

# Europe Medtec

////// Technology • Networking • Education

4-6 April 2017 Stuttgart, Germany

David Kleidermacher, Chief Security Officer for BlackBerry, will join Medtec Europe on Tuesday 4th April. We caught up with him ahead of his presentation to ask a few key questions about mHealth and Digital sector.



David Kleidermacher,  
Chief Security Officer,  
BlackBerry

As Chief Security Officer for BlackBerry, David oversees product security strategy, directs the Center for High Assurance Computing Excellence (CHACE) research team, and manages security communications and technical analyst relations. David has 25 years of security strategy and product engineering experience. Prior to joining BlackBerry, David served as Chief Technology Officer at Green Hills Software, where he was responsible for technology strategy and R&D.

## **Your presentation will focus on the mobile device as a medical device, why is this topic so crucial now?**

Today, the FDA does not permit the use of off-the-shelf mobile devices in life-critical therapy because they are not developed and approved against FDA medical device standards. Yet the use of connected healthcare systems, such as cardiac pacemakers, home infusion pumps, and diabetic wireless insulin patch pumps, is growing. The inability to leverage mobile devices to control these systems represents a massive missed opportunity.

## **What are some of the latest innovations in this space?**

One area of innovation involves the secure isolation of medical software on a mobile device, so that life-critical functions can be assured even in the presence of mobile malware and other threats. A second area involves the development of new, cost effective standards to evaluate the security of mobile medical software and connected healthcare devices so that patients, caregivers, regulators, manufacturers, and other stakeholders can achieve the level of assurance needed for deployment of these solutions.

## **What tangible benefits can mobile devices offer to patients when used in this way?**

The use of mobile devices to control medical equipment will improve therapy and reduce the cost of healthcare. For example, a diabetic child could use a smartphone app, instead of an obtrusive and expensive custom controller, to program a patch insulin pump, dramatically improving her quality of life while reducing treatment cost.

## **One key challenge around the use of mobile devices in healthcare is how data and privacy is managed, what are the main concerns and how can these be allayed?**

As we connect more things and use them to manage our medical lives, the risk to and concern for our privacy is increasing. However, privacy is simply a subset of security in which the desired security

controls focus on protection of personal information and other rights (e.g. right of consent and right to be forgotten). Secure medical devices and software, along with high quality security standards, can protect privacy as well as life-critical function. In fact, the potential for improvements to privacy may well drive these initiatives since the variety and number of people leveraging mobile devices for privacy-sensitive healthcare will far exceed those using them for life-critical therapy.

## **You are leading a variety of security policy initiatives and you also received Diabetes Technology Society's 2016 Leadership Award for pioneering work on medical device security standards. Was that an award you expected and how did you get there?**

The award was quite a surprise as there are many incredible diabetes technology researchers, engineers, and other leaders who are working every day to improve quality of life for diabetic patients and deserving of this award. Security is a hot topic as medical systems are constantly being shown to be vulnerable. Yet today we utterly lack a comprehensive program to evaluate the security of medical systems. I don't see a way forward for the world to gain the confidence it needs by simply crossing our fingers and hoping developers will eventually do a good job on security. The world needs assurance that comes from independent evaluation, and this need applies not only to medical systems but also across the connected world and Internet of Things. Filling this need has been my passion for many years, and this new medical security standard represents the current best approach in the world today. I hope many others will join the fight.

“  
**The use of mobile devices to control medical equipment will improve therapy and reduce the cost of healthcare.**  
”

## **What opportunities do you foresee for mHealth in the coming year?**

We're just starting to scratch the surface of how to leverage smartphones and wearables in healthcare, reducing hospital time and costs while improving outcomes and quality of life. I have total confidence that technologists will continue to innovate and amaze us. However, I have zero confidence that privacy and security concerns will be adequately met on our current path. In fact, security will act as a barrier to innovation, unless we make it a higher priority in the coming year and convince key stakeholders that status quo is not cutting it. When it comes to security, hope is not a good strategy.

