The Connected Healthcare Cybersecurity Technology and Policy Workshop, held on December 1, 2021, was the fifth in the IEEE Global Connected Healthcare Cybersecurity (GCHC) Virtual Workshop Series presented by the IEEE Standards Association Healthcare and Life Science Practice and the Northeast Big Data Innovation Hub. It attracted 67 attendees including healthcare, technology and policy experts and advocates. The workshop also included panelists from past workshops in the series.

Opening remarks were delivered by the co-moderators of the session Florence Hudson, Executive Director of the Northeast Big Data Innovation Hub at Columbia University and Maria Palombini, Director and Healthcare and Life Sciences Practice Leader of the IEEE Standards Association.

Webinar attendees were then asked to participate in the first polling question of the webinar, which was: "*How likely is it that regulatory policy, at the country, state, or regional level, will be a catalyst for technology innovations and collaboration in solving connected healthcare cybersecurity and privacy issues?"* Options for answers were: *very likely, somewhat likely, somewhat unlikely, and unlikely*. The majority of participants chose *very likely and somewhat likely* as their answers, pointing towards optimism in approaching regulatory policy. The panelists discussed the poll results, with some agreeing with the participants, citing these policies as incentives for change, while others leaned more towards the *somewhat unlikely* side. Florence mentioned that the European Union (EU)'s General Data Protection Regulation (GDPR) has already been a catalyst for technology innovation and has increased the focus on privacy preservation.

The panelists then introduced themselves and presented their opinions on connected healthcare cybersecurity, technology, and policy considerations. The panel included Dr. Robert Graboyes, a Health Economist focused on technology and innovation and a Senior Research Fellow at the Mercatus Center at George Mason University, U.S.; Dr. Tamás Haidegger, Associate Professor and Director of the University Research and Innovation Center (EKIK) at Óbuda University, IEEE Senior Member, Associate VP for Industrial Activities of IEEE Robotics and Automation Society, and IEEE Hungary Section chair; and Jennifer Stoll, Executive Vice President, Government Relations and Public Affairs at OCHIN (Oregon Community Health Information Network).

The next polling question to engage the participants was: *"Which areas of policy do you feel are most important in connected healthcare cybersecurity and privacy? [Choose all that apply]."* Answers included: *privacy, security, trust and identity, protection and safety, data sharing, interoperability, other (with the option to input a response), all of the above, and none.* Top results from this poll included *Security, Trust and identity, Privacy, Protection and Safety.* Robert

mentioned that he believes all of the aforementioned areas are important and work together to drive improvement. Tamás commented on how people tend to give up privacy for security in a constantly changing world. All of the panelists agreed that priorities are circumstantial and will differ by situation. Florence noted that she leads an IEEE working group on this topic, creating a standard for clinical Internet of Things (IoT) data and device interoperability with TIPPSS - Trust, Identity, Privacy, Protection, Safety and Security, and invited the audience to reach out if they would like to join this standards effort. She also mentioned a book she published with Springer Nature on the topic in 2019 called *Women Securing the Future with TIPPSS for IoT*, and the next to be published in March 2022 on *Women Securing the Future with TIPPSS for Connected Healthcare.*

The third polling question presented to the audience was: *"Which areas of policy do you think have the most promise that we might focus on together in connected healthcare cybersecurity and privacy, leveraging the IEEE community? [Choose all that apply]."* Options presented were: *privacy, security, trust and identity, protection and safety, data sharing, interoperability, all of the above, and none.* Most participants voted for *security, then privacy, trust and identity, and protection and safety.* Once again, the panelists agreed that these policies are so interwoven that it can be difficult to address one while ignoring the others. Jennifer believes addressing privacy policies will not happen in the near future in the U.S.. She hopes that the government sets a national framework to help establish trust, stating that this is a vital cornerstone in healthcare development. She shared as an example the perceived lack of an organized or structured coronavirus management policy in the United States and the resulting issues in increasing popular acceptance of the coronavirus vaccines. Tamás sees data sharing and interoperability as an area with the most promise, but also the most work to be done right now. Improvements in this area will lead to better and more robust systems. He believes that whatever knowledge can be gained from telehealth will be empowered by strong, robust systems that communicate with each other. A participant mentioned that while the list of things to do seems long and insurmountable, he believes the key lies in interoperability with the goal of data sharing, as it ties the rest of the areas together.

After referring to Jennifer's comment regarding the lack of privacy policy in the United States, Florence asked why the EU seems to have figured out their privacy policies ahead of several other regions. Robert mentioned that the EU has a different system of device approval that is a combination of several governing bodies that handle approvals for different devices. This difference in systems could explain, in part, the lack of privacy policy in the U.S. He also believes that the FDAhas strong incentives to delay device approval in the interest of consumer safety, but few incentives to approve devices faster. Tamás added that unless the government makes fundamental changes to the approvals process by pushing more safety responsibilities to the companies, manufacturers will keep creating high-risk devices and avoid potential future liabilities under the auspices of the approving government agency, which maintains complete control over approvals. Insurance companies also play a big role in driving new policies.

Jennifer touched on how historical differences between global regions led to different ways of looking at policies and priorities. Another thing she mentioned is that the U.S. is a federation composed of 50 states, each with a unique different perspective on privacy. Even if the U.S. Congress was to establish a national policy framework, individual States would still have the authority to tweak those policies for their State, turning this policy into a fragmented structure.

One of the participants asked *"To all the speakers, as digital services work across borders easily and help patients [sic] in several countries, how can we achieve a global consensus on a global governance of these systems in an inclusive and fair way? Can this be the WHO [World Health Organization] or the UN [United Nations]? Or does it have to be NGOs [Non-Governmental Organizations]? Or IEEE? Or another organization that either exists now or doesn't exist yet."* Tamás discussed his startup's work with the WHO to bring the benefits of technology to society. He believes that none of these organizations alone can solve the issues being discussed, but maintaining healthy conversations and establishing trust in the groups' work may, one day, lead to solutions.. Robert highlighted the importance of having *decentralized* organizations work together to achieve a common goal, rather than creating a new *centralized* organization that must overcome the difficulties of establishing privacy and security requirements. From an advocacy perspective, Jennifer mentioned that the role of building coalitions aligned with standardized principles that everyone supports. They can bring organizations together to advocate for the same principles. She believes coalitions have not yet been employed in this space. From a position of leadership, IEEE can bring together stakeholders with diverse goals and principles of all nations, moving their policy suggestions forward.

The conversation then moved to an open facilitation with the speakers and guests. Florence invited participants to share the challenges and opportunities that they find at the intersection of technology and policy for global health IoT. Of particular interest were challenges and opportunities related to cybersecurity and privacy. Robert reiterated the importance of having decentralized entities working towards the same goal regardless of the challenges in the way. He and Florence noted examples of ideas that seemed impossible years ago but are now meshed into our lives, like e-commerce, artificial intelligence, and machine learning. One of the participants explained how the compromise of data integrity is a risk that tends to be overlooked when people focus on the more technical aspects, like the patient's trust, medical decisions related to their devices, or the clinicians' trust in the data that they collect. He emphasized the existence of *dirty data* and the issues that arise when evaluating patient safety in the presence of *messy data*. Jennifer explained her work and excitement to be part of a project looking at artificial intelligence and machine learning within the underserved community.

One participant highlighted the reality that technology moves very quickly, but policy often lags behind. Currently, there is a lot of data that is available and the notion of leveraging this data is

already a huge challenge. Data readiness, data engineering, and data structuring will enable additional future capabilities of intelligent systems. They also hypothesized that once patients gain more ownership of their data, the paradigm of how data is viewed and used will change, maximizing the value of data. Once this data ownership is established, some people might not want ownership of their data, or may not know what to do with it, presenting an opportunity for third party agents to provide a digital service in overseeing or managing data according to individuals' particular needs.

The webinar concluded a discussion about the tradeoff between individual data ownership and the product features that would be rendered useless if customers stopped sharing data, creating divergence in the market. Once this happens, companies will need to establish incentives for data sharing and convey the end goal of this data collection and the value it presents to customers. Another comment was made about how in the U.S. healthcare space, incentives are not aligned towards informatics, IT, and data. Instead, they are instead aligned towards care delivery. This presents a skill problem within healthcare technology. This issue is magnified in underserved communities. Currently, healthcare technology and care delivery needs are not being met by the available U.S. workforce, which presents room for job opportunities and career development for those who possess these skills. Applying policies to incentivize the development and deployment of these skills can help fill this gap.

SPECIAL THANKS TO THE FOLLOWING INDIVIDUALS AND SUPPORTERS OF IEEE SA GCHC VIRTUAL WORKSHOP SERIES:

THE EXPERT SPEAKERS

- **Dr. Robert Graboyes, Senior Research Fellow & Healthcare Scholar, Mercatus Center George Mason University**
- **Dr. Tamás Haidegger, Associate Professor, Director, University Research and Innovation Center (EKIK), Óbuda University; IEEE Senior Member, Associate VP for Industrial Activities, IEEE Robotics and Automation Society; IEEE Hungary Section chair**
- **Jennifer Stoll, Executive Vice President, Government Relations and Public Affairs, OCHIN, Inc**

THE PLANNING ADVISORY BOARD

- 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 P2933 Co-Vice Chair
- Dr. Nada Y. Philip, Associate Professor, Kingston University, London; IEEE P2933 Privacy Subgroup Leader
- David Snyder, MBA, PE, CISSP, Consultant, 42TEK, Inc.; IEEE P2933
- Parthiv Shah, Sr. Manager, Security Consulting, Cerner Corporation; IEEE P2933 Security, Protection and Safety Subgroup Co-Leader
- Konstantinos Votis, Researcher, CERTH/ITI; IEEE P2933

REPORT AUTHOR

Special thanks to Ms. Macy Moujabber, Graduate Student Ambassador from Columbia University for her diligent note-taking during the session and organizing this paper from the proceedings of the workshop held on 1 December 2021.