicians for the unscheduled, cross-border care of a patient.
ISO 01.040.35	International Organization for Standardization (ISO) 01.040.35 provides a list of Information technology vocabularies in healthcare technology
ISO/IEEE 11073-10101:2004	ISO/IEEE 11073-10101:2004—Health informatics—Point-of-care medical device communication covers nomenclature architecture for point-of-care (POC) medical device communication (MDC). It defines the overall architecture of the organization and relationships among nomenclature components and provides specifications of semantics and syntaxes.
LOINC	Logical Observation Identifiers Names and Codes (LOINC) is a database and universal standard for identifying medical laboratory orders, observations and documents.

Standards	Descriptions and Notes
OWL 2 EL	The OWL 2 Web Ontology Language for the Semantic Web provides classes, properties, individuals, and data values stored as Semantic Web documents. OWL 2 ontologies can be used along with information written in RDF. OWL 2 ontologies are primarily exchanged as RDF documents. OWL 2 EL is designed as a subset of OWL 2 that is particularly suitable for applications employing ontologies that define very large numbers of classes and/or properties, capturing the expressive power used by many such ontologies. For example, OWL 2 EL provides class constructors that are sufficient to express the very large biomedical ontology SNOMED CT.
QI-Core	Quality Improvement Core (QI-Core) uses FHIR, Quality Information and Clinical Knowledge (QUICK), and Clinical Quality Language (CQL) to create interoperable and executable knowledge artifacts for data gathered from IoT devices.
QUICK	The Quality Information and Clinical Knowledge (QUICK) data model provides a logical view of clinical data from the perspective of representing quality measurement and decision support knowledge.
RDF	Resource Description Framework (RDF) is a standard model for data interchange on the Web. FHIR resources can be represented as an RDF graph to assist bridging between operational data exchange and formal knowledge processing systems.
RxNorm	RxNorm is a catalog of the standard names given to clinical drugs and drug delivery devices in the United States to enable interoperability and clear communication between electronic systems, regardless of software and hardware compatibility.
SNOMED CT	Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT) is a standardized, multilingual vocabulary of clinical terminology used by physicians and other healthcare providers for the electronic exchange of clinical health information.
SOLOR	System Of Logical Representation (SOLOR) leverages a combination of SNOMED CT, LOINC, and RxNorm, merging these three terminologies that cover a vast breadth of clinical medicine, to form the foundation to address the inconsistent and fragmented clinical terminology landscape. SOLOR dictates that all of its content conforms to a consistent representation, specifically OWL 2 EL. This allows consistent reasoning and interaction with all of the content, regardless of its source terminology. SOLOR content is not limited to SNOMED CT, LOINC, and RxNorm. As needed, other individual concepts or entire terminologies can be added as long as they comply with OWL 2 EL semantics. SOLOR also interacts with the HL7 Clinical Information Modelling Initiative (CIMI).
X73 PoC-MDC	X73 Point of Care Medical Device Communications (X73 PoC-MDC) (ISO11073/IEEE1073) is an international standard to provide interoperability for Point of Care Medical Device Communication.

Table 6. Potentially useful standards efforts for Clinical IoT data validation into the future

Standards	Descriptions and Notes
Arden Syntax	Arden Syntax is an open standard for representing clinical knowledge, to be used by individual clinicians, institutions, and vendors to develop clinical rules (rules that directly impact patient care) using a standard format and language.
CDS on FHIR	Clinical Decision Support on Fast Healthcare Interoperability Resources (CDS on FHIR) is a project to investigate the use of FHIR in a Clinical Decision Support context. The goal is to identify best practices for the use of FHIR in support of the primary use cases of Clinical Decision Support, namely 1) Sharing Clinical Decision Support (CDS) knowledge artifacts, and 2) Obtaining Clinical Decision Support guidance as part of a clinical workflow.
CPT	Current Procedural Terminology (CPT) is a medical code set developed and maintained by the American Medical Association through the CPT Editorial Panel.
ICD-10	International Statistical Classification of Diseases and Related Health Problems, 10th revision (ICD-10) is a medical classification list by the World Health Organization (WHO). It contains codes for diseases, signs and symptoms, abnormal findings, complaints, social circumstances, and external causes of injury or diseases.
EHRS FM	Electronic Health Record System Functional Model (EHRS FM) outlines important features and functions that should be contained in an EHR system. Through the creation of functional profiles, this model provides a standard description and common understanding of functions for healthcare settings. To date, HL7 has developed or is developing profiles for areas such as child health, emergency care, long term care, behavioral health, and vital statistic reporting.
PHRS FM	Personal Health Record System Function Model (PHRS FM) defines a standardized model of the functions that may be present in Personal Health Record Systems. The information exchange enabled by the PHRS supports the retrieval and population of clinical documents and summaries, minimum data sets, and other input/outputs.
GELLO	GELLO is a standard query and expression language that provides a framework for manipulation of clinical data for decision support in healthcare. It is a class-based object-oriented programming language and a relative of the Object Constraint Language (OCL). OCL is a well-developed constraint language that makes it attractive for use as an expression language. GELLO uses an abstract "virtual medical record" (vMR) so that the same GELLO code can run on multiple systems accessing data stored in different formats. The vMR is a simplified view of the HL7 Reference Information Model (RIM).

IV. TIPPSS—TRUST, IDENTITY, PRIVACY, PROTECTION, SAFETY AND SECURITY

TIPPSS Architectural Framework

The use of wearables, accompanied by increased data sharing across medical devices, systems, solutions, and countries to promote the progress of precision medicine, is growing.[1], [2]. We can all be part of the solution to increase TIPPSS in IoT and medical interoperability. The ecosystem of partners to address these issues in Wearables and Medical IoT Interoperability & Intelligence (WAMIII) include IT and medical device hardware, firmware, software, and service developers and manufacturers; regulators; payers; providers; healthcare delivery organizations (HDOs); network service providers, and standards developers.

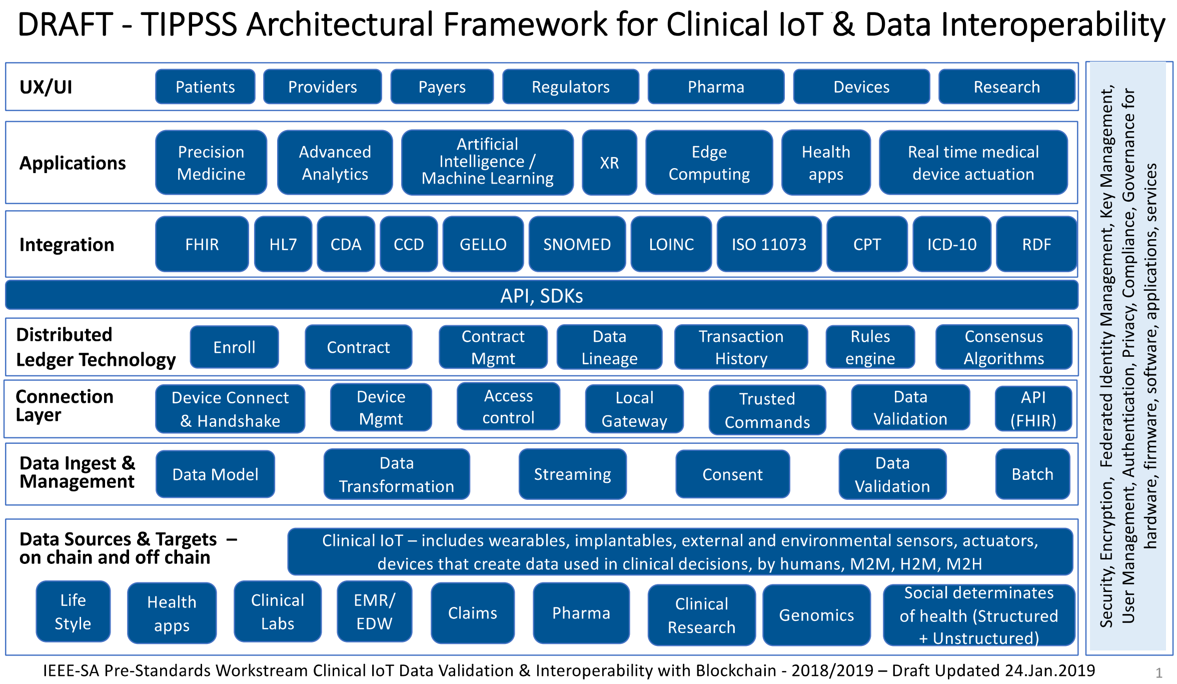
TIPPSS elements, including defense in-depth measures, have been deployed in information technology (IT) infrastructures for years. The increased connectivity of operational technology (OT) of critical infrastructure systems with IT has resulted in the growth of the IoT, with an increasing need for diligence in ensuring the trust, identity, privacy, protection, safety and security (TIPPSS) in our physical systems including industrial control systems (ICS), smart and connected communities, intelligent transportation systems, and connected healthcare. Adding to the complexity of the ecosystem of the IoT is the need to include privacy considerations of healthcare data in multiple highly regulated regions such as the United States and European Union.

The use of TIPPSS and defense in-depth strategies provide a layered approach to protecting devices, the humans involved with the device, as well as the data collected, gathered, and distributed. Technologies including key pairs, trusted platform modules, even newly announced crypto-anchors from IBM, can enable defense-in-depth for hardware, firmware, software, and service-level security, as discussed in a 2015 KPMG report on security and the IoT ecosystem.[9] Processes enabled with technologies such as leverage of ‘whitelist’ device registries, challenge-response, behavioral signatures, environmental checks, or one-time trust events can enable defense in depth. Potential standards recommendations for identity and authentication with security can include these capabilities for Clinical IoT data and device validation.[10], [11]

Increasing the focus on the multiple technologies available for end-to-end trusted environments and security frameworks, the New England Journal of Medicine in 2018 called out the need to include Real World Evidence (RWE) leveraging Unique Device Identifiers (UDIs), bringing the medical and IT communities together in the pursuit of safe and secure connected healthcare.[12] A key component to RWE is consideration of risk as part of the overall cybersecurity equation. By understanding risk, each participant in the healthcare ecosystem can make educated decisions on current and future technology implementations. This risk analysis must be performed for each layer of the technology stack for a defense-in-depth strategy for hardware, firmware, software, and service levels to be truly and holistically effective. As the security boundary continues to blur, understanding the risk impact becomes a cyclical process and a key measurement for a cyber-resilient organization.

The “TIPPSS Architectural Framework for Clinical IoT Data Interoperability and Blockchain” team of the pre-standards effort created recommendations for standards work to be done to ensure Trust, Identity, Privacy, Protection, Safety and Security leveraging blockchain in Clinical IoT data and device interoperability, related to patients, providers, and devices. This is to ensure end-to-end trust and security to keep patients safe, devices secure, data private and secure, and ensure healthcare providers and device manufacturers provide TIPPSS for their patients and systems.

The DRAFT TIPPSS architectural framework in Figure 3 brings together identified pieces of a digital architecture to support the processes for Clinical IoT data and device validation and interoperability leveraging Distributed Ledger Technology (DLT) or blockchain. Security, Identity and Privacy are critical up and down the stack as depicted in the light blue box on the right. The standards effort would include clarifying this framework, its elements, and ensuring data provenance, validation, identities, and credentialing of users, for Clinical IoT in connected healthcare use cases.



DRAFT - TIPPSS Architectural Framework for Clinical IoT & Data Interoperability

UX/UI: Patients | Providers | Payers | Regulators | Pharma | Devices | Research

Applications: Precision Medicine | Advanced Analytics | Artificial Intelligence / Machine Learning | XR | Edge Computing | Health apps | Real time medical device actuation

Integration: FHIR | HL7 | CDA | CCD | GELLO | SNOMED | LOINC | ISO 11073 | CPT | ICD-10 | RDF

API, SDKs

Distributed Ledger Technology: Enroll | Contract | Contract Mgmt | Data Lineage | Transaction History | Rules engine | Consensus Algorithms

Connection Layer: Device Connect & Handshake | Device Mgmt | Access control | Local Gateway | Trusted Commands | Data Validation | API (FHIR)

Data Ingest & Management: Data Model | Data Transformation | Streaming | Consent | Data Validation | Batch

Data Sources & Targets – on chain and off chain: Clinical IoT – includes wearables, implantables, external and environmental sensors, actuators, devices that create data used in clinical decisions, by humans, M2M, H2M, M2H

Life Style | Health apps | Clinical Labs | EMR/ EDW | Claims | Pharma | Clinical Research | Genomics | Social determinates of health (Structured + Unstructured)

Security, Encryption, Federated Identity Management, Key Management, User Management, Authentication, Privacy, Compliance, Governance for hardware, firmware, software, applications, services

IEEE-SA Pre-Standards Workstream Clinical IoT Data Validation & Interoperability with Blockchain - 2018/2019 – Draft Updated 24.Jan.2019

Figure 3: Draft TIPPSS architectural framework

Terms used in Figure 3:

API: Application Programming Interface*;*

Clinical IoT devices: include low latency requirements for real time and command driven applications, in the microsecond timeframe*;*

Consensus algorithms: there could be different consensus models based on use cases;

Consent: patient consent and provider consent to the use of the data that belongs to them*;*

Edge Computing: compute on the edge in routers or storage devices, in the home or institutional settings, or in smart and connected cities and vehicles as part of the healthcare ecosystem*;*

EMR/EDW: Electronic Medical Records and Enterprise Data Warehouse*;*

Enroll: for devices, people (patients, providers, payers, etc.), organizations, administrators*;*

H2M: Human to Machine, such as a brain creating commands and actuating with devices*;*

M2H: Machine to Human*;*

M2M: Machine to Machine*;*

Pharma: Pharmacies or Pharmaceutical Companies*;*

SDK: Software Developer Kit*;*

Social determinates of health: geographic and other demographics, social media, etc.;

UX/UI: User Experience / User Interface*;*

XR: Extended Reality, including Augmented Reality, Virtual Reality, Mixed Reality, etc.

Potential ecosystem partnerships to enable TIPPSS, including standards

Partnerships will help us work collaboratively across the healthcare and blockchain ecosystem to develop a comprehensive, coordinated standards effort. Potential partnerships for the recommended standards effort are listed in Table 7. The standards efforts listed in Table 5 and Table 6 are also potential partnership opportunities for the recommended standards effort moving forward.

Table 7. Potential ecosystem industry partnerships to enable TIPPSS

Category	Potential partnerships (alphabetically)	
Hardware: Medical device manufacturers	• Abbott Labs • Amazon • Apple (iPhone, iWatch [w/Kardai, Pulse, etc.]) • Biomed • Boston Scientific • Edwards Lifesciences • Embleema • Fitbit, Inc. • Google	• iHealth (SpO2, BP, pulse, glucose, weight, etc.) • Johnson & Johnson • Medtronic, plc • Microsoft • Novartis • Pfizer • Roche • Samsung
Non-Health related technology that may transport data that impacts health	• IEEE 802.11x • Bluetooth • Cellular • Data Storage • Extenders/Repeaters • IR • Networking Hubs • RF	• Routers/Access Points • Ultrasound • Wired (rj-11, rj-45, USB, DVI, HDMI, rs-232/455/485, etc.) • Wireless communications • Zigbee • Z-Wave
Healthcare business units/departments that may integrate patient data	• Asset/Inventory Tracking • Business Intelligence and Analytics • Data Protection/Encryption/ Storage/Backup/Recovery • Database Management • Distributed Systems (e.g., virtual systems and/or cloud-based solutions) • Document Management • Electronic Prescriptions/ Pharmaceuticals	• Information Technology (IT)/Informatics • Patient Scheduling • Payment Processing/Billing (e.g., EHR's and EMR's) • Quality Control/Regulatory • Sales Management and Digital Marketing • Supply Chain/Enterprise Resource Planning • Web Services/Networking
Regulators	• TÜV (Technischer Überwachungsverein [Technical Inspection Association]) • UK/England National Health Service (NHS)	• US Centers for Disease Control and Prevention (CDC) • US Department of Health and Human Services (HHS) • US Food and Drug Administration (FDA)

V. DATA VALIDATION

This document provides directional guidance on the contents, boundaries, and purposes of a standard framework to be consistent in structure, style, intent, and granularity with other existing IEEE (data, communications, etc.) standards to support Clinical IoT data validation and interoperability. A compendium of external standards that we believe IoT data should be validated against, and standards efforts the recommended IEEE standard effort needs to collaborate with for international harmony on standards for Clinical IoT and blockchain, are included in Section III.

The Standard for Clinical IoT Data and Device Interoperability with TIPPSS—Trust, Identity, Privacy, Protection, Safety, Security—that we recommend be developed will set forth consistent, reliable, extensible, and reproducible structures, methods, processes, and concepts for the validation of data generated and/or managed by the Internet of Medical Things (IoMT)—which should be adhered to by manufacturers to enable IoMT assets to harmonize, exchange, interoperate, and integrate IoMT data streams and repositories with other operational and analytical data streams, across their enterprises and extended networks.

Clinical Data Validation involves identifying, and potentially remediating, discrepancies and/or flaws in up to eight characteristics of "good clinical data" (Table 8). Additional insights on data validation include the following:

- Data translation will be dependent on data validation standards
- Interoperability with blockchain includes defining what is and is not kept on chain
- Data on-chain and off-chain needs to be validated
- Privacy and protection, including de-identification of PHI / PII / PCI / HIPAA related data, has a dependency on IoMT data validation.

Table 8. Characteristics of "good clinical data"

Characteristic	Defined
Attributable	• Sources of the data are known and recorded
Legible	• Data are human or machine readable
Contemporaneous	• Source data are recorded when generated
Original	• All data come from the original source • Copies and transformations of the data are accurate and complete, do not overwrite original data, and are traceable back to original data
Accurate	• Data are correct, given the context of their use
Enduring	• The data are available for the entire time they are required to be kept
Complete	• All pertinent and contextual data, including metadata, transactional and detail, are included
Consistent	• All data use consistent terms and are non-contradictory

VI. DATA INTEROPERABILITY

Data and device interoperability includes methods for data collection, storage and transformation to enable safe and secure data interoperability for Clinical IoT and healthcare.

Technical Interoperability is defined in this report to be the ability of two or more information and communication technology applications to accept data from each other and perform a given task, in an appropriate and satisfactory manner, without the need for extra operator intervention.[4]

One consideration is whether the technology will use the data or just pass the data through to another technology. Potential actions include examining, analyzing, adding to, subtracting from, encrypting, or reporting out on the data. If the technology is just passing through the data to another technology, it is basically a data tunnel, but the veracity and provenance of the data must still be maintained.

Interoperability must be considered at all levels of technology—hardware, software, firmware—and service layers such as on line communication layers, as well as including the human element.

Considerations of the impact that Clinical IoT data and device interoperability has on healthcare organizations and medical device manufacturers is pertinent as well. Healthcare organizations include payers and providers, the World Health Organization (WHO), Department of Health and Human Services (HHS), Centers for Disease Control and Prevention (CDC), Government, Laboratories and Diagnostic Clinics.

VII. IDENTITY

Identity is an important element of the TIPPSS framework for Clinical IoT. Identity challenges and needs can be expressed and understood in practical terms through the exploration of use cases for Clinical IoT. The identity team in this IEEE pre-standards effort for Clinical IoT developed use case examples, listed requirements for each use case, researched existing frameworks in the marketplace as examples and finally suggest an optimal tool/workflow for each use case.

Healthcare and Clinical Trial Use Cases were considered to identify these identity elements to be included in the recommended Clinical IoT standards work (Table 9).

Table 9. Identity elements to be included in the recommended Clinical IoT standards

Elements	Action
Patient Identity in healthcare and clinical trial scenarios	a. Validate the identity of the patient to ensure this is the right patient's data b. The patient must always be able to recover their identity even if they forget the device ID or security mechanism, so they can use the device. This is a unique requirement as compared to the way blockchain works today.
Patient identity related to the Clinical IoT device and software	a. Ensure this is the right person using the device b. Ensure this is the right system and software using the device
Clinical IoT device identity and data transfer	a. Data transfer from the Clinical IoT device to blockchain with valid identity b. Ensure from a system to system perspective that the credentials are correct c. Must support device data sharing with physician/provider
Physician / Clinician / Organization Identity related to Patient Data	a. Ensuring this physician/clinician/organization has rights to this particular patient's data b. Ensuring this physician/clinician/organization is currently certified to access this patient's data
Patient and their data identity in clinical trials	a. A clinical trial sponsor or academic institution may need validated identification of the patient, their device and data b. Determine how respective data is identified when certain data must be masked from either the clinician or the trial sponsor c. Sponsor should not identify or have access to patient's personal information, however, physician will be the facilitator d. Consider technical and regulatory aspects, including security and privacy e. The identity problem may be solved using "Zero-Knowledge Proof," a masking mechanism
Publisher-subscriber identity	a. A subscriber interface of a device in the patient data exchange system may receive a particular set of uniquely identified patient data b. A publisher interface may receive a request for the patient data, wherein the publisher interface may determine, based at least in part on privacy attributes, whether to provide a response to the request

We believe that Sovrin [13] is a valuable partner for the standards work to be done. Sovrin is an open source project creating a global public utility for self-sovereign identity, which can be leveraged for Clinical IoT and healthcare. The Identity team discussed our goals with the Sovrin CTO and Cybersecurity leader. Both agree we need standards in the use of blockchain for Clinical IoT data validation and interoperability.

Sovrin facilitates the identity of user/device in the decentralized blockchain world—similar to a peer-to-peer network. Their tenets of IoT & Human Identity and Interaction are listed below:

- Permanent ownership over the identity
- Complete control of the identity
- No reliance on external authorities to use the identity
- No single entity to control all identities

- A guardian can be appointed to control the identity where it is necessary (an IoT device would have a manufacturer own the identity)
- Multiple identities may be owned by the same entity (a device could have a unique identity for each pairing with a human identity)
- Identities should be usable across multiple blockchains/environments
- Must ensure data portability for all data associated with the identity regardless of where the data is stored, off blockchain for example
- Privacy and Security by Design and as a default
- Creating and having an identity is open to all
- Each Identity has a Decentralized Identifier (DID)that can use zero-knowledge proof to keep the legal identity blinded

The Decentralized Identifier (DID) explanation from W3C includes a DID method, which specifies the set of rules for how a DID is registered, resolved, updated, and revoked on that specific ledger or network. This design eliminates dependence on centralized registries for identifiers as well as centralized certificate authorities for key management—the standard pattern in hierarchical PKI (public key infrastructure). Because DIDs reside on a distributed ledger, each entity may serve as its own root authority—an architecture referred to as DPKI (decentralized PKI). Identity Elements are listed in Table 10.

Table 10. DPKI (decentralized PKI) identity elements

Elements	Defined
Things	• Devices, pets, physical or digital objects (should not be held liable for actions)
Identity Owner	• Individuals or organizations (may be held liable for their actions)
Individuals are further broken down into…	• Independents, those who have direct control over their Private Keys • Dependents, those who do not have direct control over their Private Keys (could be a guardian situation; or in a clinical trial the Site may maintain the Private Keys for their participants)

Questions and considerations to be further developed and answered during the standards effort regarding identity include the following:

- Building upon existing device identities, can it be a part of the Thing identity?
- Authenticity of the device (e.g., if a device says it is a certain model of Medical blood pressure cuff, can it be verified?)
- Perhaps require manufacturers to include something that can authenticate it is a real device.
- Cryptography needs to match the Privacy by device (i.e., identifiers should be contextual).
- More to be done on how to standardize the authentication with identity for device, user, application, etc.

Figure 12 shows a Draft Digital Identity Architecture to further develop the identity elements in the Draft TIPPSS Architectural Framework in Figure 3 of Section IV.

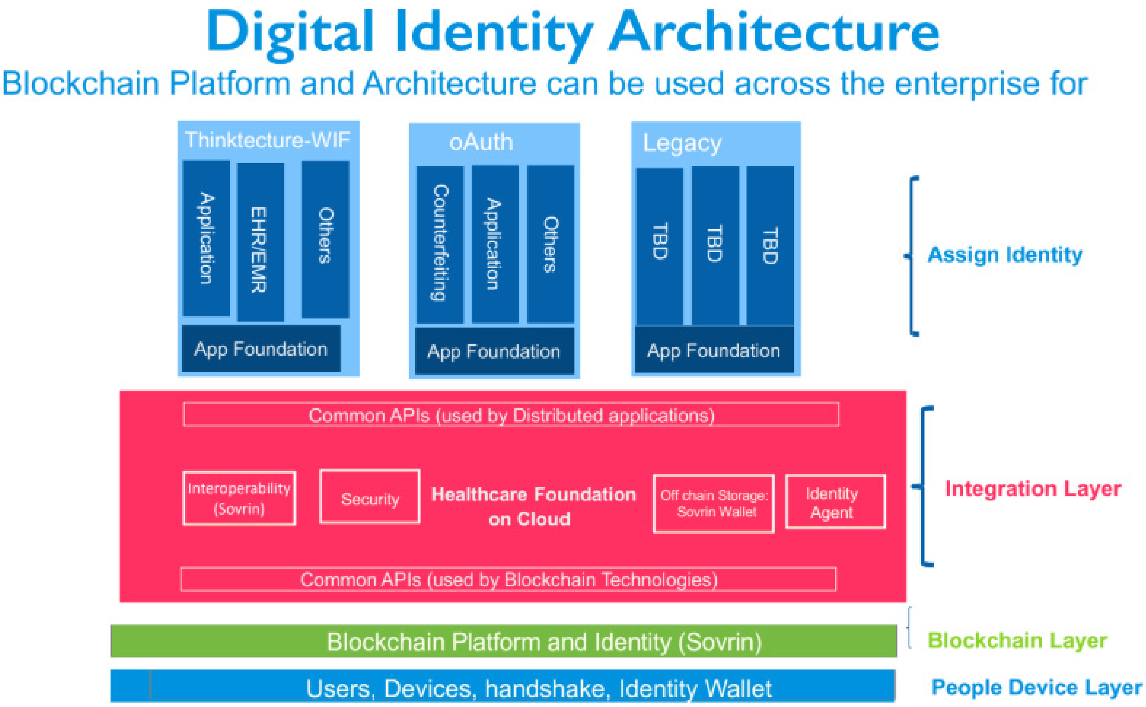

Digital Identity Architecture
Blockchain Platform and Architecture can be used across the enterprise for
Thinktecture-WIF
Application
EHR/EMR
Others
App Foundation
oAuth
Counterfeiting
Application
Others
App Foundation
Legacy
TBD
TBD
TBD
App Foundation
Assign Identity
Common APIs (used by Distributed applications)
Interoperability (Sovrin)
Security
Healthcare Foundation on Cloud
Off chain Storage: Sovrin Wallet
Identity Agent
Common APIs (used by Blockchain Technologies)
Integration Layer
Blockchain Platform and Identity (Sovrin)
Blockchain Layer
Users, Devices, handshake, Identity Wallet
People Device Layer

Figure 12. Draft digital identity architecture for Clinical IoT

VIII. Conclusion

The IEEE-Standards Association pre-standards workstream for Clinical Internet of Things Data Validation and Interoperability with Blockchain began with a specific focus on blockchain. Throughout the process of the workstream, we realized that blockchain could be a part of clinical IoT data validation and interoperability, but it is not a required element. There are concerns regarding the security and privacy of a blockchain enabled system, including the ability to hack a blockchain through collusion of 51% of the nodes based on the current standard blockchain consensus algorithm. We also considered the need for defense-in-depth strategies for the devices and systems in a clinical IoT ecosystem. Therefore, the pre-standards workstream team developed the recommendation to propose an expanded standards effort for Clinical IoT data and device interoperability with TIPPSS—where the Trust, Identity, Privacy, Protection, Safety, and Security elements are of the utmost importance. We agree that blockchain or more generically distributed digital ledger technology is an option but not a requirement, and in fact might not meet the TIPPSS requirements in clinical IoT use cases.

The pre-standards workstream led to the recommendation of the development of an IEEE-SA Standards effort on Clinical IoT data and device interoperability with TIPPSS in connected healthcare, with the opportunity to leverage blockchain along with other complementary technologies to improve data sharing and healthcare outcomes. This standard will establish the framework with TIPPSS principles (Trust, Identity, Privacy, Protection, Safety, Security) for Clinical Internet of Things (IoT) data and device validation and interoperability. 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. The resulting IEEE Standards Association P2733 Clinical IoT Data and Device Interoperability with TIPPSS standards effort kicks off July 17, 2019, sponsored by the IEEE-SA Engineering in Medicine and Biology Society. For more information and to join the P2733 working group, visit the working group website https://sagroups.ieee.org/2733/ .

~~~~~
~~~~~

Appendix A. Pre-standards workstream participants

Workstream leader: Florence D. Hudson, flo1980@alumni.princeton.edu

Members: 22 active participants = 10 Industry, 6 Academia, 3 Government, 3 IEEE

- Abhivyakti Sawarkar, MD, MMSc, Staff Fellow, Office of Translational Sciences Center for Drug Evaluation & Research, U.S. Food and Drug Administration
- Alfred F. Sorbello, DO, MPH, Medical Officer, Center for Drug Evaluation and Research, Office of Translational Sciences, U.S. Food and Drug Administration
- Bina Ramamurthy, PhD, Research Associate Professor, Computer Science and Engineering Department, University at Buffalo
- Bob Clint, CTO, Spiritus Partners
- Doug DeShazo, Assoc Dir Standards & Interoperability, Cognizant Technology Solutions -Healthcare
- Emily Dillon, Technical Engineering Analyst – Medical Device Security, Ascension Technologies (also a student intern for NSF Cybersecurity Summit)
- Florence D. Hudson (Workstream Leader), Special Advisor Northeast Big Data Innovation Hub at Columbia University; Special Advisor NSF Cybersecurity Center of Excellence at Indiana University; Board, Blockchain in Healthcare Today; Co-founder, Blockchain in Healthcare Global IEEE-ISTO
- Gerry Hayes, PhD, President & CEO, Wireless Research Center of North Carolina, Chair IEEE Industry Connections Program
- Henry “Skip” Francis, MD, Deputy Director, Office of Surveillance and Epidemiology, Center for Drug Evaluation and Research, U.S .Food and Drug Administration
- Jia Chen, PhD, Offering Leader, Blockchain for Healthcare & Life Sciences, IBM
- Karin Beckstrom, Senior Product Manager, Innovation Lab, ERT
- Maria Palombini, Director Emerging Communities & Opportunities, IEEE Standards Association
- Mike Taborn, Chief Platform Architect, IoT Healthcare Group, Intel
- Mitch Parker, Executive Director, Information Security and Compliance, Indiana University Health
- Olivia Choudhury, Postdoctoral Researcher, Learning Health Systems, IBM Research
- Pamella Howell, NIH Fellow in Biomedical Informatics, University at Buffalo
- Prashanth Areddy, Lead Data Acquisition Programmer, Bayer
- Sanjukta Das Smith, PhD, Assoc Prof, Dept Head & Dir of MS in MIS Program, University at Buffalo
- Saswata Soumya Dash, Graduate Student, Management Information Systems, IOT and Cloud, University at Buffalo
- Sri Chandrasekaran, Connectivity of the Digital Citizen, Industry Connections program, IEEE
- Srinivas Karri, Senior Director, Product Strategy, Clinical Data Warehousing Cloud, Oracle
- William Harding, Distinguished Technical Fellow, Medtronic, plc

Appendix B. References

[1] CIO Magazine, “Unlocking the Value in Patient-Generated Health Data.” 28 February 2017.

[2] Healthcare IT News, “87 Percent of Health Organizations Plan to Adopt IoT Technology by 2019, Study Shows.” 28 February 2017.

[3] IEEE Standards Association, IEEE Trust and Security Workshop for the Internet of Things, 4 Feb 2016, © 2016 IEEE; https://internetinitiative.ieee.org/images/files/events/ieee_end_to_end_trust_meeting_recap_feb17.pdf

[4] F. Hudson and C. Clark, "Wearables and Medical Interoperability: The Evolving Frontier," in *Computer*, vol. 51, no. 9, pp. 86-90, September 2018, © 2018 IEEE, DOI: 10.1109/MC.2018.3620987, https://ieeexplore.ieee.org/document/8481273

[5] Data Driven Schema for Patient Data Exchange System, 2018; http://www.freepatentsonline.com/10147502.pdf

[6] EHealth Governance Initiative. (2017). Discussion paper on semantic and technical interoperability; https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20121107_wd02_en.pdf

[7] F. D. Hudson, "Enabling Trust and Security: TIPPSS for IoT," IT Professional, vol. 20, no. 2, pp. 15-18, Mar./Apr. 2018, © 2018 IEEE, doi: 10.1109/MITP.2018.021921646, https://ieeexplore.ieee.org/document/8338006

[8] F. D. Hudson, Editor, “Women Securing the Future with TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things”, © 2019, Springer Nature Switzerland AG, DOI: 10.1007/978-3-030-15705-0

[9] KPMG, Security and the IoT Ecosystem, 2015, © 2015 KPMG International; https://assets.kpmg/content/dam/kpmg/pdf/2015/12/security-and-the-iot-ecosystem.pdf

[10]Network World, July 2018; “Identifying the Internet of Things – one device at a time”, https://www.networkworld.com/article/3287927/internet-of-things/identifying-the-internet-of-things-one-device-at-a-time.html

[11]IBM Research, 5 in 5, Five innovations that will help change our lives within five years, “Within the next five years, cryptographic anchors and blockchain technology will ensure a product’s authenticity -- from its point of origin to the hands of the customer”; https://www.research.ibm.com/5-in-5/crypto-anchors-and-blockchain/

[12]New England Journal of Medicine, “Medical Devices in the Real World,” February 2018, DOI: 10.1056/NEJMp1712001

[13]https://sovrin.org/

Appendix C. Glossary of Abbreviations

AKA: Also Known As

AMA: American Medical Association

API: Application Programming Interface

ASTM: American Society for Testing and Materials

ATOM: an open source text editor

BIoT: Biological Internet of Things

BP: blood pressure

CCD: Continuity of Care Document

C-CDA: Consolidated Clinical Document Architecture

CDA: Clinical Document Architecture

CDC: U.S. Centers for Disease Control and Prevention

CDS: Clinical Decision Support

CIF: International Classification of Functioning, Disability and Health,

CIMI: Clinical Information Modelling Initiative

CPT: Current Procedural Terminology

CQL: Clinical Quality Language

CQM: Clinical Quality Measures

CTO: Chief Technology Officer

DID: Decentralized Identifier

DLT: Distributed Ledger Technology

DPKI: Decentralized Public Key Infrastructure

DVI: Digital Visual Interface

eCQM: electronic Clinical Quality Measure

EDW: Enterprise Data Warehouse

EHR: Electronic Health Record

EHRS FM: Electronic Health Record System Functional Model

EMR: Electronic Medical Record

EU: European Union

FDA: U.S. Food and Drug Administration

FHIR: Fast Healthcare Interoperability Resources

GCP: Good Clinical Practice

GELLO: An HL7/ANSI standard decision support language.

HDMI: High-Definition Multimedia Interface

HDO: Healthcare Delivery Organization

HHS: U.S. Department of Health and Human Services

HIPAA: Health Insurance Portability and Accountability Act

HL7: Health Level Seven International

HQMF: Health Quality Measure Format

HTML: Hypertext Markup Language

HTTP: HyperText Transfer Protocol

H2M: Human to Machine

ICD: International Classification of Diseases

ICD-10: International Classification of Diseases, Tenth Revision

ICS: Industrial Control Systems

ICT: Information and Communications Technology

ID: Identity

IEEE-SA: Institute of Electrical and Electronics Engineers – Standards Association

IoMT: Internet of Medical Things

IoT: Internet of Things

IR: Infrared Radiation

ISO: International Organization for Standardization

ISO/IEEE 11073: Standards for point-of-care (PoC) medical device communication

ISO 11073: Family of standards for point-of-care (PoC) medical device communication

IT: Information Technology

JSON: JavaScript Object Notation

LOINC: Logical Observation Identifiers Names and Codes

MDC: Medical Device Communication

MLM: Medical Logic Module

M2H: Machine to Human

M2M: Machine to Machine

NHS: UK National Health Service

OCL: Object Constraint Language

OT: Operational Technology

OWL: Web Ontology Language

PCI: Payment Card Industry

PHI: Protected Health Information

PHR: Personal Health Record

PHRS FM: Personal Health Record System Functional Model

PII: Personally Identifiable Information

PKI: Public Key Infrastructure

POC: Point of Care

PoC MDC: Point of Care Medical Device Communication

QICore: HL7 Quality Improvement Core

QRDA: Quality Reporting Document Architecture

QUICK: Quality Information and Clinical Knowledge

RDF: Resource Description Framework

RESTful: Representational state transfer

RF: Radio Frequency

RIM: Reference Information Model

RWE: Real World Evidence

RxNorm: a normalized naming system for generic and branded drugs

SDK: Software Developer Kit

SNOMED: Systematized Nomenclature of Medicine

SNOMED CT: SNOMED Clinical Terms

SOLOR: Integration of SnOmed, LOinc, RxNorm data terminology

SpO2: Peripheral capillary oxygen saturation, an estimate of oxygen in the blood

TIPPSS: Trust, Identity, Privacy, Protection, Safety & Security

TÜV: Technischer Überwachungsverein [Technical Inspection Association]

UDI: Unique Device Identifiers

UK: United Kingdon

URI: Uniform Resource Identifier

US and USA: United States of America

USB: Universal Serial Bus

UX/UI: User Experience / User Interface

vMR: virtual medical record

WAMIII: Wearables and Medical IoT Interoperability & Intelligence

WHO: World Health Organization

W3C: World Wide Web Consortium

XML: Extensible Markup Language

XR: Extended Reality, including Augmented Reality, Virtual Reality, Mixed Reality, etc.

X73 PoC-MDC: X73 Point of Care Medical Device Communications

Funding Statement –This report was developed as part of an IEEE-Standards association pre-standards workstream with voluntary participation as noted in Appendix A.

Conflict of Interest – None.

Contributor Contributions – See Appendix A.