INTERNET OF MEDICAL THINGS

Harnessing IoMT for Value-Based Care

&

Cybersecurity: Health Care Takes On a Growing Challenge

Lessons for the health care industry from the Center for Connected Medicine's webinar series on the Internet of Medical Things

July 2017

CENTER FOR CONNECTED MEDICINE™

Key takeaways

1 Health care providers and patients benefit from the deployment of Internet of Medical Things (IoMT) devices, but challenges remain to realizing full value from the technology.

2 Remote monitoring programs utilizing IoMT devices expand the reach of providers, lower hospital utilization, and provide return on investment for health systems engaging in risk-sharing payment models.

3 Technology is allowing the patient home to become an important site of care but the lack of data interoperability is an obstacle to giving consumers a complete view of their health.

4 Many health systems believe they are not as prepared as they need to be for cybersecurity threats, which are increasing because of the value of patient data and the proliferation of IoMT devices.

5 The cybersecurity challenge is not insurmountable if health care organizations implement five key actions: Recognize that compliance does not equal protection; know your environment; have a plan; understand that security is everyone’s responsibility; stay in the fight.

6 Active cybersecurity systems utilizing software solutions and automation allow health care organizations to identify more threats, eliminate time wasted on benign threats, find real threats faster, and respond more quickly.

July 2017

CENTER FOR CONNECTED MEDICINE™

Summary

The Internet of Medical Things (IoMT) is changing health care, and the industry needs to prepare if it wants to harness the technology for value-based care. Experts are predicting rapid growth in IoMT adoption, making it vital that health systems confront challenges, such as security, interoperability, and analytics, that are needed for the technology to meet its promise of helping expand access to care, improve quality, and reduce cost. An estimated 87 percent of health systems will have IoMT technologies deployed by 2019[1], and the value of the IoMT market is expected to reach more than $160 billion by 2020[2].

At the same time, concerns are rising about the vulnerability of IoMT devices. In the wake of high-profile attacks against the industry that have led to data breaches, cybersecurity is moving to the top of the agenda for leaders of health systems. Cyberattacks targeting patient data reportedly jumped 300 percent between 2014 and 2016[3]. As a result, the U.S. health care industry is spending an estimated $6.2 billion a year in fines and other costs related to health data breaches[4].

To better understand the challenges and opportunities presented by the growth of IoMT, the Center for Connected Medicine hosted a two-part webinar series with health care technology experts representing major stakeholders in the industry. Part one – "Harnessing IoMT for Value-Based Care" – covered the increasing role of internet-connected devices in medical care. Part two – "Cybersecurity: Health Care Takes on a Growing Challenge" – focused on the threat health systems face from cyberattacks. Lessons learned from the series are summarized in this report.

The Experts

Webinar Moderator

Rasu Shrestha, MD, MBA

Chief Innovation Officer, UPMC & Executive Vice President, UPMC Enterprises

Named a leading innovator in health care IT by Health Data Management, recognized by *Becker's Hospital Review* as one of the 26 "Smartest People in Health IT" and named one of the "Top 20 Health IT Leaders Driving Change" by and *InformationWeek*.

Panelists

Tom Foley

Director, Global Health Solutions Strategy, Lenovo Health

More than 30 years of experience in information technology; focused on a global wrist-to-cloud health IT strategy for Lenovo Health.

Garrett Hall

Research Director, Cybersecurity and Implementation Services, KLAS

Co-author of "Understanding the Healthcare Security Landscape" and works to provide health systems with information and data to help them make transparent healthcare IT decisions.

Rob Marson

Head of Strategy and Business Development, Security Product Unit, Nokia

A strategic marketing, business development and product management professional with experience spanning multiple technology and business disciplines.

Beth Musumeci

Vice President, Cybersecurity, GE Healthcare

Extensive IT and cybersecurity experience, including in global comprehensive security solutions, infrastructure services, business transformation, business alignment, service management, solution development, infrastructure strategy, and global service delivery.

Gregg Pessin

Research Director, Gartner

A 32-year veteran of the IT industry, including in health care, cloud hosting, manufacturing and defense; research focuses on underlying technologies that support the real-time health care system.

Eric Rock

Founder and CEO, Vivify Health[5]

An innovator and entrepreneur who founded three highly successful software companies; Vivify Health is utilized by 600+ hospitals and health plans.

PART ONE:

HARNESSING IoMT FOR VALUE-BASED CARE

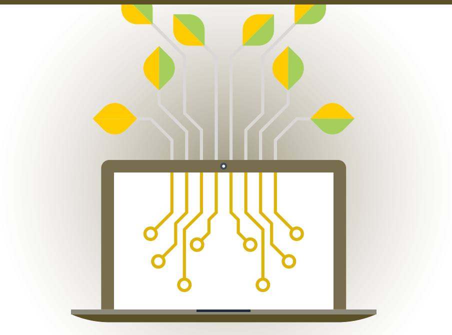
Benefits and challenges of IoMT

Health care providers and their patients are benefiting from the deployment of IoMT devices, but challenges remain to realizing full value from the technology. By collecting more data on patients – with internet-connected devices both inside and outside of health care facilities – providers have access to a more complete view of a patient's health. The health data can come from a range of sources, including personal wearable devices such as fitness trackers to heart monitors in hospital rooms. Combining those data in a software platform with analytics provides a clearer picture of patient health and leads to faster diagnoses and more effective treatments, said Gregg Pessin, Research Director at Gartner.

> "Having this holistic view of what's going on with the patient ... creates a more informed place to begin the diagnostic and treatment paths for the patient."
>
> **Gregg Pessin**

Challenges associated with IoMT center on patient data and can be broken down into the following five categories:

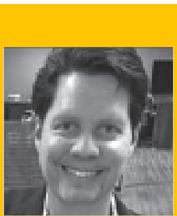
1. **Privacy and compliance:** Patient data must be protected – and HIPAA regulations followed – on the device, in transmission to the health system, and during storage and use on the network.
2. **Security:** As IoMT become a more common cyberattack vector, health systems and vendors need to redouble efforts to ensure all connected devices are secure.
3. **Data integration/interoperability:** In order to derive useful information and actionable insights from IoMT, the data generated from devices must integrate into hospital IT systems.
4. **Positive patient identification:** For IoMT to deliver useful data, it is crucial to ensure that the information collected from devices actually come from the patient, and not a child playing with her mom's fitness tracker, for instance.
5. **Data accuracy:** Some consumer-grade IoMT devices are not always accurate, which calls into question the validity of data collected from patients.



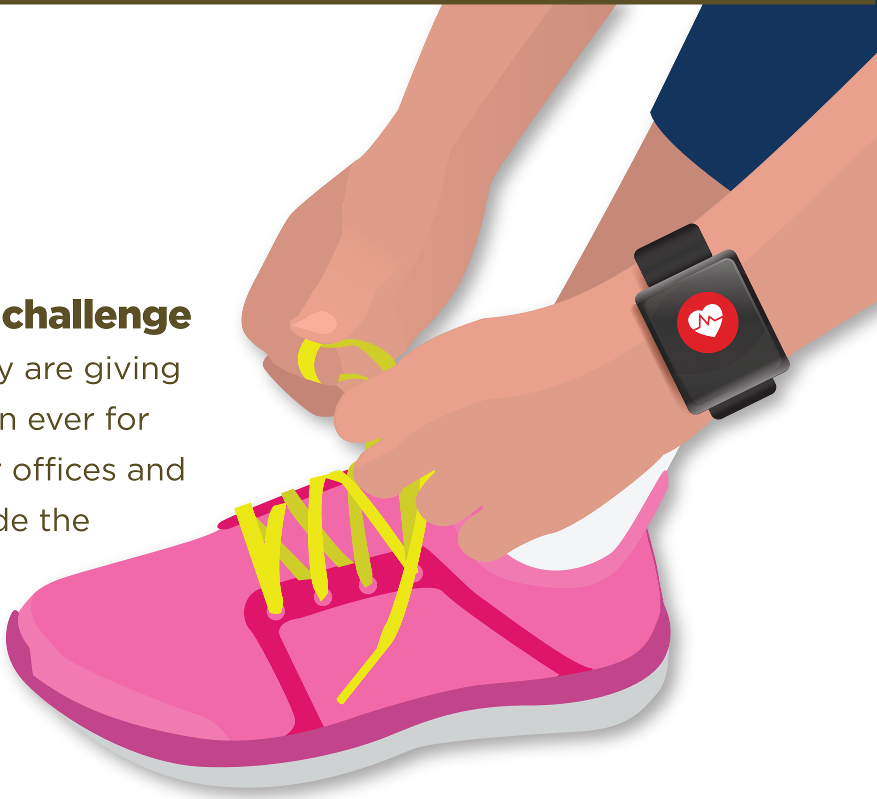
Expanding provider reach

Remote monitoring systems utilizing IoMT devices expand the reach of providers by allowing a fewer number of clinical staff to oversee a larger number of patients. Remote monitoring also acts as an early-warning system for high-risk patients, allowing providers to intervene more quickly and prevent unnecessary hospitalizations. Greater clinical efficiency and lower hospital utilization provide a significant return on investment for health systems engaging in risk-based payment models, Vivify Health Founder and CEO Eric Rock said.

While there are financial benefits to be gained for health systems deploying remote monitoring, the lack of widely accepted reimbursement models for the technology remains a challenge for providers that have been slow to transition to value-based alternative payment models. At UPMC, which operates the largest provider network and health plan in western Pennsylvania, Vivify's remote monitoring platform is being used to care for and engage with patients with Congestive Heart Failure, who are among the leading drivers of unplanned hospitalizations, and several other use cases. UPMC patients using Vivify report high satisfaction and have achieved a daily compliance rate of more than 90 percent.



> "(Vivify customers) are seeing, as a result of this, benefits such as a reduction of over 50 percent in acute utilization and costs. … There's a hard ROI when there's a … value-based model where they're taking the risk or costs associated with the patient."
>
> **Eric Rock**



Overcoming the interoperability challenge

Advances in technology and connectivity are giving patients and providers more options than ever for engagement outside traditional provider offices and other health care facilities, primarily inside the patient home. Harnessing data from traditional medical records and combining it with information that increasingly will be generated in the patient home via IoMT devices can bring tremendous value to the health care system. But patient health data is often locked within proprietary IT systems. A quarter of the American population has more than one chronic condition, and older adults with five or more chronic illnesses on average see 14 different physicians[6]. These statistics highlight the need for hospital systems, vendors and device manufacturers to pursue interoperability and make data-sharing a priority.

As devices, platforms and analytics mature, it is essential that the industry overcome the lack of data interoperability, said Tom Foley, Director of Global Health Solutions Strategy at Lenovo Health. While some in the industry are focused on establishing point-to-point protocols for information sharing, Foley argued that secure messaging standards must be based on a one-to-many model.

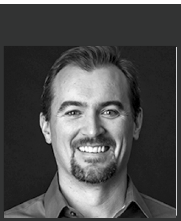
> “We can pass data. We just don’t understand the data. ... This lack of semantic interoperability prevents us from achieving this goal.”
>
> **Tom Foley**

PART TWO:

TACKLING THE GROWING CHALLENGE OF CYBERSECURITY

Playing catch-up

Many health systems are not as prepared as they need to be for cyberattacks, leading them to report feeling "behind the times" when it comes to cybersecurity, according to research by KLAS. Garrett Hall, Research Director of Cybersecurity and Implementation Services at KLAS, found that 43 percent of health systems that responded to a recent KLAS survey reported that their security program was not developed or was only starting to develop. And, the survey found, 41 percent of those respondents said their health systems dedicate less than 3 percent of the IT budget to cybersecurity. Cybersecurity has been on the backburner at some health systems because IT leadership has been focused on implementing electronic health record systems, for instance, Hall said. But with recent attention on data breaches, the vulnerability of IoMT devices, and other cyberattacks, Hall said security is quickly moving up the health IT agenda.



> "With the evolution of attacks and with the valuable nature of health care information, these attacks aren't going to go away. ... The good news is that we're starting to see more of an emphasis on cybersecurity and I think the Internet of Medical Things has really helped to push things to the forefront."
>
> **Garrett Hall**

KLAS finds that the top health systems on the leading edge of cybersecurity programs at a minimum do the following:

1. Conduct **external risk assessment**, at least annually, to find and prioritize vulnerabilities.
2. Implement a **Security Information and Event Management** (SIEM) system to detect threats.
3. Create an **incident-response plan** and designate an incident-response team.

A shared responsibility

The cyber threat challenge is not insurmountable, but achieving robust security requires many stakeholders to work together toward the shared goal – including health system leaders and their employees, IT vendors and device manufacturers.

Beth Musumeci, Vice President of Cybersecurity at GE Healthcare, recommended five key actions for "rising to the challenge" of improved cybersecurity:

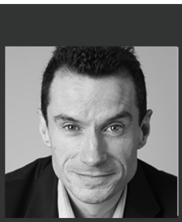
1. **Recognize that compliance does not equal protection**: Health care systems must understand that simply being compliant with privacy regulations, such as HIPAA, isn't enough. They are guidelines and should not serve as proscriptive guidance for cybersecurity.
2. **Know your environment**: Understand that criminals will take the time to understand as much about a health system's network as possible. Anything accidentally connected to the network could lead to an attack.
3. **Have a plan and be prepared**: An emergency response plan, which prioritizes key health service functions, is essential. Testing the recovery plan regularly is a must.
4. **Understand that cybersecurity is everyone's responsibility**: Make sure cybersecurity is part of your health system's culture. Cybersecurity is not just the CTO's campaign.
5. **Stay in the fight**: Don't give up. The challenge can be overcome but it requires executive support and budget.

> "You can't be a bystander, you must be an active participant. Cybersecurity for the health care environment is a shared responsibility between the manufacturers and operators."
>
> **Beth Musumeci**

Prioritize active security

Active cybersecurity systems, which employ software and automation, give health care organizations an advantage when it comes to identifying the threats they face more quickly. An active solution also helps to eliminate the time IT workers waste on benign threats and helps them to respond more quickly. Many large companies are faced with thousands of security alerts each day – many of which may not be legitimate threats – and workers are suffering from alert fatigue.

Rob Marson, Head of Strategy and Business Development for the Security Product Unit at Nokia, said more sophisticated and automated software solutions can help health systems strike a balance between proactive and reactive security measures. Active solutions measure risk, control access and limit attack vectors, while reactive practices detect indicators of compromise and respond to threats. Solutions that incorporate machine learning technology and data analytics are identifying threats earlier and earlier. While organizations should expect that they'll be attacked at some point, Marson said, a rapid response is key to minimizing the impact.



> “The art is how quickly can you detect and how quickly can you respond appropriately. What needs to happen is eliminate the time between detection and mitigation.”
>
> **Rob Marson**

About the Center for Connected Medicine

The **Center for Connected Medicine** is the world's first collaborative health care executive briefing center, supporting stakeholders in defining the transformation of health care. It serves as a resource for innovative patient-centered and population health models, showcasing strategically integrated health information technology. By facilitating connections among those who deliver, receive, and support health care, the Center helps promote cultural change, coordinated care delivery, and greater patient engagement. Located in Pittsburgh, PA, the Center for Connected Medicine is comprised of five partners — GE, IBM, UPMC, Nokia, and Lenovo Health — representing various facets of the health information community. Learn more at www.connectedmed.com.

July 2017

References

[1] https://www.healthcare-informatics.com/news-item/mobile/study-87-percent-healthcare-organizations-will-adopt-iot-technology-2019

[2] http://www.marketsandmarkets.com/PressReleases/iot-healthcare.asp

[3] https://trapx.com/trapx-reveals-2016-healthcare-breaches-increased-63-percent-year-over-year-medical-device-hijacks-and-ransomware-on-the-rise/

[4] http://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html

[5] Disclosure: UPMC Enterprises is a customer of and investor in Vivify Health

[6] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2924996/

CENTER FOR
CONNECTED
MEDICINE
™

U.S. Steel Tower, 60th floor
600 Grant Street
Pittsburgh, PA 15219
412.864.4000
www.connectedmed.com