TIPPSS to address data-related challenges in development & deployment of digital twins
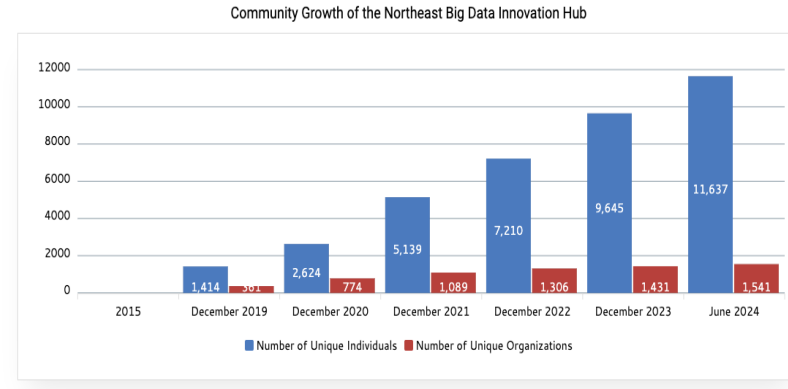
New York Scientific Data Summit 2024: Addressing Data Challenges in Digital Twins
SUNY Global Center, NYC
September 16, 2024

Florence D. Hudson, Executive Director, Columbia University
PI NSF Northeast Big Data Innovation Hub, COVID Information Commons, Proto-OKN
Founder & CEO, FDHint, LLC; Editor & Author; IEEE Engineering in Medicine & Biology Society

1

Northeast Big Data Innovation Hub

- ***Established in 2015 as a community convener, collaboration hub, and catalyst for data science awareness, education and innovation.***

- Our mission is to build a diverse, equitable, and inclusive community for data science learners, educators, researchers and professionals with open, free, online, accessible resources.

- 11,637 individuals from 1,541 organizations, in all 50 U.S. States, plus Puerto Rico, Washington, D.C., and 62 other countries! *Grew 8X since 2019!*

An Overview of our Community

Community Growth of the Northeast Big Data Innovation Hub

	2015	December 2019	December 2020	December 2021	December 2022	December 2023	June 2024
Number of Unique Individuals		1,414	2,624	5,139	7,210	9,645	11,637
Number of Unique Organizations		361	774	1,089	1,306	1,431	1,541

Northeast Big Data Innovation Hub Focus Areas

Education & Data Literacy

- National Student Data Corps (NSDC)
- NSDC Global Chapter Community
- Data Science Resource Repository (DSRR)
- Data Science Flashcard Series

Health

- COVID Information Commons (CIC)
- CIC Student Paper Challenge
- CIC Working Groups
- AIM-AHEAD Data Science Training Core Portal

Urban to Rural Communities

- Transportation Data Science Project (TDSP)
- Climate and Nature
- Smart Cities Data Exchange
- Driver Video Privacy Challenge

Responsible Data Science

Security, Privacy & Ethics

- Responsible Data Science Comic Books
- IEEE/UL 2933 TIPPSS Standard Working Group
- IEEE Cybersecurity TIPPSS for Industry 2024 Workshop Series
- IEEE Connected Healthcare Cybersecurity 2021 Workshops

http://nebigdatahub.org/about/

Leveraging advanced technologies and data can improve insights and outcomes, enable precision medicine
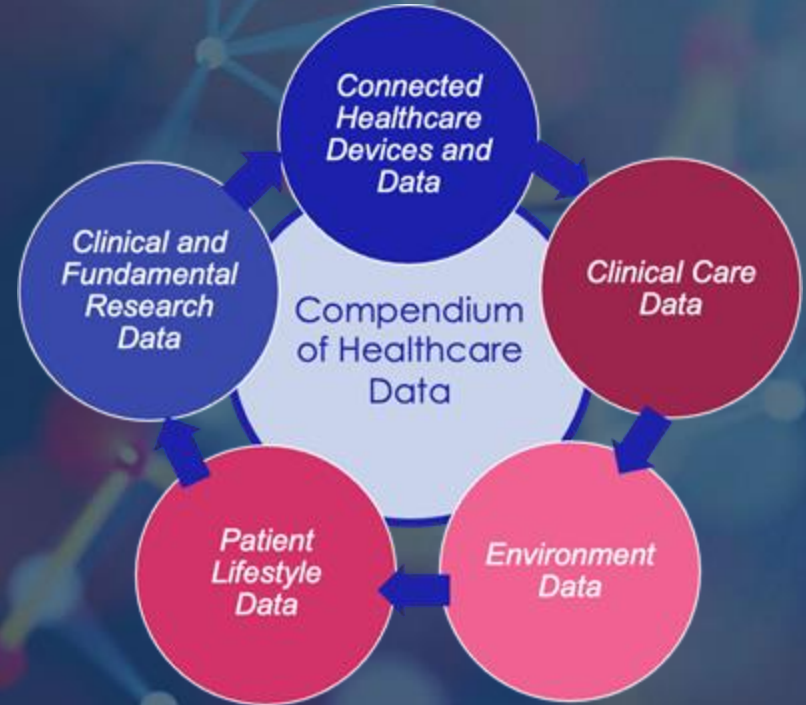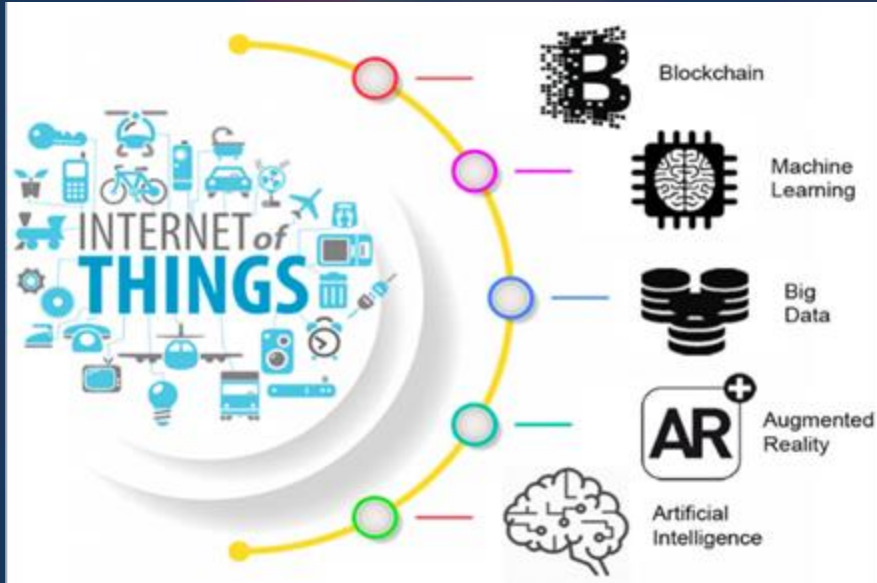
However, more devices and data create more security and privacy attack vectors and risk

"Any medical device connected to a communications network, like Wi-Fi, or public or home Internet, may have cybersecurity vulnerabilities that could be exploited by unauthorized users."

Dr. Suzanne Schwartz
Director, Office of Strategic Partnerships &
Technology Innovation,
Center for Devices & Radiological Health, US FDA
July 2019

Increased connectivity brings increased risk…
What could possibly go wrong? …

US Food and Drug Administration (FDA) identified software vulnerabilities that could let hackers take advantage of personal medical devices dating back as far as 2008.

2017 - FDA Recalled 465,000 pacemakers due to cyber hacking fears.
- Hackers could reprogram 20 types of devices with adjacent access/low skill level.
- RF Telemetry protocol utilized did not implement encryption.

2018 - FDA announced "voluntary recall" of certain internet-connected programmers for implantable cardiac devices due to cybersecurity vulnerabilities, and certain insulin pumps.

2019 - FDA recalled 80,000 insulin pumps due to hacking fears.

Sources: https://www.careersinfosecurity.asia/medtronic-cardiac-devices-recalled-due-to-cyber-concerns-a-11597 ,
https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update ,
https://www.fda.gov/medical-devices/medical-device-recalls/medtronic-recalls-remote-controllers-used-paradigm-and-508-minimed-insulin-pumps-potential

We must secure connected healthcare devices & data while enabling interoperability to help protect the humans

TIPPSS

Top concerns:
- Connected healthcare devices and data
- Connected hospitals, campuses, cities, vehicles
- Clinical, scientific and research device and data integrity

Protection needed regarding:
- Device, hardware, software, service hacks
- Physical health and safety risk
- Financial risk, reputational harm
- Data theft, data integrity, loss of privacy
- Defense in depth – Hardware, firmware, software, service

Need to evolve policy and culture.

Source: https://assets.kpmg/content/dam/kpmg/pdf/2015/12/security-and-the-iot-ecosystem.pdf

"They're going to try to hack everything," warns Florence Hudson of IBM. "I am most worried about security in healthcare, in cars and moving vehicles and in critical infrastructure.

KPMG

Security and the IoT ecosystem

"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, IBM Vice President, 2015

TIPPSS is the new Cybersecurity Paradigm - 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, and sensitive data is kept private
- **Protection:** Protect devices and users from harm – physical, digital, financial, reputation
- **Safety**: Provide safety for devices, infrastructure and people
- **Security**: Maintain security of data, devices, people, etc.

IEEE 2933™-2024 Standard for Clinical (IoT) Data & Device Interoperability with TIPPSS

Purpose: 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.

- Standard Approved by IEEE and UL in June 2024, to be published October 2024
- New IEEE initiative for TIPPSS for Remote Subject Monitoring – join the team!

- IEEE 2933 Working Group is a 2024 IEEE Emerging Technology Awardee

https://standards.ieee.org/ieee/2933/7592/

COVID Information Commons (CIC) - Portal and Community

Consider a Digital Twin Information Commons for Researcher and Practitioner Collaboration

https://covidinfocommons.net/   10

COVID Awards and Researcher (PI) Database

CIC Database includes 13,000+ NSF & NIH COVID-related awards, metadata and PI info.
Search the database by project name, topic, PI name, institution, funder, location.

NSF + NIH COVID Awards and PI Profiles

COVID Information Commons - COVID Research Explorer ML Maps Tool

Clusters projects by topic

Finds semantically-similar documents, even if the documents don't share common words or phrases.

Presents maps of COVID research and researchers by topic or Principal Investigator (PI) name, institution, location

User inputs keyword queries to focus on target domains

https://covidinfocommons.net/

Digital Twins NSF and NIH Awards in the CIC

COVID INFORMATION COMMONS

About | **CIC Search Tools ▾** | Meet the Researchers ▾ | Opportunities & Resources ▾ | Events | News ▾ | Team | Contact

COVID Awards & Researcher Database

COVID Research Explorer ML Maps

Create or Enhance your COVID PI profile

API documentation

13,300 awards + PIs

About | **CIC Search Tools ▾** | **Meet the Researchers ▾** | Opportunities & Resources ▾ | Events | News ▾ | Team | Contact

COVID-19 Research Lightning Talks

Register for the Next CIC Webinar

Video Library

5 Questions with COVID Researchers

141 Lightning Talks

29 webinars

13,800 YouTube views + 1,300 Live Attendees

About | CIC Search Tools ▾ | Meet the Researchers ▾ | **Opportunities & Resources ▾** | Events | News ▾ | Team | Contact

Career & Professional Opportunities

COVID Publications

Groups & Guides

Spanish Language Resources & Outreach

CIC Student Paper Challenge

Datasets

Research Funding

Student Working Group

20 student winners

140+ COVID publications, groups, guides, datasets, funding sources

750 students in CIC WG

Key takeaways

Develop a TIPPSS initiative for biomedical digital twins to increase Trust, Identity, Privacy, Protection, Safety and Security of the data, devices, humans, research, institutions

Build a Biomedical Digital Twins Information Commons Portal and Community, leveraging FAIR principles for Findable, Accessible, Interoperable, Reusable data and research, to enable:
- Research discovery
- Researcher collaboration
- Data sharing
- Lightning talks, webinars, working groups, student projects
- Student and professional development
- Application of the research to practice

Q&A

Thank you!

Florence D. Hudson

Executive Director, Northeast Big Data Innovation Hub at Columbia University

florence.hudson@columbia.edu

https://www.himss.org/what-we-do-opportunities/health-information-and-technology-awards