The Global Connected Healthcare Cybersecurity Workshop on Privacy, Ethics, and Trust in Connected Healthcare, the second in the Global Connected Healthcare Cybersecurity Virtual Workshop Series presented by IEEE Standards Association Healthcare and Life Science Practice and the Northeast Big Data Innovation Hub, was held on April 28, 2021. It attracted nearly 100 attendees from healthcare providers, medical device manufacturers, research patient advocates, regulators, and payors involved in the design and development of connected health systems.

Preparatory pre-reads for the workshop were the Data Responsibly Comics and "The Internet of Bodies Will Change Everything, for Better or Worse".

After the opening remarks by Maria Palombini, Director of IEEE SA Healthcare & Life Sciences Practice and Florence Hudson, Executive Director of the Northeast Big Data Innovation Hub, the conversation turned to the panel of specialists to discuss global perspectives on ethics, trust, and privacy in connected healthcare. The panel included Dr. Dipak Kalra, President of the European Institute for Innovation through Health Data; Shaneel Pathak, CEO and Co-Founder of Zamplo; Dr. Deborah C. Peel, Founder and President of Patient Privacy Rights; Dr. Julia Stoyanovich, Assistant Professor in the Department of Computer Science and Engineering at the Tandon School of Engineering and the Center for Data Science at New York University; and Dr. Jeannette Wing, Avanessians Director of the Data Science Institute and Professor of Computer Science at Columbia University. The panelists shared insights on ethics, trust, and privacy in connected healthcare. When asked about the ethical implications of a patient who chooses not to worry about data privacy in order to focus on getting better, Pathak shared how patients lack control over their health data and how some agents use privacy as an excuse for control and not progress. Dr. Wing discussed the Belmont Principles (respect for persons, beneficence, and justice) that guide the healthcare domain but mentioned the need to consider updating these principles in response to the advancements in data collection. In terms of the ethical questions and principles, she mentioned that the discussion on privacy and ethics falls under the beneficence principle, where the value gained by data sharing is weighed against the benefit gained from that action. She stressed the lack of a right or wrong answer in this situation and instead encouraged this consideration on a case-by-case basis in regards to the tradeoff at stake. Dr. Stoyanovich agreed with Dr. Wing and she deepened the conversation by considering who these benefits and tradeoffs are for in the situation at hand. She stressed the importance of identifying the stakeholders, ensuring they are all actively part of the conversation, and the need to educate these stakeholders about what is being done with their data and the benefits and risks that might arise from their use. Dr. Kalra stressed the lack of binary response to the question at hand due to the fact that people are not a homogeneous set, and individually have different views about the extent they want to prioritize knowledge discovery vs. robustly safeguarding their own identity. She concluded that our moral stance must be to help people understand the choices, but then allow them to exercise their choice.

After the keynote panel discussion, participants were invited to join one of four breakout sessions to engage in discussion with some of the panelists and facilitators on one of four topics chosen by the workshop registrants: trust and identity technology solutions; privacy by design; patient-informed consent; and ethical considerations for connected healthcare. Breakout sessions fostered meaningful conversations about each of these topics in the context of healthcare cybersecurity and discussed the challenges, risks, and threats in these areas along with the existent gaps. These conversations were followed by mitigation strategies and developing recommendations for the issues at hand.

The breakout session on Trust and Identity Technology Solutions for Connected Healthcare was facilitated by Dr. Emily Spratt, Fellow at Columbia University and Dr. Mohd Anwar, Associate Professor at North Carolina A&T State University. In defining the challenges, including the relationship between identity and trust, they first established that based on the identity of the individual or product or process, there exists varying levels of trust even though patients or users often do not have a say in these systems. Trust can be on several levels in a system, between patients and devices and even among the devices and different technologies. The perception of stakeholders, such as patients and users, affects their trust towards certain technologies and their level of interaction with them—if any at all. There also exist several barriers in representation, especially for minority patients whose experiences are unique or trust levels are different from the norm. Identity is often transferred, by changing patients on devices, or by representing patients across several devices, where they might show different identities. An interesting article shared during the conversation (https://www.newyorker.com/magazine/2021/04/26/do-brain-implants-change-your-identity) details how having a brain implant that would detect if patients have an epileptic seizure could impact a person's identity and how that would affect patient records.

In terms of gaps, they exist in data collection techniques for socio-technical data acquisition requirements where the data collected are not purely measurements and, therefore, rely on other techniques. Other gaps include creating flexible models for establishing trust in emerging technologies and how the established policies would keep up with innovation. There is a need for procedures and standards to establish identities and trust securely at the provider, patient, and device levels.

As a recommendation, the group decided to create a survey for the technical audience associated with the issue of trust and identity technology solutions for connected healthcare, and the general audience as well, to start creating a record about current perceptions of these technologies in order to base future recommendations on them. The survey can help identify the root causes of data sharing hesitancy to learn if people lack trust in a certain procedure (vaccination for example) or are concerned for their privacy and do not want their data to be shared. Another example is understanding if a patient is afraid that their shared data might affect their ability to apply for life insurance. Determining the root causes of these fears can help better design devices and systems in the future to make them as user-centric as possible. After the initial survey, there would also be a need to redistribute it over several points in time to establish benchmarks as to how this perception is growing or changing along with the rapidly-evolving industry.

The breakout on Privacy by Design was facilitated by: Parthiv Shah, formerly Senior Manager of Cybersecurity Services at Cerner; Dr. Nada Philip, Associate Professor at Kingston University London; and Mary Hodder, Technical Editor for IEEE P7012. When discussing challenges and risks present in the topic of privacy by design, points included: human challenge, where individuals might not believe that privacy by design is necessary from the get-go; and, unintended consequences to legislature such as misinterpretation or individuals not following the rules unless absolutely necessary. When asking for consent, there is often a question of what exactly the consent is for and what the request entails. Also, can we facilitate interpretability and create standards? Who has the power in the privacy dynamic and how do you distribute this power and make this more equitable?

Concerning gaps in addressing the aforementioned risks and challenges, there seems to be a gap in data ownership and jurisdiction. Who owns the data? Data should be treated in a copyright model with co-creation rights instead of as an ownership. There should not be a binary sign-off for data rights. We currently lack a roadmap that shows us how to build devices that include privacy from the get-go as well as an ecosystem that considers and sustains privacy. Individuals often provide consent but do not understand the extent of their consent and the rights involved. Also, there exists a disparity between the intent of the regulation and its implementation that should be addressed.

As recommendations for challenges in privacy by design, ideas include educating the developers and the end users using a preset repository of terms, and creating some form of a receipt for individuals as a record to what they have agreed. Privacy compliance reports have to be more regularly checked, considering distributed ownership, like a copyright model.

In the third breakout room, panelist Shaneel Pathak and Dr. Hsun-Hsein Shane Chang, Director of Science at Novartis led the conversation on Patient Informed Consent in Global Connected Healthcare. Regarding challenges and risks, participants mentioned how traditionally, physicians received consent from patients in a direct interaction. Nowadays, however, the process is much more complicated. Patients are facing several different types of devices, and data collection is not as direct as it used to be. Forms for data collection have issues pertaining to patients being in different geographies and circumstances. Therefore, a standard form will no longer suffice for all data collection requirements. Other issues include the lack of bridging between clinical protocol and consent as well as the inability to customize forms for each individual patient.. It is also hard to gage the patient's understanding of what is being agreed to and the difference between signing off on a form and understanding its contents. Finally, one participant mentioned a case in their home country where not only do they have more than 200 languages, but they also have a large population of illiterate citizens. In this case, they not only face an issue of translation but of effectively communicating data collection consent through other methodologies.

In terms of recommendations to address these challenges, participants mentioned investing in public health and education, raising awareness of patient rights through one-pagers with more information and infographics, and validating their consent by asking patients follow-up questions. Governments, companies, and patients should work together. The responsibility falls

on governments to provide policies, set up regulations, and implement education schemes; whereas, companies are responsible for creating well-defined protocols of study or product deployment. There is also a need to make patients understand what data is to be collected, how it will be processed and shared, and their rights in this process, and how to leverage technology to deploy this through interoperable devices, using Natural Language Processing, machine translation, infographics, etc. Finally, discussions emphasized using incentives to improve the stakeholders' engagement in adopting consent and a patient-centric approach.

In the last breakout room, Dr. Forough Ghahramani, Associate Vice President for Research, Innovation, and Sponsored Programs at NJEdge; Dr. Becky Inkster, Neuroscientist with The Lancet Digital Health and International Advisory Board Member; and panelist Dr. Dipak Kalra, led the conversation on Ethical Considerations for Connected Healthcare. A challenge that arises is in the definition of connected healthcare, which can differ from the perspective of the person, device, or provider and is subject to different cybersecurity standards. There is a question of the kind of information needed to create an outcome in connected healthcare—how do you use connected technology to come up with a diagnosis? Another challenge is that many clinicians are involved in the process while each is coming from siloed angles. Therefore, data needs to be integrated to be useful. On "paperless" healthcare, it is important to have a flow of information and give patients access to information. Another obstacle is the separation of data between emergency electronic medical records (EMRs), which could lead to disjointed care. In mental health, for example, the patient has to re-tell painful stories. Some issues also arise in regards to data quality in cases of misrepresentation of data, data loss, and not taking into consideration representative demographic data. When linking data, these issues can add increased challenges around bad actors and cybersecurity (example of selling data and harming the patient). While legislation helps to a certain extent, EMR vendors are all different and do not make it easy to approach a more interoperable system. H-IOT (Health - Internet of Things), which are healthcare-enabled devices, are sensitive to health-related data and impact the delivery of healthcare, which brings up a host of ethical challenges. A primary challenge of H-IoT is to ensure that devices and protocols for sharing the data that they create are technologically robust and scientifically reliable, while also remaining ethically responsible, trustworthy, and respectful of user rights and interests. Another major area of challenge is the difference in priorities and rankings based on individual and cultural preference on several topics. On privacy and trust, on the European level, there are still speculations about whether data can be trusted, but in the United States there seems to be more trust in general. Opinions also differ in contexts of public and private institutions and area of residence. Data can also be manipulated and can consequently impact employer requirements and travel restrictions. The case of COVID-19 vaccines and the opportunity to falsify this data presents strong support to this issue. Also, the presence of a centralized healthcare system in a culturally diverse population and healthcare providers may give rise to a set of ethical issues. For example, in relation to patients' waiting time for medical attention, lack of comprehension resulting from cultural differences, the language barrier between the healthcare providers and the patients, and issues relating to eligibility to health care, are all factors that should be addressed. Major ethical issues arise in patient rights, equity of resources, confidentiality of patient information,

patient safety, conflict of interest, ethics of privatization, informed consent, dealing with a person of another gender, beginning and end of life, and healthcare team ethics.

As recommendations, it is useful to follow Heinz von Forster's ethical imperative "Act always so as to increase the number of choices." To see progress, educate all the stakeholders including patients, physicians, device manufacturers, and everyone involved in between, and engage all in decision making. Another important suggestion is to establish strong guidelines. The higher authorities in the health delivery system hierarchy must initiate more in-depth discussions on the ethical issues to ultimately bring about changes in policies, particularly on resource allocation. Although a code of ethics need not lay down rules that are set in stone, it can provide guidance to deal with ethical issues as they arise. The HIPPA act (the U.S. Health Insurance Portability and Accountability Act) helps combat resistance in the market, enables the appropriate people to have access to the data, and allows patients to move their data. Providing patients with their data might allow them to identify conditions sooner and apply early intervention when necessary. Fitbit, for example, allows people to see some aspects of their health and motivates them to improve it. Also, in the case of patients with diabetes, sensors allow patients to track their levels at all times providing them with more autonomy. Finally, it is vital to leverage learnings and best practices from other industries.

- An article highly recommended for reading is: **https://www.newyorker.com/magazine/2021/04/26/do-brain-implants-change-your-identity**
- Additional resources include the cybersecurity in digital mental health project:
  - https://www.youtube.com/watch?v=irgyh0XqVuY&feature=youtu.be
  - https://www.beckyinkster.com/cybersecurity
  - https://www.beckyinkster.com/cybersecuritybackground

After the breakout sessions, the facilitators and participants gathered in the main room to share their discussion findings and open up the conversations to participants who were in other rooms.

Special thanks to the facilitators that helped moderate the breakout sessions:

- Mohd Anwar, Professor, North Carolina A&T State University
- Dr. Hsun-Hsien Shane Chang, Director of Data Science, Novartis
- Dr. Forough Ghahramani, Associate Vice President for Research, Innovation, and Sponsored Programs, NJEdge
- Mary Hodder, Technical Editor, IEEE P7012
- Dr. Becky Inkster, Neuroscientist, The Lancet Digital Health, International Advisory Board Member

- Dr. Emily L. Spratt, Columbia University
- Shaneel Pathak, CEO & Co-Founder, Zamplo
- Dr. Nada Y. Philip, Associate Professor, Kingston University London
- Parthiv Shah, Sr. Manager, Security Consulting, Cerner Corporation

SPECIAL THANKS to the Student Ambassadors from Columbia University for organizing this paper from the proceedings of the Breakout Sessions on 28 April 2021

- Haruki Gonai
- Abhishek Sinha
- Hoang Luong
- Benjamin Sango
- Macy Moujabber