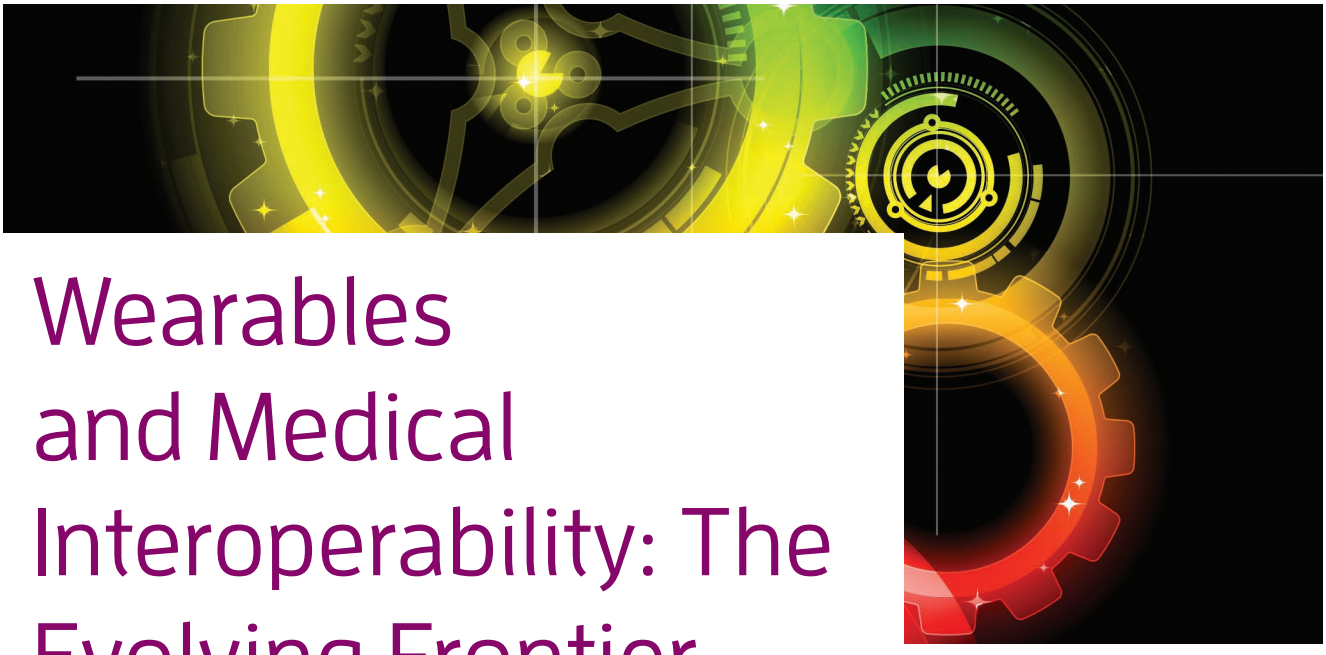

Wearables and Medical Interoperability: The Evolving Frontier

Florence Hudson, Special Advisor for Next Generation Internet, Northeast Big Data Innovation Hub at Columbia University

Chris Clark, Principal Security Engineer for Strategic Initiatives, Synopsys - Software Integrity Group

Wearables, implantables, and other medical devices are giving rise to rapidly emerging industries that are in need of comprehensive standardization solutions to address security and other needs. To meet these needs, IEEE projects are ramping up quickly.

FROM THE EDITOR

The field of wearables, implantables, and other medical devices is rapidly growing and so is the need for standardization, especially in areas like device and system security. To address this emerging need, workshops are being held to foster discussion and learning about the opportunities and challenges surrounding data interoperability of wearable devices within the connected health wearable system – users, software, communications, networks, data, hardware, services, firmware, and more. *–F.D. Wright*

Wearables and Medical IoT Interoperability & Intelligence (WAMIII), enabled by the Internet of Medical Things (IoMT), is a rapidly growing field. Many patients are wearing IoMT devices—from connected health and wellness devices to connected insulin pumps and implanted pacemakers. Leaders in the field estimate that a vast majority of health organizations—up to 87 percent—plan to adopt Internet of Things (IoT) technology by 2019.[1] The opportunity to leverage WAMIII for improved healthcare and patient outcomes is driving accelerated growth in the market.

WAMIII also creates risk. Wearables and implantables can be hacked. As reported by CNBC in 2016,[2] a security expert hacked his own insulin pump. The U.S. Food and Drug Administration (FDA) released an FDA Safety Communication in 2017 to announce that there were 465,000 implanted pacemakers requiring a firmware update to address cybersecurity

0018-9162/18/$33.00 © 2018 IEEE

EDITOR **F. DON WRIGHT**
Standards Strategies; don@standards-strategies.com

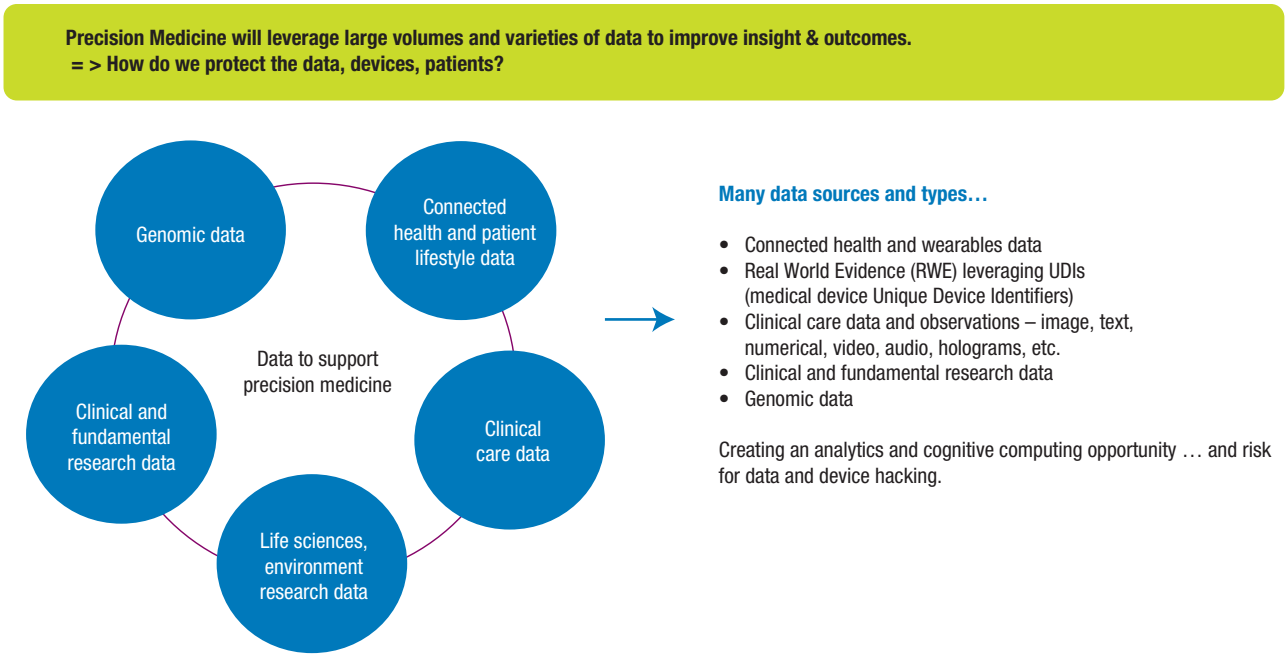

Figure 1. Precision Medicine. (Source: F.D. Hudson, NIH 2015; *"Medical Devices in the Real World," *New England Journal of Medicine*, vol. 378, no. 7, 2018.)

vulnerabilities identified in Abbott's (formerly St. Jude Medical) Implantable Cardiac Pacemakers.[3] These wearables and medical devices are from manufacturers we have known and trusted for many years. Unfortunately, the ability to hack these devices is known, and cyberattacks that can impact human lives are an increasing risk we must address.

The promise of improved healthcare and patient outcomes with precision medicine depends on leveraging many types of data from many sources—from wearables providing connected health and patient lifestyle data; to clinical care and research; to plant, animal, and human genomic data. The need for data sharing is increasing (Figure 1).

The Cancer Moonshot Summit at Howard University in Washington, DC, in 2017 resulted in a series of "New Actions to Accelerate Progress Toward Ending Cancer As We Know It," including accelerating and increasing data sharing.[4] Healthcare and medical data interoperability is at the core of curing and treating cancer via mobile health or IoMT. Actions committed as a result of the Cancer Moonshot Summit included creating a foundational system for broad sharing and analysis of cancer genomic data, which is critical for advancing the field of precision medicine and improving the care of cancer patients. This data must be protected and kept secure both at rest and in motion to ensure proper insights and maximize patient safety as new treatments are determined from data analysis. Also, the Massive Acceleration in Prevention Science (MAPS) collaboration was announced, aiming to lower the smoking rates for at-risk populations that have higher incidences of undiagnosed lung cancer and to prevent cervical and other cancers due to human papillomavirus (HPV). The program will use social media, mobile health, and a variety of technological interventions to enhance traditional approaches for reducing smoking and tobacco use.

The increased use of secure data sharing can save lives, improving the full context of a patient's clinical information and the other data elements leveraged in precision medicine. As stated in CIO Magazine, "We've killed more people because we didn't share data than because we did."[5]

To address the opportunities and challenges for interoperability and security associated with wearables, IoMT, and medical devices, IEEE and its Standards Association have been collaborating with agencies such as the FDA, National Science Foundation (NSF), National Institutes of Health (NIH), National Institute of Standards and Technology (NIST), universities

Figure 2. Trust, identity, privacy, protection, safety, and security (TIPPSS) for IoT.[11]

(including North Carolina State University, George Washington University, and Johns Hopkins University), industry, not-for-profits, start-ups, and other subject-matter experts. Since 2016, there has been a series of workshops featuring these organizations to bring together diverse contributors to determine how together as a community we can support the benefits of wearables and medical IoT interoperability and intelligence while reducing potential cybersecurity risks. Such events have included the IEEE Trust and Security workshop for the Internet of Things,[6] Wearables and Medical IoT Interoperability & Intelligence,[7,8] IEEE Connected Health: Applications, Systems, and Engineering Technologies (CHASE),[9] and IEEE Experts in Technology and Policy (ETAP)[10] Forums. Through these workshops, the community has established the need for trust, identity, privacy, protection, safety, and security (TIPPSS)[11] in IoMT devices and the data, device, and pharmaceutical supply chain to ensure patient safety (Figure 2).

The use of wearables—accompanied by increased data sharing across medical devices, systems, and countries to promote the progress of precision medicine—is huge and growing, and the time to act is now. We can all be part of the solution to increase TIPPSS in IoMT and medical interoperability. The ecosystem of partners to address these issues in Wearables and Medical IoT Interoperability & Intelligence (WAMIII) include IT and medical device hardware, firmware, software, and service developers and manufacturers; regulators; payers; providers; healthcare delivery organizations (HDOs); and network service providers and standards developers.

TIPPSS elements, including defense-in-depth measures, have been deployed in information technology (IT) infrastructures for years. When the operational technology (OT) of critical infrastructure systems became more connected with IT[12] and encouraged the growth of the IoT, TIPPSS elements became even more important to industrial control systems (ICS) operation. Adding to the complex ecosystem of the IoMT is the need to include privacy considerations of healthcare data in multiple highly regulated regions such as the United States and European Union.[13]

The use of TIPPSS and defense-in-depth strategies[14] is just one piece of the layered approach to protecting devices, as well as the data collected, gathered, and distributed. Technologies—from key pairs, to trusted platform modules, to newly announced crypto-anchors from IBM —can enable defense-in-depth for hardware, firmware, software, and service-level security as recommended in a 2015 KPMG report on security and the IoT ecosystem.[15]

Even with the multiple technologies available for end-to-end trusted environment and security frameworks, the New England Journal of Medicine in 2018 called out the need to include Real World Evidence (RWE) leveraging Unique Device Identifiers (UDIs), bringing the medical and IT communities together in the pursuit of safe and secure connected healthcare.[16] A key component to RWE is consideration of risk as part of the overall cybersecurity equation. By understanding risk, each participant in the healthcare ecosystem can make educated decisions on current and future technology implementations. This risk analysis must be performed for each layer of the technology stack for a defense-in-depth strategy for hardware, firmware, and software to be truly effective.[17] As the security boundary continues to blur, understanding the risk impact becomes a cyclical process and a key measurement for a cyber-resilient organization.

Measuring risk is a challenge for an organization, but there exists a wide range of resources that can provide expertise in assessing risk throughout the supply chain. The Association for

the Advancement of Medical Instrumentation (AAMI); Medical Device Innovation, Safety and Security Consortium (MDISS); NIST; and private companies are a few. Thankfully the FDA has taken a much-needed stance on addressing cybersecurity challenges from the standpoint of medical device manufacturing, including risk as a key component. In addition to releasing their own cyber recommendations, the FDA has acknowledged AAMI TIR 57 Principles for medical device security-risk management as a primary source for assessing risk related to medical device manufacturers.[14] The FDA "Factors to Consider Regarding Benefit-Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions" highlight four key aspects that should be considered in any multi-layered program for defense in depth:[18,19]

- Maintain the capability to monitor and detect cybersecurity vulnerabilities in devices.
- Measure, understand, assess, and detect the level of risk a vulnerability poses to patient safety.
- Work with cybersecurity stakeholders to include researchers to be able to evaluate information about potential vulnerabilities in a responsible manner.
- Provide, manage, and deploy mitigations to address cybersecurity issues early to minimize harm.

With this action, users and the IoMT industry are starting to recognize the need for standardization of both the technologies and their use. Many of the technologies mentioned in this article are driving forces in the technological advancement of patient care. Organizations will have to make new and difficult decisions to deploy, manage, and procure the right technology as these advances come into effect. For example, when looking at the next major purchase of infusion pumps, what are the critical factors that should be considered as part of any cybersecurity purchasing requirements? Fortunately, standards and regulations, such as the General Data Protection Regulation (GDPR), and Underwriters Laboratory Cybersecurity Assurance Program (CAP) certification, are currently providing organizations with a level of assurance in data privacy and cyber resilience, key factors in the deployment and manufacture of medical devices. These factors are driving the acceptance of existing standards and supporting the development of new standards for medical device safety and cybersecurity.

As IoT and IoMT continue to expand and merge, standards that focus on IoT-related technologies will have to look at the impact of patient safety and data privacy on future activities. When dissecting a defense-in-depth strategy for a single IoMT device, it becomes clear the hardware, firmware, software and communications channel have different levels of cyber resilience. Technologies like blockchain and programs such as RWE, TIPPSS, IEEE ETAP, and IEEE CHASE will help bridge the cybersecurity gap and force organizations to take an in-depth look at the very foundations of their security programs, as we as an industry move to address cybersecurity risk and associated challenges.

GET INVOLVED WITH STANDARDS ACTIVITIES

The IEEE Standards Association Association (IEEE-SA) is actively engaged in attracting subject-matter experts to help in the development of pre-standardization whitepapers and other deliverables as well as new standards projects supporting defense in depth and other solutions for WAMIII. To bring together the people with the right skills, workshops are being regularly held around the world. If you are interested in participating in the WAMIII initiative, please visit https://wamiii-ieee.org/.

In regards to work specifically on clinical IoT and blockchain, the "Clinical IoT Data Validation and Blockchain Interoperability" pre-standards activity is an open and inclusive working team. This group is developing a viable framework for a technical standard and system that can validate data from a clinical-grade IoT which will then work with the blockchain for secure and private distribution of patient data. This would also enable other use applications of the data such as patient recruitment and clinical research. Those wishing to participate should visit http://bit.ly/cliniotblkngrp.

In addition, IEEE P2418, Standards for the Framework of Blockchain Use in Internet of Things (IoT) working group is developing a standard for the common framework for blockchain usage, implementation, and interaction in IoT applications. Those wishing to participate should visit http://sites.ieee.org/sagroups-2418/.

REFERENCES

1. J. Davis, "87 percent of health organizations plan to adopt IoT technology by 2019, study shows," Healthcare IT News, 28 Feb 2017; http://www.healthcareitnews.com/news/87-percent-health-organizations-plan-adopt-iot-technology-2019-study-shows.

2. "Johnson & Johnson warns insulin pumps can be hacked," Nightly Business Report produced by CNBC, 5 October 2016; https://www.youtube.com/watch?v=YThj0Nh40KQ.
3. *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication*, U.S. Food & Drug Administration, 29 Aug 2017; https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm.
4. "FACT SHEET: At Cancer Moonshot Summit, Vice President Biden Announces New Actions to Accelerate Progress Toward Ending Cancer As We Know It," The White House Office of the Press Secretary, 28 June 2016; https://obamawhitehouse.archives.gov/the-press-office/2016/06/28/fact-sheet-cancer-moonshot-summit-vice-president-biden-announcesfnew.
5. P. Padmanabhan, "Unlocking the value in patient-generated health data," CIO from IDG, 28 Feb 2017; https://www.cio.com/article/3174732/healthcare/unlocking-the-value-in-patient-generated-health-data.html.
6. IEEE Trust and Security Workshop for the Internet of Things, IEEE Standards Association, 4 Feb 2016; https://internetinitiative.ieee.org/images/files/events/ieee_end_to_end_trust_meeting_recap_feb17.pdf.
7. IEEE Co-Sponsoring Inaugural 2017 Wearables & Medical Interoperability (WAMI) Workshop, IEEE Standards Association, 22 Sept 2017; http://standards.ieee.org/news/2017/wami_workshop_2017.html.
8. Wearables and Medical IoT Interoperability & Intelligence (WAMIII) Workshop 2018, IEEE Standards Association, 25 April 2018; https://ieee-wamiii.org/april-2018/.
9. The First IEEE Conference on Connected Health: Applications, Systems and Engineering Technologies, IEEE CHASE, 27-29 June 2016; http://conferences.computer.org/chase/.
10. The IEEE Experts in Technology and Policy (ETAP) Forums on Internet Governance, Cybersecurity and Privacy, Washington, D.C., 5 February 2016; https://internetinitiative.ieee.org/events/etap.
11. F.D. Hudson, "Enabling Trust and Security - TIPPSS for IoT," *IT Professional*, vol. 20, no. 2, March/April 2018.
12. "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, Industrial Control Systems Cyber Emergency Response Team," U.S. Department of Homeland Security, September 2016, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.
13. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," The European Parliament and the Council of the European Union, 27 April 2016; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.
14. "AAMI TIR57: Principles for medical device security—Risk management," AAMI, June 2015; http://www.aami.org/productspublications/ProductDetail.aspx?ItemNumber=3729.
15. "Security and the IOT ecosystem," KPMG International, 2015; https://assets.kpmg.com/content/dam/kpmg/pdf/2015/12/security-and-the-iot-ecosystem.pdf.
16. F.S. Resnic and M.E. Matheny "Medical Devices in the Real World," *The New England Journal of Medicine*, Vol. 378, No. 7, 2018; https://www.nejm.org/doi/full/10.1056/NEJMp1712001.
17. K. Bay, "The security tech stack is out of control, here is what to do about it," CSO from IDG, 11 October, 2017; https://www.csoonline.com/article/3229949/network-security/the-security-tech-stack-is-out-of-control-here-is-what-to-do-about-it.html.
18. "FDA Points Manufacturers to AAMI Cybersecurity Recommendations," AAMI, 5 July, 2016; http://www.aami.org/newsviews/newsdetail.aspx?ItemNumber=3719.
19. "Factors to Consider Regarding Benefit Risk in Medical Device Product Availability, Compliance, and Enforcement Decisions," U.S. Food & Drug Administration, 27 December, 2016; https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm506679.pdf.

FLORENCE HUDSON is special advisor for Next Generation Internet at the Northeast Big Data Innovation Hub at Columbia University. Contact her at florence.distefano.hudson@gmail.com.

CHRIS CLARK is a principal security engineer for Strategic Initiatives, Synopsys – Software Integrity Group. Contact him at chris.clark@synopsys.com.