Center of Excellence
WIRELESS AND INFORMATION TECHNOLOGY
AT STONY BROOK UNIVERSITY

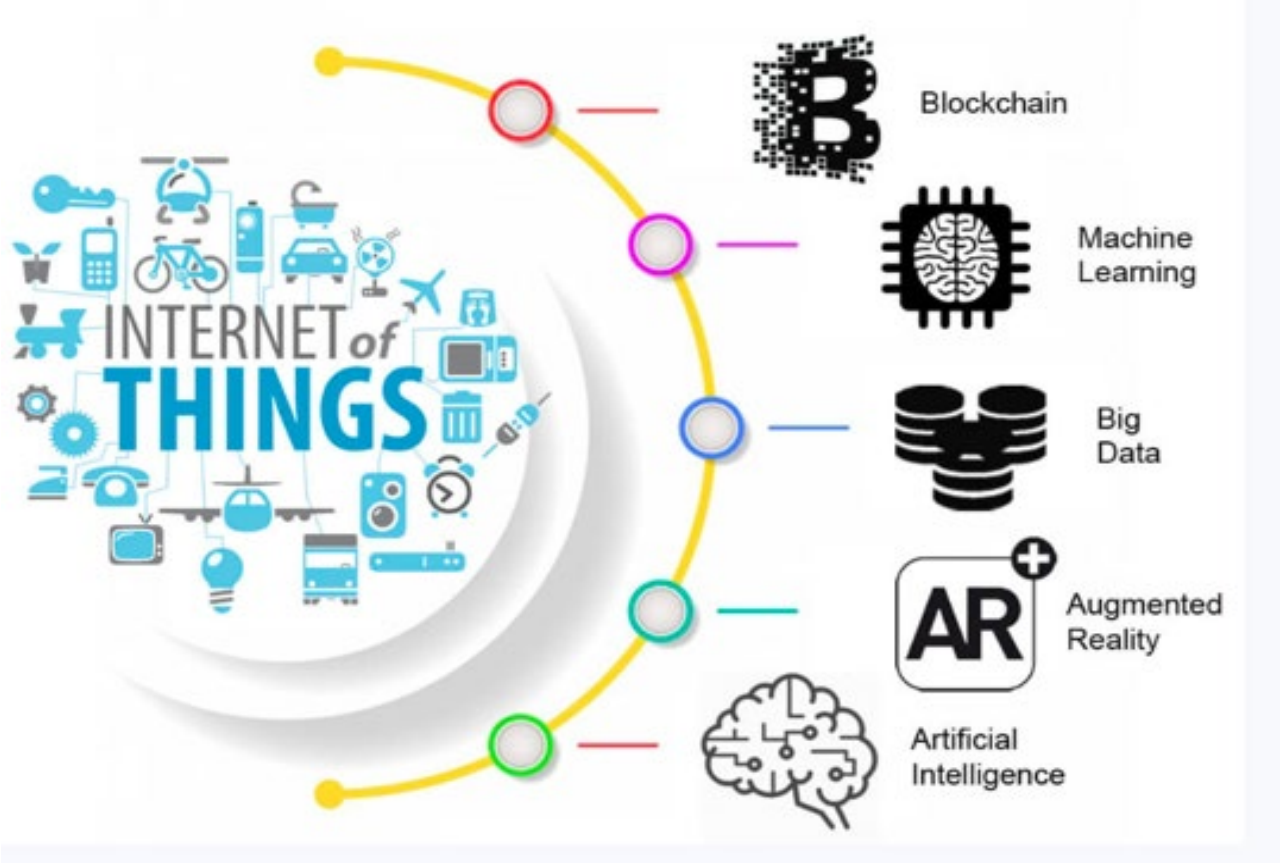
FD HINT

Harnessing Advanced Technology Innovations Today and into the Future

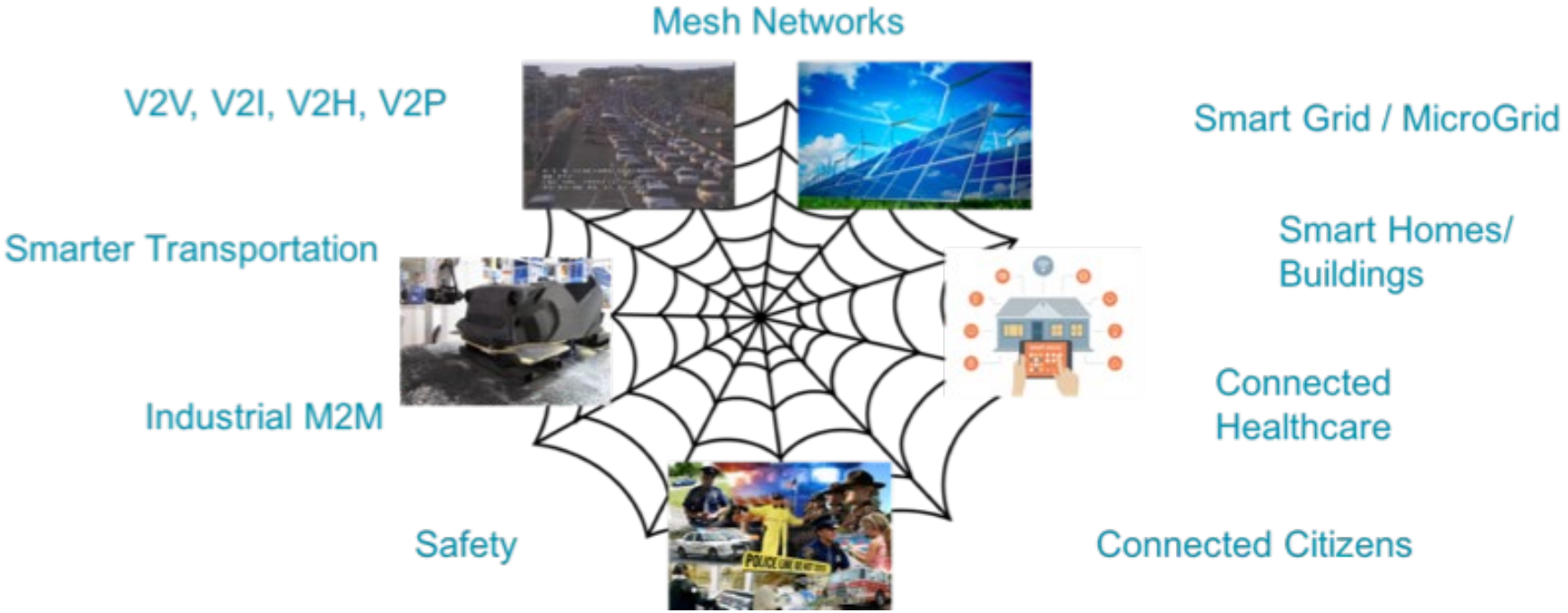
The 15th International Conference on Emerging Technologies for a Smarter World
Stony Brook, NY
November 6, 2019

Florence Hudson, Founder and CEO, FDHint LLC
NSF Cybersecurity Center of Excellence, Indiana University - Special Advisor
Northeast Big Data Innovation Hub, Columbia University - Special Advisor
IEEE Engineering in Medicine and Biology Society - Standards Committee

Advanced technology integration is enabling the future



Connectivity and IoT enable Smart Cities and Campuses with many use cases where risk needs to be managed.



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

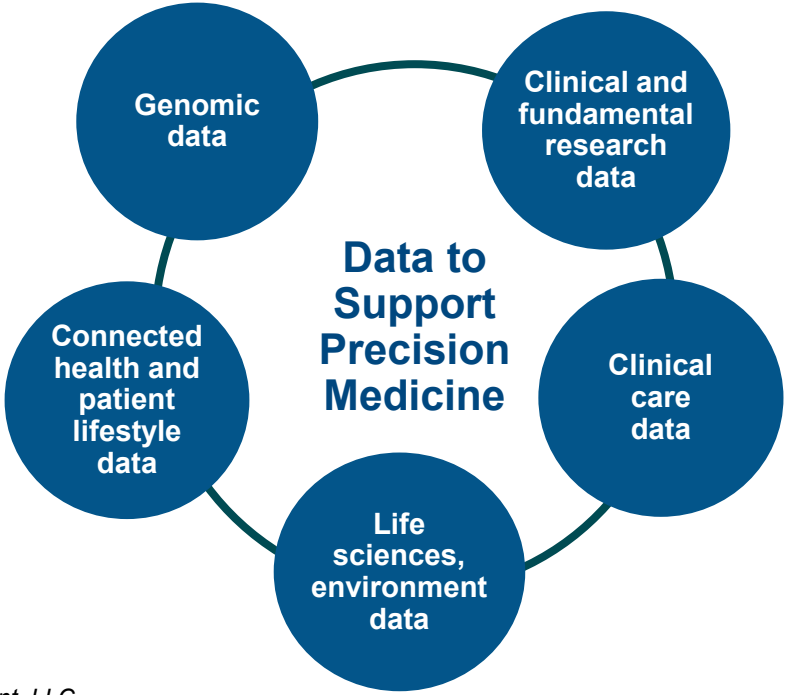
NCI Cancer Moonshot Blue Ribbon Panel[4]
- Build a national cancer data ecosystem

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.

>> *How do we protect the data, devices, patients?*



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)

*Sources: 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", 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*

Our increasingly connected world introduces increased risk to humans, vehicles, science, homes

Scientific Device Hacking

http://bit.ly/neutronstarscollide

Vehicle Hacking

http://bit.ly/jeephackwired

Smart Home Hacking

http://bit.ly/smartlockshack

Healthcare Device Hacking

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

US Dept of Homeland Security Medical Advisory

- Implanted cardiac devices & monitors can be hacked
- Exploitable with adjacent access/low skill level
- Telemetry protocol utilized within this ecosystem does not implement authentication or authorization
- Attacker can inject, replay, modify, intercept data, change memory in implanted cardiac device

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

What could possibly go wrong?
Need to protect humans, science, institutions, infrastructure.

Top concerns:

- Connected healthcare devices
- Connected vehicles
- Smart cities and campus
- Scientific device and data integrity

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)

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

IEEE is leading in creating focus on TIPPSS to improve Trust, Identity, Privacy, Protection, Safety, Security.

Trust: Allow only designated people/services to have device or data access

Identity: Validate the identity of people, services, and “things”

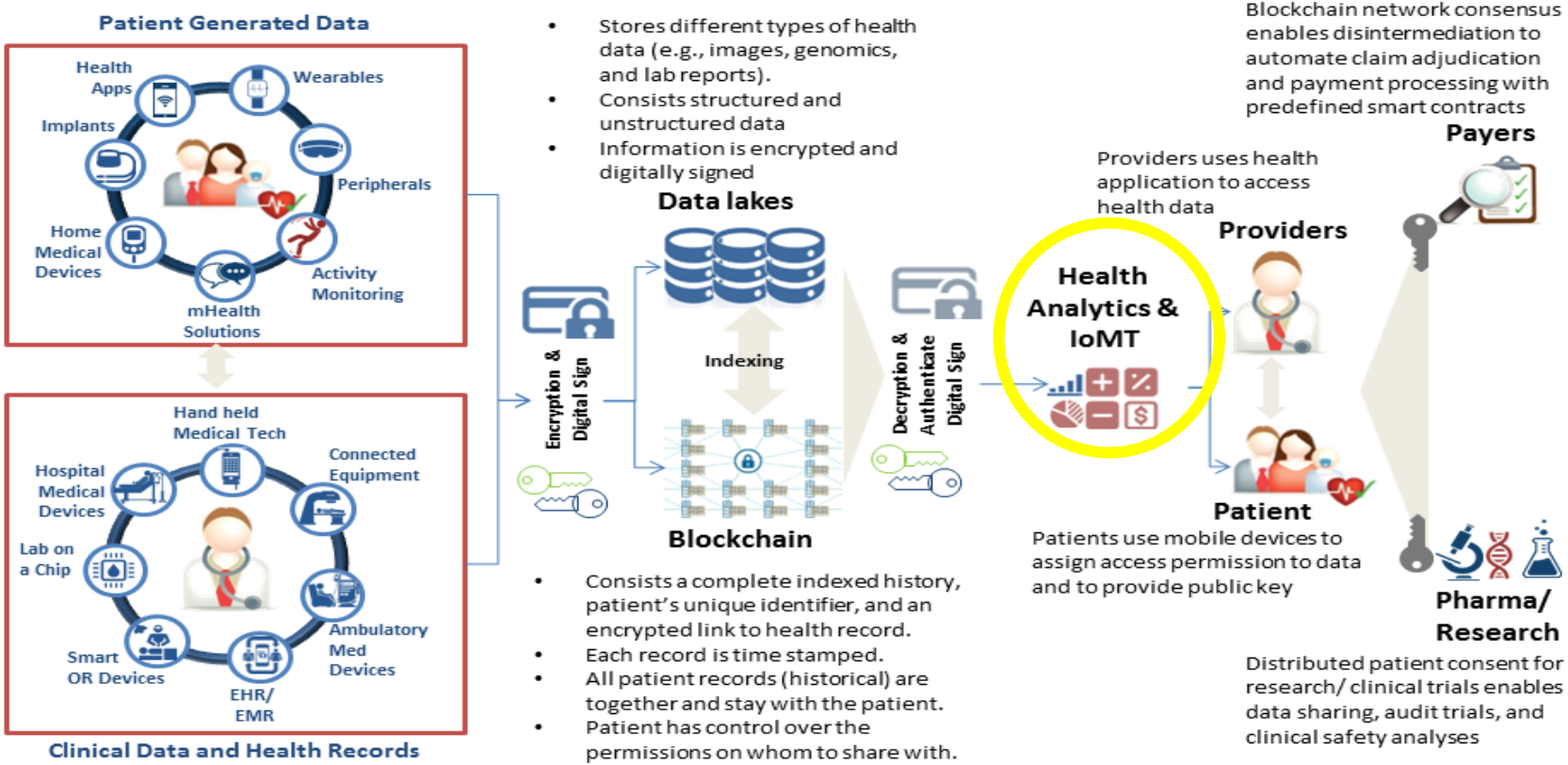
Privacy: Ensure device, personal, sensitive data kept private

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

Blockchain in healthcare use cases



Source: www.healthit.gov; Frost & Sullivan

Health IT leaders experimenting with blockchain in Synaptic Health Alliance launched 2018

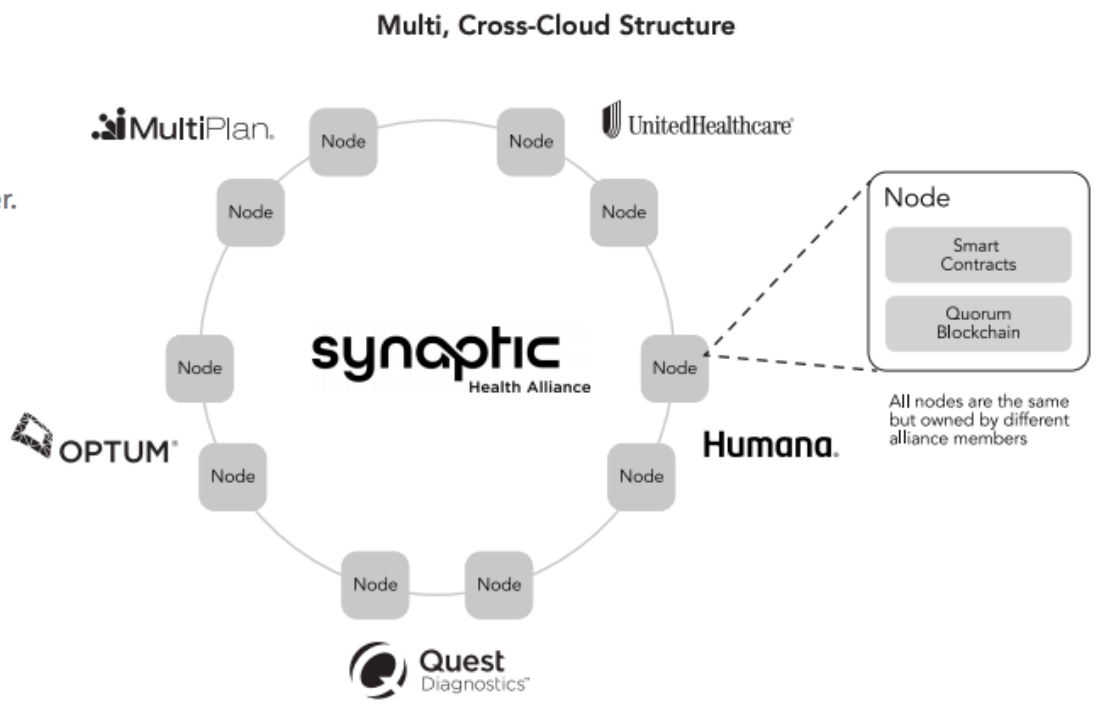
Healthcare IT News

Optum, UnitedHealthcare, Humana, others launch blockchain pilot

The alliance is one of the first, if not the first, national blockchain alliances for healthcare, says Optum engineer.

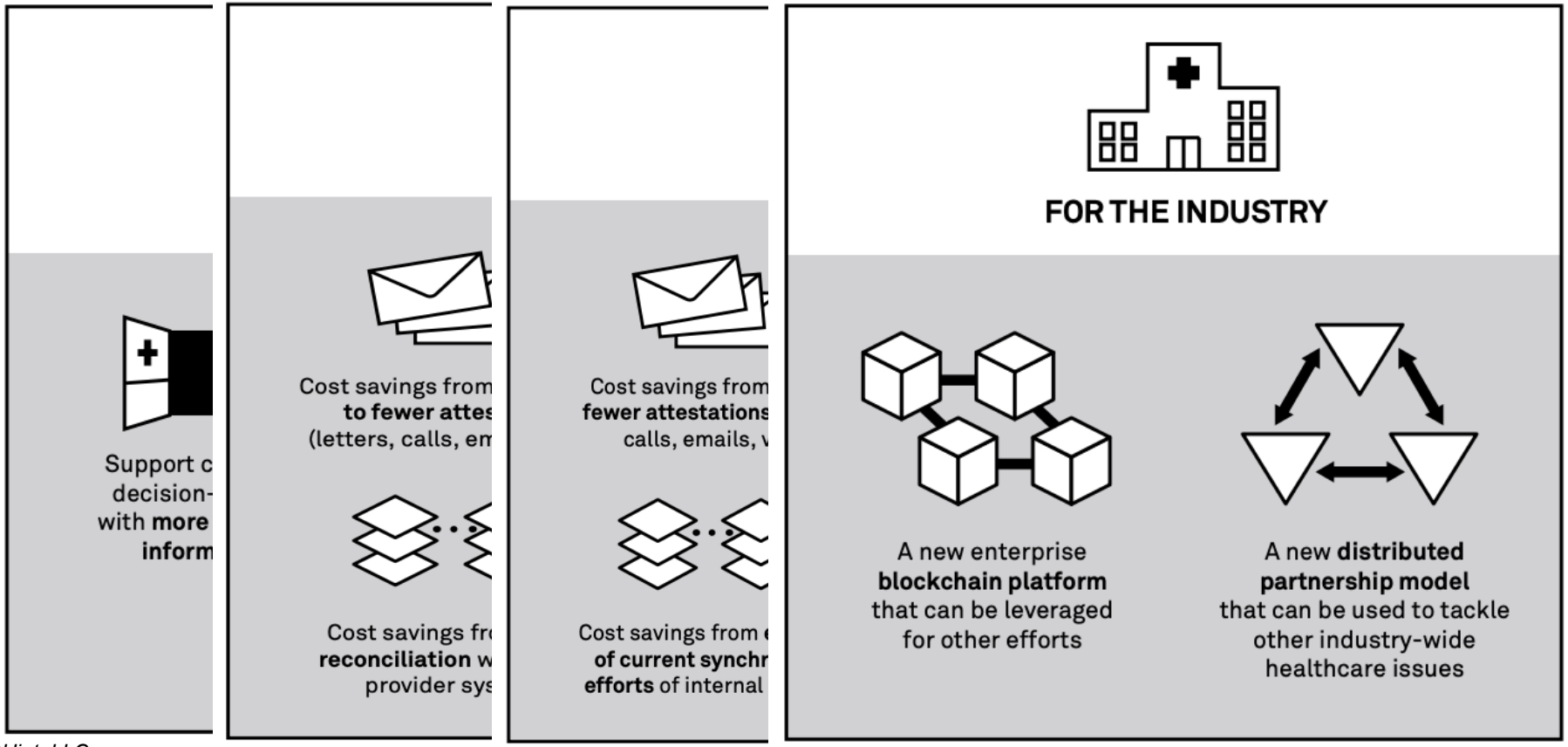
Synaptic Health Alliance includes:

- Aetna
- Ascension
- Cognizant
- Humana
- MultiPlan
- Optum
- Quest Diagnostics
- UnitedHealthcare



Source: https://www.synaptichealthalliance.com/project

Potential benefits of blockchain technology in Healthcare



Source: https://www.synaptichealthalliance.com/project

Focus on Enabling TIPPSS for IoT devices and data -

https://standards.embs.org/members/florence-d-hudson/

DEPARTMENT: INTERNET OF THINGS

Enabling Trust and Security

TIPPSS for IoT

Florence D. Hudson
Columbia University

Editors:
Phillip A. Laplante, Penn State; plaplante@psu.edu

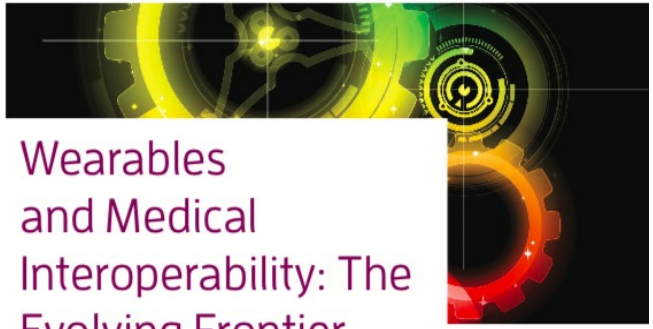
Ben Amaba, IBM; baamaba@us.ibm.com

My first summer internship as an aerospace and mechanical engineer was at Grumman Aerospace Corporation in the 1970s, where I documented the engineering changes to US Navy aircraft—electronics were added to the aircraft so they could communicate with the E-2C Hawkeye for command and control in the air and on the ground. This was long before the connected sensing and actuating systems of systems were called the Internet of Things (IoT), and before we had a commercial Internet. Defense systems were built to be defensive, with trust and security built in.

Today, there are many commercial and personal devices being created without the due diligence to ensure trust and security. Engineers need to ensure the "things" that make up the IoT and the systems they connect to 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 infrastructure using the device are protected, and that we maintain safety and security. We call this TIPPSS for IoT[1] (see Figure 1):

- 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, and so on.

STANDARDS



Wearables and Medical Interoperability: The Evolving Frontier

Florence Hudson, Special Advisor for Next Generation Internet, Northeast Big Data Innovation Hub at Columbia University

Chris Clark, Principal Security Engineer for Strategic Initiatives, Synopsys - Software Integrity Group

Wearables, implantables, and other medical devices are giving rise to rapidly emerging industries that are in need of comprehensive standardization solutions to address security and other needs. To meet these needs, IEEE projects are ramping up quickly.

Wearables and Medical IoT Interoperability & Intelligence (WAMIII), enabled by the Internet of Medical Things (IoMT), is a rapidly growing field. Many patients are wearing IoMT devices—from connected health and wellness devices to connected insulin pumps and implanted pacemakers. Leaders in the field estimate that a vast majority of health organizations—up to 87 percent—plan to adopt Internet of Things (IoT) technology by 2019.[1] The opportunity to leverage WAMIII for improved healthcare and patient outcomes is driving accelerated growth in the market.

Source: "Enabling Trust and Security: TIPPSS for IoT", IEEE IT Professional 2018; "Wearables and Medical Interoperability: The Evolving Frontier", IEEE Computer 2018, ©2018 IEEE

IEEE-SA 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.

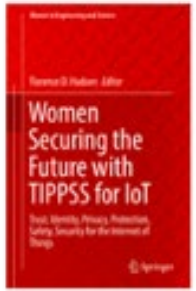
Stakeholders: Medical device manufacturers, hardware, software, and service developers and users for connected healthcare, payers, providers, patients, patient advocates, regulatory.

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

The Book: Women Securing the Future with TIPPSS For IoT

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

Women in Engineering and Science



© 2019

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 individuals from industry, VCs, academia, research, labs, government, Europe, UK, USA.

- *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*

Learn more about Blockchain in Healthcare Use Cases and Research in “Blockchain in Healthcare Today” Open access peer-review journal

- On-line journal
- Published on a continuous basis
- Original manuscripts, use cases, unpublished research
- 26,000 downloads read in 70 countries
- International & Acclaimed Editorial Board
- Available on Alexa!

Hippocratic Oath for Connected Medical Devices. Do no harm, on purpose. Disclose vulnerabilities.

Hippocratic Oath for Connected Medical Devices

I will revere and protect human life, and act always for the benefit of patients. I recognize that all systems fail; inherent defects and adverse conditions are inevitable. Capabilities meant to improve or save life, may also harm or end life. Where failure impacts patient safety, care delivery must be resilient against both indiscriminate accidents and intentional adversaries. Each of the roles in a diverse care delivery ecosystem shares a common responsibility: As one who seeks to preserve and improve life, **I must first do no harm.**

I Am The Cavalry @iamthecavalry iatc.me/oath

BIOHACKING VILLAGE

I Am The Cavalry

Think you found a vulnerability? Disclose it! Try these steps.

- Search for a company's policy on the Internet, review their site for contact information, and check 3rd party coordinator sites.
- Email common addresses, such as security@, psirt@, safety@, etc.
- Connect with 3rd party coordinators, HackerOne, BugCrowd, CERT/CC, ICS-CERT, FDA (AskMedCyberWorkshop@fda.hhs.gov) etc.
- See if anyone in your network has contacts at the company, without inadvertently disclosing the issues.

More at iatc.me/disclosure-resources

Thank You

Florence D. Hudson
Founder & CEO
FDHint, LLC
fdhint.com

florence.distefano.hudson@gmail.com
@Flo4Princeton
@FDHint