IEEE-SA EMB Standards Committee Meeting – 11 June 2019

Overview of P2733 –Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS (Trust, Identity, Privacy, Protection, Safety, Security)

Florence D. Hudson, P2733 WG Chair
Founder and CEO, FDHint
Special Advisor, NSF Cybersecurity Center of Excellence at Indiana University
Special Advisor, Northeast Big Data Innovation Hub at Columbia University

Agenda

- Industry context regarding Clinical IoT and TIPPSS
- IEEE – SA Pre-Standards Workstream: Clinical IoT Data Validation and Interoperability with Blockchain
- P2733 Overview – Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS
  (Trust, Identity, Privacy, Protection, Safety, Security)
- Educational Resources
- Next Steps

Health data sharing and Medical IoT usage is increasing

"We've killed more people because we didn't share data than because we did."
- *CIO Magazine*[2], Paddy Padmanabhan

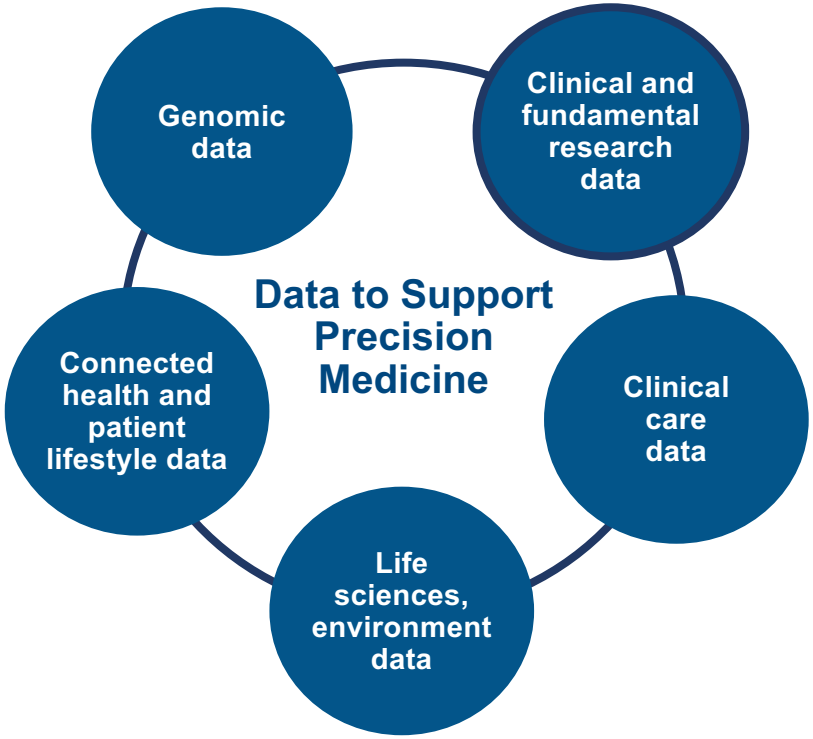
"87% of health organizations plan to adopt IoT technology by 2019."
- *Healthcare IT News*[3], Jessica Davis

NCI Cancer Moonshot Blue Ribbon Panel[4]
- Build a national cancer data ecosystem

Computational Approaches for Cancer annual SuperComputing workshop[5]

Sources: [1]*Frost & Sullivan,* [2]*CIO Magazine 28 Feb 2017*, [3]*Healthcare IT News 28 Feb 2017,* [4]https://www.cancer.gov/research/key-initiatives/moonshot-cancer-initiative/blue-ribbon-panel, [5]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6302370/

Precision Medicine will leverage large volumes and varieties of data to improve insight & outcomes



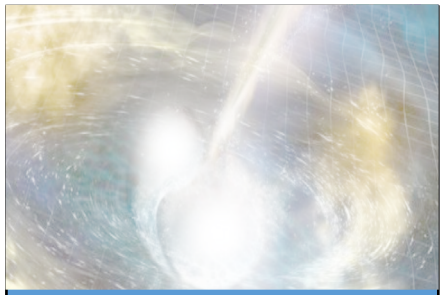
Many data sources and types…

- Genomic data
- Clinical and fundamental research
- Clinical care data and observations – image, text, numerical, video, audio, etc.
- Life sciences, environment data
- Connected health and wearables data
- Real World Evidence (RWE) leveraging Unique Device Identifiers (UDI)

Source: NIH The Precision Medicine Initiative Cohort Program - Building a Research Foundation for 21st Century Medicine." September 2015;
**The New England Journal of Medicine, Vol. 378, No. 7, February 15, 2018 "Medical Devices in the Real World"*

Awareness & reporting of security and privacy risk increasing

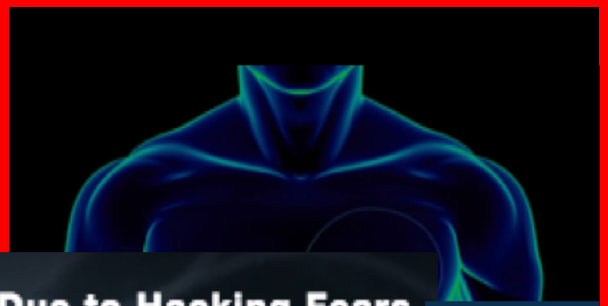
Vehicle Hacking
http://bit.ly/jeephackwired



Scientific Device Hacking
http://bit.ly/neutronstarscollide

Healthcare Device Hacking

http://bit.ly/jnjinsulinpump
http://bit.ly/medtronicinsulinpump
http://bit.ly/fdarecallspacemakers



FDA Recalls 465,000 Pacemakers Due to Hacking Fears

Hackers could reprogram the devices.

Aug 2017: https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals

Medical Advisory (ICSMA-19-080-01)

- Radio Frequency Telemetry Protocol
- Exploitable with adjacent access/low skill level to exploit.
- Telemetry protocol utilized does not implement encryption.
- Attacker with adjacent short-range access to a target product can listen to communications, including transmission of sensitive data.
- 20 products utilizing this telemetry protocol are affected.

March 2019: https://ics-cert.us-cert.gov/advisories/ICSMA-19-080-01

What could possibly go wrong? We need to protect the humans.

Top concerns:

- Connected healthcare devices
- Connected vehicles

Protection needed regarding:

- Defense in depth – Hardware, firmware, software, service
- Physical health and safety risk
- Financial risk, reputational harm
- Data theft, data integrity, loss of privacy

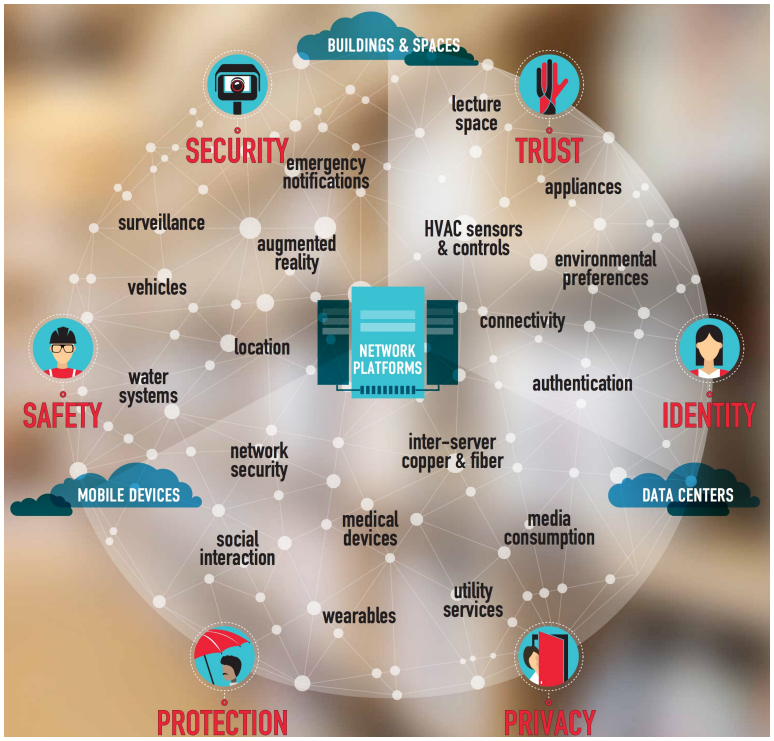
Need to evolve policy, culture, expectations.

> "Security really needs to be designed into IoT solutions right at the start. You need to think about it at the hardware level, the firmware level, the software level and the service level. And you need to continuously monitor it and stay ahead of the threat."
>
> —Florence Hudson, Senior Vice President and Chief Innovation Officer Internet2 (formerly with IBM)

Source: Florence D. Hudson; KPMG - Security and the IOT Ecosystem, 2015

TIPPSS: an imperative for Connected Healthcare

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



IEEE

IEEE-SA Pre-standards Workstream in WAMIII:
Wearables and Medical IoT Interoperability and Intelligence

Clinical IoT Data Validation & Interoperability with Blockchain

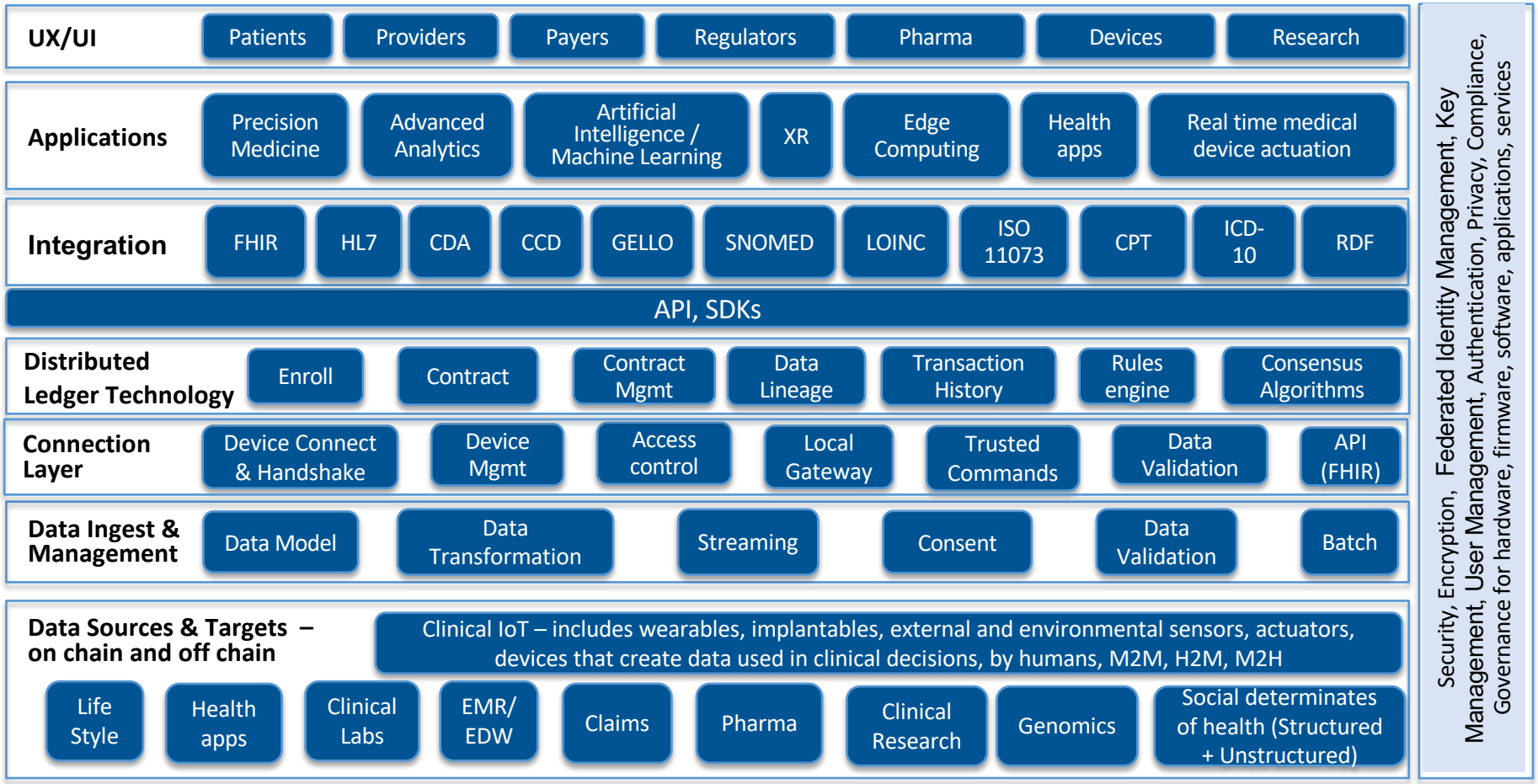
Pre-Standards Activity Completed Aug 2018-Feb 2019 – Recommendations Led to P2733

The charter and mission of the workstream was to determine if a viable standards framework, that would enable the validation of data generated from a clinical-grade IoT device and shared through the interoperability of blockchain technology, could be established.

Pre-standards workstream participants included industry, academia, government representatives from Ascension, Bayer, Cognizant, ERT, FDHint, IBM, IEEE, Indiana University Health, Intel, Medtronic, Oracle, Spiritus, Synopsys, University at Buffalo, US FDA, Wireless Research Center of North Carolina.

This PAR submission is a recommendation of the report created from the IEEE-SA Pre-standards workstream on "Clinical IoT Data Validation and Interoperability with Blockchain" which convened 22 active participants from government, industry and academia from August 2018 through February 2019. The report includes a draft TIPPSS Architectural Framework for Clinical IoT Data Validation & Interoperability which would be a starting point to be further vetted and developed as part of this proposed standards work.

DRAFT - TIPPSS Architectural Framework for Clinical IoT Data & Device Interoperability



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

P2733 – Standard for Clinical IoT Data and Device Interoperability with TIPPSS Working Group

Scope: This standard establishes 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.

Purpose: To enable secured data sharing in connected healthcare, improve healthcare outcomes, and protect patient privacy and security. There needs to be a set of guidelines and standards to standardize use of clinical IoT devices for precision medicine, data sharing, interoperability, and security with a goal of improved and measurable healthcare outcomes.

Stakeholders: Medical device manufacturers, hardware, software, and service developers and users for connected healthcare, payers, providers, patients, patient advocates, regulatory.

Standards Committee: EMB Standards Committee, Engineering in Medicine and Biology Society
PAR Approval Date: 21-May-2019, PAR Expiration Date: 31-Dec-2023

P2733 – Clinical IoT DDI with TIPPSS Working Group Officers

Chair
Florence Hudson, florence.distefano.hudson@gmail.com

Vice Chair(s)
William Harding, william.harding@medtronic.com

Mitchell Parker, mparker17@iuhealth.org

Secretary
Ganeshumar Jayaramakrishnan, ganeshkumar.jayaramakrishnan@uhc.com

Staff Liason
Tom Thompson, thomas.thompson@ieee.org

EMB Standards Committee, Engineering in Medicine and Biology Society

Standards Committee Chair: Carole C. Carey c.carey@ieee.org

EMB Standards Educational Corner

IEEE P2733 WG: Clinical IoT Data and Device Interoperability with TIPPSS
Working Group Chair, Florence Hudson

IEEE Standards Association, IEEE Trust and Security Workshop for the Internet of Things, 4 Feb 2016, © 2016 IEEE
Link: See the meeting recap here.

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, Read paper here.

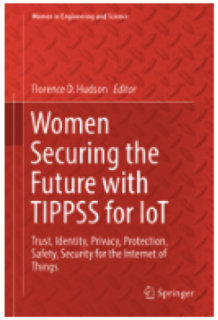
F. Hudson and C. Clark, "Wearables and Medical Interoperability: The Evolving Frontier," in Computer, vol. 51, no. 9, pp. 86-90, September 2018, © 2018 IEEE,
DOI: 10.1109/MC.2018.3620987, Read paper here.

http://standards.embs.org/standards-corner/

Women Securing the Future with TIPPSS For IoT

Trust, Identity, Privacy, Protection, Safety and Security for the Internet of Things

Women in Engineering and Science



Women Securing the Future with TIPPSS for IoT

Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things

Editors: **Hudson**, Florence D. (Ed.)

Provides insight into women's contributions to the field of Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS) for IoT

Presents information from academia, research, government and industry into advances, applications, and threats to the growing field of cybersecurity and IoT

Includes topics such as hacking of IoT devices and systems including healthcare devices, identity and access management, the issues of privacy and your civil rights, and more

Authors include:

- *AlphaEdison*
- *CERN*
- *CISCO*
- *City of San Francisco*
- *GÉANT*
- *GlaxoSmithKline*
- *IBM*
- *Indiana University*
- *Judge*
- *REN-ISAC*
- *Start-ups*
- *UC Berkeley*
- *UC Santa Cruz*
- *University of Kentucky*
- *Venture Capitalists*
- *Virginia Tech*

The Book: Women Securing the Future with TIPPSS for IoT

- IoT: Is It a Digital Highway to Security Attacks? - Cisco
- IoT: Privacy, Security, and Your Civil Rights – Colorado Judge
- Privacy in the New Age of IoT - GSK
- A Business Framework for Evaluating Trust in IoT Technology – Alpha Edison
- Ahead of the Curve: IoT Security, Privacy, and Policy in Higher Ed – REN-ISAC, VTC
- Trust, Identity, Privacy, and Security for a Smart Campus – Virginia Tech
- Security for Science: How One Thing Leads to Another - CERN
- The Dark Side of Things - GÉANT
- Public Safety and Protection by Design: IoT and Data Science – UC Berkeley, SF
- Privacy Management in the Internet of Things (IoT) – University of Kentucky
- Securing IoT Data with Pervasive Encryption - IBM
- Secure Distributed Storage for the Internet of Things – UC Santa Cruz
- Profiles of Women Securing the Future with TIPPSS for IoT - FDHint

Next Steps

- ❑ *Recruit members for the P2733 working group*
  - IEEE, LinkedIn, Twitter, interested individuals
  - Share working group homepage https://sagroups.ieee.org/2733/

- ❑ *P2733 Kickoff Meeting, July 17, 2019, 3-5pm ET*
  - To participate in the IEEE P2733 Working Group, please subscribe to the Listserv by sending an email to ListServ@ieee.org. Please be sure to include the following text in your email.
    - Subject: stds-P2733-wg
    - Body: subscribe stds-P2733-wg YourFirstName YourLastName

- ❑ *Publish whitepaper from pre-standards workstream*

Thank You

Florence D. Hudson
http://fdhint.com

flo1980@alumni.Princeton.edu

Twitter @Flo4Princeton
@FDHint