The Global Connected Healthcare Cybersecurity Workshop on Data & Device Identity, Validation & Interoperability in Connected Healthcare, held on June 16, 2021, was the third in the Global Connected Healthcare Cybersecurity Virtual Workshop Series presented by the IEEE Standards Association Healthcare and Life Science Practice and the Northeast Big Data Innovation Hub. It attracted 50 attendees, including technology and policy experts, healthcare providers, medical device manufacturers, patient advocates, researchers, and payors involved in the design and development of connected healthcare systems.

Welcoming remarks were delivered by the hosts of the workshop series, Maria Palombini, Director of the IEEE SA Healthcare & Life Sciences Practice, and Florence Hudson, Executive Director of the Northeast Big Data Innovation Hub. The opening presentation on *Ensuring Sustainable and Scalable Data & Clinical Internet of Things (IoT) Interoperability with TIPPSS (Trust, Identity, Privacy, Protection, Safety, and Security)*, was delivered by Dr. Orlando Lopez. Dr. Lopez is Director, Dental Materials and Biomaterials Programs, and Coordinator, Small Business (SBIR/STTR) Program, at the National Institutes of Health/National Institute of Dental and Craniofacial Research (NIH/NIDCR). He also leads the interoperability subgroup in the IEEE/UL P2933 standards working group on Clinical IoT Data and Device Interoperability with TIPPSS. Dr. Lopez presented the challenges and opportunities in value-based connected healthcare, and how we can address them with emerging digital technologies, improved data and device interoperability, and related standards. He posited that the desirable attributes of connected healthcare systems are effectiveness, efficiency, transparency, collaboration, compliance, accuracy, scalability, security, trustworthiness, and ethics. Improved interoperability will help us realizate these attributes, providing better integrated and optimized systems for care delivery, disease prevention, and health promotion. Improved data sharing and stakeholder communications can also fuel improvements in scientific discovery, product development, and supply chain security and efficiency. Improving operational efficiency will save time and money, lead to better use of resources, and enable the automation of workflows, which in turn can improve care pathways. The P2933 subgroup which Dr. Lopez leads on Data and Clinical IoT Interoperability with TIPPSS will establish criteria, frameworks, guidance and recommendations to enable scalable, sustainable and adaptable interoperability of clinical data and device systems with TIPPSS. They are accomplishing this task by assessing the connected healthcare ecosystem to identify needs and gaps limiting the interoperability of relevant systems. This assessment includes what is working, what is not working, and what areas offer opportunities for improvement. Dr. Lopez welcomed the workshop participants to join the global P2933 working group to develop standards that enable improved data and device interoperability for connected healthcare.

After the opening presentation, a panel of experts discussed global perspectives on data validation and the interoperability of medical devices in connected healthcare systems. The panel included: Dr. William Harding, Distinguished Technical Fellow at Medtronic, PLC and IEEE/UL P2933 Co Vice-Chair; Jim Nasr, CEO, Acoer; and Simona Carini, Programmer Analyst, University of California, San Francisco, and IEEE P1752.1. They discussed current standards

for interoperability for data, devices, and the humans involved with the devices from the perspective of the patient, caregiver, and provider. As we consider how human identity and device identity interact, including the validation of devices with the people who wear or access them, the panel discussed the potential for traditional forms of identity and access management (IAM) to provide the needed trust and identity elements in connected healthcare systems. Emerging technologies, including Decentralized Identifiers (DIDs), were also discussed as a potential component of the solution as they provide a new type of identifier that enables verifiable, decentralized digital identity in our increasingly decentralized connected healthcare world. Considering recent advances in connected healthcare and the projected growth of clinical IoT devices, the panel encouraged continued innovations and standards efforts in data and device identity, validation and interoperability, such as the IEEE/UL P2933 standard being developed for clinical IoT data and device interoperability with TIPPSS.

After the expert panel discussion, participants were invited to join one of four breakout sessions. These sessions were: Clinical Data and Device Interoperability; Authentication for Human & Device Identity; Data Validation and Harmonization; and Human Factors in Clinical IoT Interoperability. The breakout sessions were facilitated by experts in the field from industry, academia and nonprofits who lead meaningful conversations about each of these topics in the context of healthcare cybersecurity. They encouraged discussion of the challenges, risks, threats, potential mitigation strategies, and recommendations in these areas. Each group's findings were shared with the broader workshop audience, and are highlighted below.

The first breakout session on Clinical Data and Device Interoperability was facilitated by the opening presenter, Dr. Orlando Lopez, as well as panelist Dr. William Harding, Distinguished Technical Fellow at Medtronic, PLC, and David Snyder, Consultant at 42 TEK, Inc. The group established that the interoperability of a multi-vendor network of devices will drive clinical decision-making, and emphasized the importance of validating the devices and data for improved patient care and outcomes. Validating a medical device will allow it to be treated as a trusted player in the system. Trustworthiness of the data is critical to ensure the best care. The group discussed the need for manufacturers to be held to a standard for data accuracy, with the opportunity to leverage HL7 and FHIR for interoperable communications.

In terms of gaps, an underlying issue discussed was the disparity in connected healthcare infrastructure, including various levels of security capabilities and protocols and the range of communications across controlled and uncontrolled networks. Another gap to be addressed in clinical IoT data and device interoperability is the data accuracy issue, including the risk that devices will fail to record accurate data. For example, if the device is not properly calibrated, the data received may be ingested seemingly without an error, but the inaccurate reading could lead to incorrect data which may be promulgated through interoperability. Consequently, devices must be calibrated for accuracy and the data must be validated before it is shared. Another issue discussed was the methodology for establishing which party retains liability for cybersecurity attacks in an interoperability scenario.

Recommendations discussed by the breakout group included securing communications between devices, and validating trust in the device security and the data captured and stored.

Another recommendation was to incorporate biometrics in clinical devices to reduce possible compromises to its security. The use of artificial intelligence and machine learning could also be valuable as this may allow the device to recognize data anomalies or unusual and unexpected data updates, and provide alerts. This could also allow for recognition of unusual attempts to access clinical data and devices. The group agreed that harmonized standards and regulations would be valuable, as this could encourage manufacturers to take responsibility for the processes that relate to their device cybersecurity, and to enable safe and secure interoperability for connected healthcare scenarios. An interesting reference that emerged in this discussion was "Health software and health IT systems safety, effectiveness and security."

The second breakout session on Authentication for Human and Device Identity was facilitated by John Cyrus, IEEE Northern Virginia Section, former USPTO IT Executive, and Dr. Lina Garcés, Associate Professor, Institute of Mathematics and Computer Sciences, Universidade Federal de Itajubá (IMC/UNIFEI), Brazil. The group discussed the challenges of data security related to both the human and the device, for data at rest and data in motion. The group agreed that authentication of the human and the device, initially and on an on-going basis, is important to maintain data security. The challenges discussed included:

- How to verify data ownership when data is being moved between devices and systems
- How to trust and validate whether a connected device has the authorization to use or to modify data produced by another device
- How to track authorization (approval of use) when an individual's data is being used/shared between different devices/components
- How authentication and identity of the individual and device could be managed between systems ruled by different regulations (e.g., data shared between different countries)
- How to deliver technologies and data to other countries with transparency and authentication

Concerning the aforementioned risks and challenges, the team discussed the gap in authenticating user identity, and the need for a system that provides a trusted service with accountability. They recommended the potential use of biometrics for user authentication. The need for worldwide data security system standards was discussed, including current advanced data security systems for healthcare in Japan. In some countries, such as Brazil, many systems were created before data protection laws, and therefore must be updated.

Recommendations included developing a system of trust based on the relationship between humans and devices to track data, decisions and authorization. The systems need to provide tools to validate human and device identity and authentication. The need for external and internal review boards, and checks and balances to ensure authentication and verified access to data and devices, was also noted.

The third breakout session on Data Validation and Harmonization was facilitated by Simona Carini, Programmer/Analyst, University of California, San Francisco, IEEE P1752.1, and David Rotenberg, Senior VP, R&D and Engineering, Telefire, and Technical Editor for IEEE P7012. The main challenge addressed was the existence of multiple systems lacking coherence in data standards which would enable data validation and harmonization with respect to different data

types and formats. It was discussed how data may be validated with machine learning algorithms. Government regulations to protect the data were also mentioned as part of this evolving field.

With regard to the gaps in validating and regulating data, the group recommended regulation in moderation, and an increase in collaboration for global data and system harmonization. The use of machine learning techniques to identify data validation flaws and anomalies was also recommended. Continued work to develop a unifying global standard, if adopted by the majority of countries worldwide, could facilitate the exchange and harmonization of data.

The final breakout session on Human Factors in Clinical IoT Interoperability was facilitated by Mitchell Parker, CISO, Indiana University Health, and Kit (Katherine Grace) August, Ph.D., Research Guest, Stevens Institute of Technology. Many topics were discussed, including digital literacy, universal design, inclusion, and accessibility. Improving the focus on human interaction with systems may lead to more widely adopted clinical IoT systems to improve healthcare outcomes, the scalability of systems, and the confidence of users and stakeholders. Leveraging artificial intelligence, machine learning, and natural language processing of large amounts of data from clinical IoT devices can enable safe and secure interoperability. There is an increasing need for user-friendly data representation, given accommodation needs, for the large amounts of data produced today and in the future. This approach could improve data usability by the healthcare provider and patient. The team discussed how systems can be designed to communicate recommended methods or approaches, and even suggest potential diagnoses, procedures, and actions in various healthcare settings. The interoperability can be enabled behind the scenes while remaining transparent to the user, requiring limited human intervention.

Human factors are increasingly important as healthcare administration and delivery is shifting to a hybrid space between healthcare facilities and the home. Clinical IoT devices are increasingly being used to measure and monitor patients and deliver medicine and care. These devices may be prescribed and provided by medical professionals or introduced by the patient. The plethora of devices may provide the patient with access to a large amount of data that require explanation by a professional. Patient tools to understand the data would help individuals administering self-care, including the ability to share data with professionals to get a second opinion. In sharing the data, the rights for use must be clear. The group also discussed the patient's lack of control over their own data. An important question raised by the group was what to do when a patient or provider knows there is data missing or incorrect, or when a system is not operating properly. Another challenge is privacy and trust and the lack of explicit and contextual guidance in how the data should be treated.

Strategies were recommended on how to take human factors into consideration as related to clinical IoT interoperability. An important step is to establish trust between patients, healthcare providers and connected healthcare systems, so patients feel secure in sharing their data, and providers feel confident in the data to use in healthcare scenarios. Another recommendation is to develop master classes to teach medical professionals how to perform better data analysis and interpret data from all devices, enabling data-driven decisions.

After the breakout sessions, the facilitators and participants gathered in the main session to share breakout discussion findings and open the conversation to attendees in other sessions. The conversation ended with an invitation to the next workshop in the series, which is planned for September 22, 2021. This event will focus on Integrated Systems Design for Connected Healthcare.

Special thanks to the facilitators who moderated the breakout sessions:

- Dr. Orlando Lopez, Director, Dental Materials and Biomaterials Programs, and Coordinator, Small Business (SBIR/STTR) Program, National Institutes of Health/National Institute of Dental and Craniofacial Research (NIH/NIDCR); IEEE/UL P2933 Subgroup Leader on Data and Clinical IoT interoperability with TIPPSS
- Dr. William Harding, Distinguished Technical Fellow at Medtronic, PLC; IEEE/UL P2933 Co-Vice Chair
- Simona Carini, Programmer/Analyst, University of California, San Francisco; IEEE P1752.1
- Jim Nasr, CEO, Acoer
- David Snyder, Consultant, 42 TEK, Inc.; IEEE/UL P2933
- John Cyrus, M.S.E.E, PMP, SMIEEE, Director, IEEE Northern Virginia Section
- Dr. Lina Garcés, Institute of Mathematics and Computing - IMC/UNIFEI, Brazil; IEEE/UL P2933
- David Rotenberg, Senior Vice President, R&D and Engineering, Telefire; IEEE/UL P2933
- Mitchell Parker, CISO, Indiana University Health; IEEE/UL P2933 Co-Vice Chair
- Dr. Kit (Katherine Grace) August, Research Guest, Stevens Institute of Technology; IEEE/UL P2933

<u>The Global Connected Healthcare Cybersecurity Virtual Workshop Advisory Board</u>

- Dr. Mohd Anwar, Professor, North Carolina Agricultural and Technical State University
- Florence Hudson, Executive Director, Northeast Big Data Innovation Hub; IEEE/UL P2933 Working Group Chair
- Ms. Grace Wilson Marshall, Cybersecurity Consultant, FSS TECHNOLOGIES (FSST), IEEE SA
- Ms. Macy Moujabber, Graduate Student, Columbia University
- Maria Palombini, Director, Healthcare and Life Sciences Practices Leader, IEEE SA
- Mitchell Parker, CISO, Indiana University Health; IEEE/UL P2933 Co-Vice Chair
- Dr. Nada Y. Philip, Associate Professor, Kingston University, London; IEEE/UL P2933 Privacy Subgroup Leader

- David Snyder, MBA, PE, CISSP, Consultant, 42TEK, Inc.; IEEE/UL P2933
- Parthiv Shah, Sr. Manager, Security Consulting, Cerner Corporation; IEEE/UL P2933 Security, Protection and Safety Subgroup Co-Leader
- Konstantinos Votis, Researcher, CERTH/ITI; IEEE/UL P2933

Special thanks to the Student Ambassadors from Columbia University and the IEEE Standards Association internship program for their note taking during the breakout sessions and organizing this paper from the proceedings of the breakout sessions held on June 16, 2021:

- Sam Chen
- Paula Guevara
- Hoang Luong
- Haleigh Stewart