Transcript:

Sean Kelley: Hello and welcome! Today I am sitting with Dr. Paul Cordts – Director and Functional Champion, Military Health System Defense health, Dr. Suzanne Schwartz – Associate Director for Science and Strategic Partnerships, Center for Devices in Radiological Health at the FDA and Mr. Scott Blackburn – Acting Chief Information Officer, Office of Information Technology at the Department of Veterans Affairs. We are going to discuss the challenges facing us today with medical device security. Thank you all for joining me today! So, I will start with Dr. Schwartz; last month you were speaking and you said that the approach that we're taking in medical devices is evolving, can you expand on that?

Suzanne Schwartz: Oh, absolutely. So, we have seen over the past few years that this state of cyber security within the health care ecosystem and medical devices specifically has been one that has been evolving and this has been a journey for all of the stakeholders; medical device manufactures, health care delivery organizations and for us at the FDA as well. So, as we mature, as we come to learn more, as we experience some of the challenges within the cyber security realm, we are evolving as well in terms of what our expectations are of the industry and how we move from point A to point B to point C to generate greater and greater strength of cyber security within the health care space.

Sean Kelley: When we look at medical device, we kind of relate them Internet of Things; they are connected devices that kind of now we have to approach what we are looking at. But a medical device, depending on agency, depending on the device can be on a network for a period of time. Do we have an average or knowledge of how long that is on a network from start to finish once we buy it?

Suzanne Schwartz: There is a good spectrum of device life time, life cycle and you can have devices that are considered legacy devices. Many of the imaging equipment for example that hospitals will procure, it's with the intent that there would be capital expenditure. Those are investments that are intended to last for a good long time. That can be 10 years, 15 years, and in some cases, we have seen devices have actually been in use for even longer than 15 years, up growth of closer to 20 years. You compare that with other devices where devices may turn over within a shorter life span. But I think that that get to the point of problem here with regard to how do you maintain the security posture of a system and of the devices on that system when these devices were initially designed many years ago without the same level of rigor in terms of security, the same robust security built into them. So, this is where we really see this as a communal problem, a community challenge that we are working towards addressing.

Sean Kelley: Mr. Blackburn, you have by many lists the largest healthcare system in the country, millions and millions of medical devices. Is there an approach that the VA is taking to tackle this?

Transcript:

Scott Blackburn: There is, and thank you Sean, it's an honor to be on your show, and congratulation on the first show here. Veteran care and patient safety is our primary focus and right now at the VA, we are going through a process to really modernize that care. And this is a big priority. As it's mentioned, it can take 10 years or even longer to replace a lot of these legacy medical devices in mitigating security issues is a key component of modernizing VA IT. So, as we work internally with equipment and software vendors to ensure system used are most up to date, security methods and provide continuous monitoring and alerts. VA employs and in-depth strategy that we call medical device protection program to really mitigate the risk of operating older devices on the VA network in taking care of our patients' data and security is imperative for us.

Sean Kelley: So! Dr. Cordts, on that, you have the functional management and bring providers who are specialist in each one of those areas. How are you attacking the medical devices problems?

Paul Cordts: Very similar to the two previous speakers here Sean, I would like to speak to the older medical devices and the new medical devices here. Every device we have, that is connected to network creates some level of risk, perhaps the older devices more than the new devices, we are aware of that. We use a risk mitigation frame work called the Risk Mitigation Framework. And when we do that assessment of the device, we come up with the detail plan and milestones to mitigate all the risk and so that helps us to ensure a level of confidentiality, integrity and availability of our devices that are critical in the IT domain and this is important to the providers too. The providers' want to know that their data is safe and that it's available. So, that's very important to the doctors, the nurses, the medical technicians in our system. The other piece I would like to mention is that we are trying to get our arms around the inventory of disparate medical devices in our system. If we have for example 15 kinds of intravenous pumps, perhaps that number can be reduced from 15 to 3. Or if we have 25 types of defibrillators, why couldn't that number reasonably be 3 – 5. And so, we reduced the number of that type of device in our inventory and we think that that would lead to more efficiency when it comes to doing these RMF frame works.

Sean Kelley: And Scott I believe you are using the RMF frame work as well?

Scott Blackburn: We are!

Sean Kelley: Dr. Schwartz, when we look at all these different types of devices, I think DHA has 4,000 different devices and Dr. Cordts talks about it. Is standardization part of the first step in bringing this risk down?

Suzanne Schwartz: When you speak about standardization, are you talking about the use or adoption of various standards?

Sean Kelley: Selecting fewer devices. So, having similar devices on the network so they can have one approach and kind of know how that device reacts on a network.

Transcript:

Suzanne Schwartz: You know that I think that that's very much a decision of an individual health delivery organization as to what suits their particular architecture, and I think that the point that Dr. Cordts made regarding having an inventory of ones' assets from a device perspective is absolutely crucial. And that is an area that we have heard in our discussions with many health care delivery organization can be a struggle because, in order to be able to secure a device, you have to know what you have, you need to know what's on your network. So, establishing that inventory and then been able to monitor what is on the networks are initial preliminary steps that become really important. But with respect to whether the standardization should be undertaken, I do think that's something that would be individual to the organization that FDA wouldn't necessarily weigh in on one way or another.

Sean Kelley: My guests today are: Dr. Paul Cordts, Director, Functional Champion, Military Health System, Defense Health Agency. Dr. Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, Center for Devices and Radiological Health at FDA. Mr. Scott Blackburn, The Chief Information Officer, Office of Information Technology, Department of Veteran Affairs. Cyber chat on federalnewsradio.com in 1500AM

Sean Kelley: Welcome back to cyber chat on federalnewsradio.com in 1500AM, my guest today are Dr. Paul Cordts, Director, Functional Champion, Military Health System, Defense Health Agency. Dr. Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, Center for Devices and Radiological Health a FDA. Mr. Scott Blackburn, The Chief Information Officer, Office of Information Technology at Department of Veteran Affairs. Scott, has the EO – the Executive Order that was put out earlier in the administration helped in with this area of medical devices?

Scott: I think that it has Sean. I think the cyber EO has helped in two areas; I think number 1; it has really helped the VA collaborate with other federal governments partners, whether it's on medical devices or other topics. I think since the EO has been released, we have seen, an increased federal agency collaboration in information sharing across the medical devices space and in other areas as well. I think number two; it has really helped with mobile security as well. And it has really enabled the VA to make more risk-based decision regarding mobile security, particularly on mobile business transactions with veterans and business partners. And that has really helped us.

Sean Kelley: Dr. Cordts, earlier you talked about the functional program where you have clinical nurses and doctors that helps makes decision about purchases in medical equipment and medical devices. How does that work when it comes to medical devices?

Paul Cordts: Yes, Sean. Interestingly, we have recently created a medical device task force, that's actually led by a clinician but it includes cyber security experts, the analyst, logistic expert and biomedical engineers. So really, there are two issues here; one is around patient safety and I believe in military health system, we a have a very robust patient safety and logistics community and they are able to communicate effectively, I would say in terms of warnings and alerts and defect notices when it comes to medical devices. But the other piece is the cyber

Transcript:

security issue and you know, how do the functionals view that? Part of the role MDI taskforce – the medical device taskforce will be to go to one of our hospital, say what medical devices do you have? And then create that inventory and then ask the clinical functionals what devices is need to be connected to the network because, perhaps they don't all need to be connected to the network and then the piece about the risk management framework. If risk management framework is performed in one of our hospitals, do we have reciprocity, so the next hospital doesn't have to repeat the work associated with doing and RMF. And then the piece I mentioned earlier about some standardization and creating a comprehensive list of medical devices across our entire system. One other piece I noticed are clinical teams moves around between our hospitals and our healthcare systems. Perhaps that's the uniqueness that would lead to wanting us to have fewer medical devices as well as the need to having medical device that's functional both in our garrison hospitals as well as in our operational environments.

Sean Kelley: Dr. Schwartz, as it comes, they say on average, on the literature that I have ready, I am not an expert, that from the design to the element to the point in which a medical device gets their device ready for sale, it takes them around 18 months. Once it gets to the FDA, what does that process looks like?

Suzanne Schwartz: So, depending upon the type of medical device that's coming to the FDA, and FDA regulates medical devices based on a risk basis, so we have Class I, Class II, Class III devices, and depending upon the risk level of the device that will determine the kind of submission that a manufacturer, a vendor would provide to the agency. And as a result of that determination, the time that it takes to review the information that comes into submission may differ. So, class two devices which are often in what we call cleared forward marketing, they come in with something we call 510k Pre-Market notification. And the process for class two device to get cleared and be available to the market is going to generally be much more streamlined to what would be the highest risk device called a class 3 device, which warrants something called a PMA – a Pre-Market Approval application, and because of the evidentiary basis that's needed in order to support a PMA. It's going to take longer time first of all for that device review to be done because, there is often a lot of clinical data as well that has to be carefully gone through to determine what we call a reasonable assurance of safety and effectiveness. You can vary anywhere from 510k a class two device been cleared in a period of, you know I would say I can't give you what the actual averages are but in several months to a year to two years. And a PMA can sometimes take somewhere in the range of several years depending again upon the complexity of the device.

Sean Kelley: So, Scotts and Dr. Cordts, so the question is, you have millions of these devices and as you try to get ready for your FISMA audit and try to get these device on a network, you have these legacy devices. How do you approach such a problem? I mean how do you move from a functional level, from a physician stand point and from a CIO stand point, really looking at the problem like this and say "I can make short term and long term gains but this is where I will go with that.

Scott: Well, it's a challenge, particularly at the VA, we have a 168 major hospitals, over a thousand clinics all across and we need to make sure as Dr. Schwartz mentioned earlier that the physician have the right pieces of equipment in place to be able to do the right clinical

opportunity and at the same time having to secure the patient data and it is a big challenge. I think this is an area where we need to work very closely with our partners in the Veterans' Health Administration, the doctor's and clinicians to make sure that we are doing the right thing, that we are putting the right equipment on a risk space fashion as Dr. Schwartz mentioned but at the same time making sure that we are modernizing to get our veterans the care that they deserve.

Sean Kelley: So, with those kinds of timelines that Dr. Schwartz just gave us, you know we look at budgets, our budgets are shrinking. Is it something that we need to at a technological control or do we really need to start looking at removing some of these devices from the network and how does that really impact patient care?

Paul Cordts: Well! I will take that Sean. We understand that the government budgets are shrinking, but this has to be solvable. We don't have a choice here; the devices have to be secured. We are certainly, acutely aware of instances of malware, and hospital systems been locked out of their electronic health record. We are also acutely aware of the risk of the release of PII – Personal Identifiable Information and Protected Health Information. So are acutely aware of those risks. So, we have to provide safe high quality care for our military beneficiaries on one hand, on the other hand having to protect the D.O.D system from cyber threats. So, I do think it's a challenge for us. And so, we are managing our devices, we are identifying them, we are looking at their risk framework and mitigating the risk. We have created an architecture that will segment the medical devices from the rest of our network and we are moving forward to deploy our new electronic health record MHS genesis.

Sean Kelley: My guests today are: Dr. Paul Cordts, Director, Functional Champion, Military Health System, Defense Health Agency. Dr. Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, Center for Devices and Radiological Health at FDA. Mr. Scott Blackburn, The Chief Information Officer, Office of Information Technology, Department of Veteran Affairs. Cyber chat on federalnewsradio.com in 1500AM.

Sean Kelley: Welcome back to cyber chat on federalnewsradio.com in 1500AM, my guest today are Dr. Paul Cordts, Director, Functional Champion, Military Health System, Defense Health Agency. Dr. Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, Center for Devices and Radiological Health a FDA. Mr. Scott Blackburn, The Chief Information Officer, Office of Information Technology at Department of Veteran Affairs. Scott, has the EO – the Executive Order that was put out earlier in the administration helped in with this area of medical devices?

Sean Kelley: Dr. Schwartz, from the device stand point, are we talking about protecting data or are we talking about protecting patient's safety?

Suzanne Schwartz: That's a really important question Sean! So, thank you for asking and of course FDA is concerned that patient data be properly protected and that data actually not be in some way manipulated either because, integrity of data becomes important from a patient safety standpoint as well. But I want to put our focus for today on the fact that devices since they are providing such important functions, if the performance of that device is somehow impacted as a result of a security vulnerability that has been exploited. Then the performance of that device can result in consequences to the patient that could bring about patient harm. And

Transcript:

so, from our perspective, our mission being one of protecting and promoting or protecting and advancing public health, we want to make sure that we are cyber security and patient safety cross over that we have provided appropriate recommendations and we have set what those expectations are for manufacturers as they; number 1) design and develop new devices. So, on the premarket side, and we have done that through our policy, our premarket guidance. As well as taking the holistic view of making sure that device, once they are deployed, once they are already in distribution and they are in use, that there are expectations and there is management program of risk for those devices throughout its entire life time until its ready to be obsoleted.

Sean Kelley: And Dr. Cordts, from a strategy for Internet of Things, connected devices, does DHA have a strategy?

Paul Cordts: Yes Sean! We have been thinking carefully about that. And mention was made about cyber security in the device of course which we are interested in. But then we have an architecture that provides a secure network of the Internet of Things devices such as alarms, temperature monitor, sensors and things like that. But two other areas that we are thinking about, one example is out intensive care unit, we want medical devices to talk to each other. So, if we have 10 devices that are used to monitor a patient, we want those devices to be able to talk to each other in assessing the sickness of that patient in the intensive care unit. That's one point I would like to make. And the second is, we are looking at consumer wearables and the consumer Internet of Things, thing such as such activity monitor, home blood pressure and glucose monitors, Bluetooth connected to your weight scales and smart phone apps. These pieces of heath information about a patient are useful to the providers. So, we like to have a system and a process whereby we can capture the health information of our patients in our electronic health record with the ultimate goal of having a personal health record which patient could use to store all of their medical and health related data.

Sean Kelley: Scott, I am going to ask everybody their final though as we close this program, but I have one critical question, I hate to put you on the spot. Boston or Cleveland in World Series!

Scott: Red Sox all the way!!

[Cross talk]

Sean Kelley: Scott I will let you kick it off, final thoughts that you would for our listeners to hear.

Scott: I think as we all move forward and as we are modernizing government, modernizing healthcare at the same time, there is all kinds of exciting opportunities whether we are talking about wearable devices, Internet of Things, to improving patient safety, I think there are tremendous opportunities and we are very very excited to pursue those opportunities but I think as we have talked about today, making sure that we are both maintaining the integrity of the devices and patient safety, protecting of data and information, I think this is only going to be a

Transcript:

more and more important topic and these are things that we have the responsibility to make sure that we are staying on top of them and been industry leaders.

Suzanne Schwartz: We are very excited at the FDA about the work that is being done really throughout the entire community. And we are seeing more and more involvement and proactive efforts by our manufactures and other members of the stakeholder ecosystem, so this is not only inspiring, it's very gratifying, and I think that it's going to take time as I said at the beginning, ''This is an evolving journey but we are making great strides and we are looking forward to continue to push that envelope further''. Especially as we look to engage more of our physicians and patients as part of this dialogue.

Paul Cordts: Sean thank you very much and on behalf of my colleagues, thanks for the invitation. I am very pleased to be sitting next to my colleague from the FDA as well as the VA. Particularly as it comes to the Electronic Health Records and the opportunities that we have there, but huge opportunity we think for standardization across our military health care system. Shout out to 3 offices here that really have been rapidly improving our cyber security posture and that's the department of defense CIO's office, AT&L office which is acquisition technology and logistics, specifically the Program Executive Office for MHS genesis, as well as our cyber security experts within the Defense Health Agency. So, I feel like we are rapidly improving in our cyber security domain.

Sean Kelley: Well thanks to all 3 of you. I think this is a topic that we will continue discussing, we would continue evolve as Dr. Schwartz said at the beginning. My guest today have been Dr. Paul Cordts, Director, Functional Champion, Military Health System, Defense Health Agency. Dr. Suzanne Schwartz, Associate Director for Science and Strategic Partnerships, Center for Devices and Radiological Health a FDA. Mr. Scott Blackburn, The Chief Information Officer, Office of Information Technology at Department of Veteran Affairs. I am Sean Kelley and thank you for listening. You can also follow me on twitter @Mrseankelley. We will see you next month!