[Music]

Female: Welcome to Conversations on Health Care with Mark Masselli and Margaret Flinter. It's a show where we speak to the top thought leaders in health innovation, health policy, care delivery and the great minds who are shaping the health care of the future. This week Mark and Margaret speak with David Houlding, Principal Healthcare Lead at Microsoft responsible for health care initiatives within the Microsoft Azure Industry Experiences Team. He's Chair of the Health Information and Management System Society, Blockchain Health Care Taskforce, talks about the growing cyber security challenges in health care and what needs to be done to protect people's health data.

Lori Robertson also checks in, the Managing Editor of FactCheck.org looks at misstatements spoken about health policy in the public domain separating the fake from the facts. We end with a bright idea, that's improving health and well being in everyday lives. If you have comments, email us at chcradio@chc1.com or find us on Facebook, Twitter, iTunes, or wherever you listen to podcasts. You can also here us by asking Alexa to play the program Conversations on Health Care. Now stay tuned for our interview with David Houlding, Principal Healthcare Lead at Microsoft on Conversations on Health Care.

Mark Masselli: We're speaking today with David Houlding, Principal Healthcare Lead at Microsoft responsible for health care initiatives at the Microsoft Azure Industry Experiences Team. He is chair of the HIMSS Blockchain in Healthcare Taskforce, he's also an advisor to the British Blockchain Association. Previously, Mr. Houlding served as Director of Healthcare Privacy and Security at Intel Corporation, where he established the Intel Healthcare Security Readiness Program. He holds several patents in information technology, architecture and security. He earned his master's of applied science at Simon Fraser University in Vancouver. David, welcome to Conversations on Health Care.

David Houlding: It's great to be here. Thanks for the opportunity.

Mark Masselli: Yeah, you know you've been at the forefront and really been thinking a lot about data security for a quarter of century. And I think it's fair to say that the industry has gone through this incredible revolution over the last decade or so of moving from paper to electronic and digital data. Given your background in data and health security, I'm wondering, do you think the industry is ready for the cyber security side of having this much data in a digital format?

David Houlding: Yeah, you're right. So digitizing paper and sort of moving to electronic health records was the first step and we've come a long way. But once that data is digitized, if it's locked away in silos like centralized databases, that's only have limited use, right? If it's not shared when necessary for health information exchange and other things then it's

limited use in terms of improving health care. I think the opportunity beyond just digitizing health records is to facilitate secure targeted sharing and unlock the potential of the data. I think cloud computing can play a key role in that.

The reality is also that a lot of health care organizations lack the resources, the cyber security resources to adequately secure on premise infrastructure. They can get a lot of that with secure platforms, tools and partnership from and focus more on the higher levels of the stack, the applications, the business, the innovation and not have to have the capital costs the same degree of on premise cyber security resources.

We're really focused on four key business goals of health care, right? Reducing health care costs is the first one and really using the cloud can free up a lot of health care organizations from the capital expenditure associated with on premise infrastructure versus in the cloud, but also improving patient outcomes right? Through the improved accessibility and secure information sharing that you can get with cloud based data. That gives us an opportunity to improve patient outcomes through better care collaboration, and so forth. Improving patient engagement and experiences is another third key goal of health care.

You have things like patient portals that can run in the cloud, can also have intelligent health care agents, think Chatbots but health care agents to be much broader than that. Running all the time in multiple languages, very cost effective and it can really boost patient engagement to that next level. But the fourth sort of key goal we're really focused on is also improving the experience of health care professionals, right? That's all about intelligent health. It's all about, AI machine learning for clinical decision support. Rather than give those clinicians the raw data and drown them in raw data, use the AI machine learning.

In many cases running from the cloud to get actionable insights near real time so they can be acted upon if there's a dangerous sort of condition evidence in the in the raw data from the patient, then they can intercept that really quickly and intervene and hopefully avoid an episode, right, which can really impact the quality of care for the patient. I'm thinking heart attack or something like that, if you can intercept and avoid that, that's a major quality of life improvement for the patient and definitely a cost reduction improvement for the health care organization as well.

Getting back to the cyber security side, I think of it as privacy, security and compliance. On the privacy side, it's really about transparency, right? Notice to the data subject and we often just focus on patients as a data subject, but any kind of personnel identifiable information

could also be the healthcare professionals, right? We need to be concerned about privacy of that information and being transparent about how it's being used, how is it collected, how is it stored, and how is it disposed of. We often don't think about at the end of life of data, disposing of it, disposing of it, security is a good thing to do, right? Privacy to me is really about empowering the data subjects including the patients to access, review, amend their data and so forth. There's some really interesting opportunities around new technologies like Blockchains really have that up to the next level.

As a security professional, we're trained to break it down into CIA confidentiality, integrity and availability. Protecting confidentiality of data, we got to make sure it's adequately secured against unauthorized access. On the integrity side, we really got to make sure the data is kept accurate, complete and up-to-date and isn't tampered with. Protecting data integrity can be done with things like hash codes and digital signatures and there's some super interesting capabilities with Blockchain and the immutability side which can really take protecting integrity of data up to the next level. Even things like AI machine learning models, right, as we learn to depend on those we got to protect them and make sure they aren't tampered with.

Lastly, the availability, this is one that I don't think we paid enough attention to in health care. Availability is all about ensuring timely and reliable access, the systems and data. Prior to Ransomware, I think most people equated security with protecting confidentiality and avoiding breaches and that's certainly a big part of it. But it actually turns out, especially for health care providers, protecting availability can actually be far more important. If you have a Ransomware event and your data is not available, because somebody's trying to extort money out of you for a ransom. That can be an immediate disruption and it can really impact the quality of patient care and safety, frankly, as well.

Now, we also got to think about new types of attacks that aren't new conceptually, but they're relatively new in health care, like distributed denial of service attacks. As we move more and more infrastructure to the cloud, there's fantastic benefits again in freeing up health care from the burden of on premise sort of legacy infrastructure maintenance and enabling them to focus on the health care and innovating. But we got to think about ensuring, how do we ensure the availability of those systems in the cloud? So we can do that with things like redundant connectivity to the cloud. You can have a cloud mitigation provider that helps you filter out, good, legitimate requests from bad requests and basically ensure that you're not being drowned by a DDoS sort of blast.

Margaret Flinter: I was particularly struck by some of the work that you're doing and

developing these new care delivery clinical support systems, including remote patient monitoring, which has been around for a long time, but we're seeing it taken to a whole new levels. Mark we had Noelle LaCharite from Microsoft here with us not too long ago, she was talking about the work that she's doing in voice technology in health care which is also seeing significant growth. I wonder if I could ask you to talk a little more about programs like the recently launched Microsoft Healthcare Bot Service, which I think you might have referred to in your comments as one example of health care agents and other new tech and voice enabled interfaces maybe just expand on that a little bit.

David Houlding: Microsoft's approaches platforms, tools and partnerships, so we don't generally create like health care and solutions. Think of the Healthcare Bots Service as a tool that can be used to build out healthcare bot capabilities into a myriad of different partner health care solutions. This is super exciting because technology can be exciting, but what's most interesting to me is how its applied for the health care benefits and the bot service and those kinds of capabilities. It's all around patient engagement and experiences as well as reducing costs.

On the engagement side, the gist of it is really all hours of the day, never sick, multiple languages concurrently, engagement options for patients, whether it's a text interface, whether it's a voice interface. It's reaching patients in ways just not possible before, right. It's not that the only interface available to patients going forward will be these automated agents. But think of the 80-20 rule, I think 80% of the request could be handled by these agents, and it really reduces the repetitive noise type requests to the human operators, the nurse on call, for example. If the intelligent agents can help patients with the basic types of requests and that also improves the experience of the health care professional, because I think some of them get the same question hundreds of times a day, and that's not a good use of their time.

Just the continuous availability of intelligent health care agents is going to really improve the experiences of patients. Picture of your mom and you have a sick child and you need help now, and so if it happens to be after hours on the weekend, or you speak a different language. These kinds of agents could really improve the experience of the patient and enable their self-help, right. The patients motivated to help themselves so this could also help health care professionals right. Think if they're being credentialed or if there's other services they need to get updates on or processes. These kind of intelligent agents could really help expedite and empower health care professionals with the actionable insights and information they need. Hopefully avoid or at least alleviate some of the clinician burnout

we're seeing.

On the cost reduction side, of course, handling all of these different types of languages concurrently 24 by 7 by 365 can really help improve the cost picture, whether it's a health care provider, whether it's the payer on eligibility request, could even be a pharmaceutical or life sciences. Let's say if they're doing a clinical trial and patients have questions and there's wonderful opportunities there as well for cost reduction across all those segments of health care.

Mark Masselli: David, your dramatic innovation and it doesn't seem that the regulatory landscape is keeping up. But I didn't know that the Centers for Medicare and Medicaid Services announced a new rule that by next year, all patients should be able to have access to their health data delivered to their smart phones within 24 hours. Wonder if you could tell us whether or not it's doable given where we are in terms of our technology and our ability to transfer that information safely and securely to patients?

David Houlding: Yes, I definitely think it's a good thing, right? Forever we've been talking about the need for patients to own their data, and it's all part of empowering patients and take control of their health care, right? They got to have access to their data. I think as an industry we'll figure out how to do that efficiently and cost effectively. Cloud can play a key role in that, right, it can enable, again, health care to free themselves from those low level infrastructure on premise type costs, and focus more on business innovation and applications with cloud based deployment. One can really break it down into privacy and security.

I think a lot more could be done to empower patients in any data subjects, including health care professionals with their privacy. More could be done around data sovereignty and transporter data flow. If your data is collected, how is it shipped around the world? I don't think HIPAA does as much in that area, as well as patients control over their data, even the right to be forgotten, right. If a patient goes to a provider and for some reason they opt not to go to that provider anymore, and they request for their data to be deleted. I don't think that's something that most health care providers do today. But, it is a reasonable request.

I think there's new capabilities available that could really help us amp privacy up to the next level. For example, Blockchain offers ways to empower patients with privacy in ways not possible before. Think of a patient being able to see on Blockchain what data is being used, be able to consent or opt in, or even opt outs and control their data in ways not possible before. There's new technologies like Blockchain that can pave the way for new policy requirements.

We've seen the devastation of breaches in health care and Ransomware and definitely more could be done on the HIPAA security rule to keep track of what's going on since the last revisions to ensure that health care organizations are adequately protected. The risk is never fully eliminated, but I think from the policy side we've got to make sure that health care organizations at least have adequate levels of security. I think more could be done on confidentiality and avoiding breaches for sure. We need to continue with the access control the encryption, the key management to track new vulnerabilities threats and really approach security as a team, not each organization alone, which is just not reasonable.

But, there's a lot more that could be done on protecting the integrity side of data. I don't think we've paid nearly enough attention there and there's wonderful new opportunities with capabilities like Blockchain to bolster the integrity protections of all kinds of data and then the need to protect availability of systems and data. Ransomware has taught us that if data is not available, or systems are not available and those are mission critical, that can be severely disrupted to health care and on the health care provider side, that's a degradation of quality of service for the patient. It could be a patient safety risk, right.

I think we need to really approach security from a three prong standpoint. One is prevent, so do what we can to anticipate threats and vulnerabilities and mitigate those. Even though you teach people not to click on links and unsolicited emails, they're going to click at some points and what you need to be able to do is detect new intrusions, new security incidents very quickly. There's wonderful new opportunities with technologies like artificial intelligence and machine learning to collect all this telemetry. Think of log data going into a bank of AIs that are looking continuously around the clock for any kinds of new threats and vulnerabilities. As soon as those are detected, detected quickly and use AI machine learning for that and respond quickly to stop loss and remediate. I think we need to really get in the mindset of do what we can to prevent, but really bolster the detect and respond side of security.

Margaret Flinter: David, I want to take it to the level of the individual. Clearly personal genomic, self generated health data are increasingly going to be part of the health record. We here in our organization are participating in the All of Us Project contributing their genetic data as well as their personal health data, family data. When we think of how most people sign off on that data, they sign that I've read my HIPAA notice and I agree, right. What should consumers be looking at here? Now we're talking about the electronic health record having data not just on you, but your antecedents your ancestors. What do you say to the person in the street about what should they look for in order to have

reasonable assurance that they're well protected?

David Houlding: It's from a privacy standpoint, it's about risk reward, right? Think about if you get a request for your data, what's the potential benefit in opting in or consenting to the use of your data? This fantastic capabilities and potential for precision and personalized health care. Really to get the benefits of those, you have to consent and opt into sharing your data, why? Because your data is used to actually tailor the precision medicine to the personalized health care for you. Sometimes there's rewards in terms of if you're participating in clinical trials, you can get updates on the findings directly if you opt into participation and sharing your data.

Sometimes this compensation involve, that could be another part of reward that patients could get for participation. But think about the risk, I think of it in terms of the full lifecycle like what data are you consenting to the use of? How will it be collected? How will it be used? Will it be shared with any other third parties? Then what is done with the data at the end of the life cycle? Is it going to be disposed off or is somebody just keeping it indefinitely? Obviously the risk of breaches and things is vastly increased if there's no disposal of the data. I think we need to get past just thinking that there's these huge nebulous privacy risks, because frankly that will shoot patients in the foot in terms of their ability to participate in precision medicine and personalized health care. We've got to opt in but we've got to do it with our eyes wide open in terms of what are the risks and what are the rewards in terms of benefits to health care.

Mark Masselli: We've been speaking today with David Houlding, Principal Healthcare Lead at Microsoft. You can learn more about their work by going to Azure.Microsoft.com or you can follow him on twitter @David Houlding and that's H-O-U-L-D-I-N-G. David, thank you for your groundbreaking work as a leader in health data security and for sharing your expertise and wisdom with us on Conversations on Health Care.

David Houlding: Thanks very much for the opportunity. Great to speak with you both.

[Music]

Mark Masselli: At Conversations on Health Care we want our audience to be truly in the know when it comes to the facts about health care reform and policy. Lori Robertson is an award-winning journalist and Managing Editor of FactCheck.org a nonpartisan nonprofit consumer advocate for voters that aim to reduce the level of deception in US politics. Lori what have you got for us this week?

Lori Robertson: A false claim about Medicare eligibility and cost has been shared nearly 500,000 times on Facebook. The false claim says, “Why do

seniors on social security have to pay for Medicare and a supplemental insurance and the illegals get it all for free?" Medicare isn't available for people living in the US illegally. It is available only to citizens and lawful permanent residents who have lived in the US continuously for at least five years and meet other criteria such as being at least 65 years old and having paid Medicare payroll taxes.

Also, most seniors don't have to pay for the basic Medicare coverage. There are four parts to Medicare. Medicare Part A covers inpatient stays at hospitals and nursing facility. It is funded largely through payroll taxes, and those who paid into the system for at least 10 years or are married to someone who paid into the system don't pay premiums. Medicare beneficiaries can purchase additional coverage for doctor's visits and outpatient care through Medicare Part B or through a private insurance provider with Medicare advantage. Most people who receive social security benefits and use Medicare Part B pay $130 per month.

Those living in the US illegally may actually provide a net contribution to the Medicare Part A Trust Fund through taxes. From 2000 to 2011, such immigrants contributed an estimated net total of $35.1 billion to the trust fund. That's according to a study led by a Harvard Medical School professor and published in the Journal of General Internal Medicine, and that's my fact check for this week. I'm Lori Robertson, Managing Editor of FactCheck.org.

Margaret Flinter: FactCheck.org is committed to factual accuracy from the country's major political players, and is a project of the Annenberg Public Policy Center at the University of Pennsylvania. If you have a fact that you'd like checked, email us at chcradio.com we'll have FactCheck.org's Lori Robertson check it out for you here on Conversations on Health Care.

[Music]

Margaret Flinter: Each week Conversations highlights a bright idea about how to make wellness a part of our communities and everyday lives. Childhood obesity is a national epidemic, but in the south it's far more prevalent. In Louisiana for example, over half of the children are either obese or overweight, with many experiencing symptoms such as high blood pressure, high cholesterol and prediabetes. Louisiana State University researcher Dr. Amanda Staiano has been studying protocols to tackle childhood obesity, tapping into readily available resources that make it easier for kids to adopt better exercise and activity habits. Since video games are ubiquitous in children's lives, she thought that would be a great place to start.

Dr. Amanda Staiano: I was trying to think of a way to meet children where they are so they can be more physically active. Children now are spending seven to eight hours every day using screen technology. Video games are still

very popular. With these new active video games that require physical activity to play. I thought this might be an innovative way to make physical activity and exercise fun, but also to help these children to lose weight and get a healthier heart.

Margaret Flinter: Her team at the Pennington Biomedical Research Center at LSU developed an intervention called Game Squad giving prescriptions for playing movement video games for a full hour three times a week.

Dr. Amanda Staiano: In addition to giving the kids these extra games to play with, we gave them a fitness coach that they would talk to over their video game, and the coach would check in with the parent and child once a week. We also gave the kids a step tracker so that they could objectively keep track of their physical activity throughout the six months.

Margaret Flinter: And kids were encouraged to have other family members join them in the movement video games, which added yet another level of engagement like this young 12 year old boy who enjoyed gaining a competitive edge over his mom who was often dancing right alongside of.

Boy: My mom want to race me, I have to say like 60% of the time I beat her. I love to do this with my mom. It really does build up your cardio and stamina for football and for different other sports.

Margaret Flinter: Dr. Staiano says during the six month Game Squad trial, over 90% of the kids who are given video game prescriptions and the fitness coach intervention stayed active throughout the study. The gaming group reduced their BMI by about 3%, while the control group saw an increase in theirs. Staiano says the added bonus was that kids gained confidence and improve self-esteem with their newfound activity. Game Squad an effective intervention to increase exercise in sedentary and overweight kids, improving health and fitness for kids and a fun engaging and sustainable way.

Boy: Well, when this is all over, I'll still do it. We'll keep on continuing doing the games.

Margaret Flinter: Now that's a bright idea.

[Music]

Mark Masselli: You've been listening Conversations on Health Care, I'm Mark Masselli.

Margaret Flinter: And I'm Margaret Flinter.

Mark Masselli: Peace and health.

Female: Conversations on Health Care is recorded at WESU at Wesleyan University streaming live at chcradio.com, iTunes or wherever you

listen to podcasts. If you have comments, please email us at chcradio@chc1.com or find us on Facebook or Twitter. We love hearing from you. The show is brought to you by the Community Health Center.