The Global Connected Healthcare Cybersecurity Risks and Roadmaps workshop, the first in the Global Connected Healthcare Cybersecurity Virtual Workshop Series presented by IEEE SA and the Northeast Big Data Innovation Hub, was held on February 24, 2021. It attracted more than 60 attendees from healthcare, technology, research, academia, industry, and government entities across the globe.

The workshop kicked off with a keynote by Julian Goldman, MD, Medical Director of Biomedical Engineering at Mass General Brigham Health Systems and Director of the Medical Device Interoperability Program – a multi-institutional federally funded program to advance medical device interoperability to improve patient safety and Health IT innovation.

Goldman first highlighted that cybersecurity must be considered in context as it is system-dependent. He elaborated on the generalization of rules and procedures that often overlook several scenarios in healthcare cybersecurity. Another challenge that is present in cases where patients have an infectious disease and has become more prominent during the pandemic is that physicians cannot hear alarms outside the room or control the machines without stepping in. The deployment of new ventilators with non-interoperable data connections made it almost impossible to hear ventilator alarms from patients in isolation rooms due to the inability to connect remote alarm systems. This situation creates the need for "alarm sitters" who are hospital staff that sit out in the hallway and call for help when they hear an alarm. This became an acute issue during the COVID-19 pandemic. Another issue is the inability to transmit ventilator data to EMR (Electronic Medical Record) flow sheets. Solutions to these problems include a remote control to facilitate controlling the ventilator outside the patient's room. As a response to the pandemic, the FDA released several Immediately in Effect Guidance documents regarding currently-FDA-approved devices that allow the addition of a remote control, which many companies employed; however, that, in turn, brought up several layers of considerations and challenges. Goldman highlighted the National Emergency Tele Critical Care Network (NETCCN), an initiative that is part of a virtual hospital concept with additional capabilities focused on building a virtual critical care ecosystem based on very light technologies like smartphones. It would allow critical care experts to provide teleconsultation, coverage, and support to bedside caregivers, especially in rural areas. During the time of the COVID-19 pandemic, tele-critical care is especially important because it reduces exposure, provides more access to resources, and augments capacity.

After the keynote presentation, participants were invited to join one of four breakout sessions to engage in discussion with subject matter experts on four topics: security and interoperability; privacy, ethics, and trust; technology and policy consideration; as well as software and hardware supply chain and proactive risk mitigation. Breakout sessions featured meaningful conversations about each of these topics in the context of healthcare cybersecurity and covered the challenges, risks, and threats in these areas followed by identifying and discussing the gaps and mitigation strategies, and developing recommendations for a standards roadmap into the future.

The breakout session for Security and Interoperability in Connected Healthcare was led by Parthiv Shah from Cerner and Mohd Anwar from North Carolina A&T State University. When asked what cybersecurity risks or threats they are most concerned about when using medical devices, participants shared the worry of compromised credentials that allow people to access a system, change privileges, and alter readings and results. This risk raises questions such as: Is password protection enough? How do we train and successfully execute security awareness for the systems and humans involved? What is the difference between administrator and user access? What are the hazards if user access is overly constrained? How do we incorporate FDA pre- and post-market guidance? Other risks and threats discussed include how devices can be deployed beyond the healthcare environment, for example at home, and the accompanying increased risks. Another issue is understanding context, use cases and requirements of the software bill of materials, including updates and maintenance to ensure software security, ensuring firmware updates for internet connected devices, and managing embedded operating systems. These issues all revolve around the risk of requiring layered security and ensuring this security is solid and updated at every stage. In terms of future innovation and applications, when asked what worries them most when it comes to security of medical devices in the future, participants mentioned the following:

- User and device authentication, device intercommunication, and credentials of humans.
- Inequity in costs, healthcare access, and access to education.
- How artificial intelligence and machine learning factor in, who manages this factor, and how this impacts the delivery of healthcare services.
- How systems are being used in different places.
- Telemedicine and robotic surgery in the future in terms of how systems and humans can accurately deliver the service and minimize associated errors.
- The ecosystem of medical technology that is not built to be managed by way of privacy and security. How are devices in this ecosystem configured? Are they vulnerable? If yes, to what?
- What is the trade-off between new life-saving technologies and the potential for attack or problems with systems that can harm lives and push innovation back?
- Can devices in the future be autonomous or is that far-fetched? What is the difference between standalone devices operating through their own sensors and interconnected devices, like traffic lights, for example?
- How do hospitals trust these devices? When they are removed, how do we ensure they are also removed from the trusted list?
- How do we identify devices? What are the risks included in wireless intrusion entry, where human workers double check the identity of machines, access, and the association of devices?
- Understanding the context of trust. How do we develop use cases and ultimately decide to trust devices in some scenarios over others?
- How do we ensure the relation between user identity and device identity?

- How do we achieve accurate baselining? How does a false baseline affect the device, and if it yields false negatives or false positives?

In terms of gaps in security and interoperability in connected healthcare, participants mentioned the trust in the source and the data, the source tied to device authentication, system complexity, and the temporality of trust, i.e., what can be trusted today might not be trusted tomorrow.

Finally, in a case study, facilitators mentioned that “We all state that you should never deviate from your incident response plan when it comes to responding to a cybersecurity incident. Would you deviate from it if the incident was related to a medical device? Would it be better to have a separate incident response plan for medical devices/IoMT (Internet of Medical Things)?” The first instinct was to stop the treatment immediately, but secondary thoughts include considering if the patient’s life is jeopardized if the treatment is stopped. They identified the need for a break-the-glass policy that is dependent on the context and the device. Finally, there should be a differentiation between the break-the-glass strategy and creating a different medical device incident response plan.

In the breakout session moderated by Emily Spratt from Columbia University in New York and Nada Philip from Kingston University in London, participants discussed Privacy, Ethics, and Trust in Connected Healthcare. In terms of challenges and risks in this area, the topic of applied uses of technology for healthcare vs. the ethics of technology in general was discussed. Uses of AI(Artificial Intelligence) in healthcare specifically brings out questions in AI more broadly and its applications, such as local vs. cloud data storage. Participants mentioned how user perspective is often not factored into the medical discussion, despite it being essential for the care of interactive healthcare, such as in the case of a pacemaker. “In non-clinical environments, as implantable, wearables, telehealth, and m-usage (mobile usage) increases, we have to consider the privacy, ethics, and trust in homes, assisted living facilities, schools, and other arenas,” said one participant. Another question discussed was that with the existence of more data and data types, how do we link that information back to individuals, and how do we handle consent and differential privacy?

In terms of gaps in ethics and trust in connected healthcare, participants mentioned that when data flows become continuous from implants and wearables there are special problems in non-anonymizing, and the very communication raises both communication security issues as well as how the integration of AI can be linked to their data flows. Another gap is how ethics are interpreted very differently by organizations and people. There exists varied contexts and perspectives in the many professions now converging in digital medicine. Another participant mentioned the complexity that exists on the mere sensor data level, therefore bringing up the need to create further distinction between sensor data captures, the secure transport of this data, and the machine learning aspect of this data. In addition, there is a need to build a basis for understanding these various aspects to allow for trust to emerge. Standardizing the level of knowledge would allow for more advanced discussions in AI. Further identified gaps include the understanding of consent and trust by the public. How sure can you be of the real meaning of ‘informed consent’? What does this mean for trust and how can we be sure what it is based on?

Proposed potential mitigation strategies include addressing levels of vulnerability by creating architectural frameworks to address them. These frameworks give way to trust and compliance measures. From a risk management perspective, there is a challenge in providing a sense of security with the existence of limitations that require flexibility and openness. Another aspect of mitigation is keeping up with the evolution of cybersecurity and unknown future threats. Also, there is the need to designate ownership and responsibility potentially in the form of regulatory agencies.

As for recommendations, discussions concluded that frameworks should be more global, rely on the ethics system, and include the patient perspective. Patients should be able to decide how much information they want to share based on their level of comfort and consent. Agency should be provided for patients to be treated as people rather than research subjects, keeping in mind that the people are the purpose of the object and not the other way around. There is a need for a consent management framework to help explain consent in an accessible way to patients, explaining what will be used and how it will be used with the goal of making it easier for patients to understand to what they are consenting. (An interesting read on this topic is Research from Deepti Anand: https://www.indiastack.org/depa/)

On the topic of Technology and Policy Considerations in Connected Healthcare, in the breakout session facilitated by Shane Chang from Novartis and Forough Ghahramani from NJEdge, participants identified several areas of focus on the topic. In terms of infrastructure, healthcare systems must provide the capability for secure connectivity and set the standards for private vs. public devices. Data flow and the liquidity of interoperability is dependent upon the clinician’s use at the time. A liver transplant, for example, is discrete. The selectivity and timeliness of instances is important. Data representation is different among clinicians. What is humanly available to one clinician may be different from another. Therefore, there exist issues in transference latency. While moving to advanced capabilities, we have to be sure we are using the same data points. In terms of data acuity, there is a need for data to be volumetric without letting other data get in the way during data processing. Data acuity can make data more or less relevant. Predictive analytics can be present on each instance during which the scenario is presented along with the best experience or advertisement for that moment. Further challenges include the balance between seamless user experience and data safety, real-time data and control, importance of latency in remote monitoring, the need to address control of data, and the proper balance of data. Risks in communication include the need for guaranteed minimum bandwidth for real-time healthcare services, and encrypted and secured private connectivity in the operating room. As for IoT devices, challenges exist in data gathering and communication between hospitals, tracking, and even between devices in the same room. At the moment, very little of the data is interoperable and challenges still exist in cloud-based dashboards for data collection. On the topic of voice-enabled devices, there is a need for communications platforms to provide timely communication between clinicians. There also exists the topic of allowing audio archival and proxy calling to better monitor high data acuity exchanges. Participants also mentioned the need for standards for interoperability with an example that if the same device supplier transmits data at the same time, depending on the interests of the viewer, they can look at different aspects of the data. This can be supported by creating standards for devices from different suppliers and ensuring accompanying policies are enforced. While authorities have been pushing standards for years, data is still not interoperable, which reinforces the need for policies on standardization, identification, and authentication of devices for IoT systems.

As recommendations for the aforementioned challenges, participants mentioned establishing an interoperability standard that would encourage different manufacturers to speak the same technological language. Defining interoperability will allow for more advances once the concept is clear to everyone involved. This also goes hand-in-hand with the need to come up with new paradigms and establish technical documentation. From a policy perspective, researchers need to filter out which areas need to have full-stack integration because of criticality of care, which areas are not as important, and in which areas it is not needed. Finally, it is recommended that government enforcement be strengthened within a single country and across countries. For instance, reliable infrastructure is critical for connected healthcare. Electricity, heat, water, and communication providers need to be able to guarantee services wherever necessary.

In the final breakout session on Software and Hardware Supply Chain Security and Proactive Risk Mitigation facilitated by Mitch Parker from Indiana University Health and David Snyder from 42TEK, Inc.,participants also discussed the challenges, risks, and gaps. They then moved on to mitigation strategies and recommendations. In terms of challenges, there is a need for long-term device component software support as well as long-term operating environment support. Challenges exist in cases of configuration change support to deal with what happens when cloud providers or supply chain components change mid-stream. There is a lack of incentives for manufacturers to monitor each step and build in secure practices. Open source presents vast opportunities but also presents challenges like invading user systems. FDA guidance is currently acting as more of a recommendation than a “force of law” and therefore there is a lack of uniformity. In line with the challenges and risks, the gaps in software and hardware supply chain and proactive risk mitigation in connected healthcare include lack of enforcement and that people do not know what they have to do. How do they search for material from manufacturers and vendors? There is a lack of prescriptive guidance that leads to identifying breaches at a late stage (when it has already happened) as opposed to during earlier times. There is also a need for resources for risk assessment and contract negotiations.

To address these challenges and gaps, mitigation recommendations include producing a Software Bill of Materials (SBOM), screening the device and components at the procurement stage, and monitoring hardware and software during the day-to-day of the operating phase. Other mitigation strategies include alignment with established international standards and deviating towards top-down goal-oriented leadership as an antidote to fragmentation. In terms of recommendations, they include developing a plan with well-established and reasonable goals to address these problems with industry input and moving the process from theory to implementation. Recommendations also include providing incentive programs to manufacturers, mandating good compensating sets of controls to use, providing a more ubiquitous platform, and addressing insecure legacy equipment with incentives, compensating controls, and deadlines.

Relevant links provided by the facilitators and participants include the following:

- Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) V2.0. September 2020. https://healthsectorcouncil.org/hic-scrim-v2/
- Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. National Institute of Standards and Technology. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Cybersecurity in a Complex Healthcare Ecosystem - Remote Patient Monitoring Data Supply Chain. February 2021. https://42tek.com/RPM-system-cybersecurity.pdf
- The SolarWinds Hack and The Arrival of Software Supply Chain Attacks. December 18, 2020. https://www.breachlock.com/the-solarwinds-hack-and-the-arrival-of-software-supply-chain-attacks/
- Validating the Integrity of Computing Devices - Supply Chain Assurance. National Institute of Standards and Technology, National Cybersecurity Center of Excellence. March 2020. https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/tpm-sca-project-description-final.pdf

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

Mohd Anwar, North Carolina A&T State University
Shane Chang, Director of Data Science, Novartis
Forough Ghahramani, Edge
Emily Spratt, Columbia University
Mitch Parker, Indiana University Health
Nada Philip, Kingston University London
Parthiv Shah, Cerner Corporation
David Snyder, MBA, PE, CISSP, Consultant, 42TEK, Inc.

The Global Connected Healthcare Cybersecurity Virtual Workshop Advisory Board

Mohd Anwar, Associate Professor, North Carolina A&T State University
Florence Hudson, Executive Director, Northeast Big Data Innovation Hub and IEEE/UL P2933
Ms. Grace Wilson Marshall, Cybersecurity Consultant, FSS TECHNOLOGIES (FSST), IEEE SA
Ms. Macy Moujabber, Student, Columbia University

Maria Palombini, Director, Healthcare and Life Sciences Practices Leader, IEEE SA
Mitchell Parker, CISO, Indiana University Health
Dr. Nada Y. Philip, Associate Professor, Kingston University London
David Snyder, MBA, PE, CISSP, Consultant, 42TEK, Inc.
Parthiv Shah, Sr. Manager, Security Consulting, Cerner Corporation
Konstantinos Votis, Researcher, CERTH/ITI

SPECIAL THANKS to the Student Ambassadors from Columbia University for organizing this paper from the proceedings of the Breakout Sessions on 24 February 2021.

Teah Selkin
Haruki Gonai
Haleigh Stewart
Macy Moujabber