by Miles Johnson, MS; Scott Thiel, MT (ASCP), MBA, RAC; and Jennifer Mitchell, JD, CIPP/US

The Internet of *Medical* Things: Cybersecurity and diabetes device risks

» Internet-connected devices are gaining popularity, but introduce security vulnerabilities.
» Cybersecurity breaches of unsecure devices threaten patient privacy and safety.
» Manufacturers and hospitals must recognize vulnerabilities and implement security countermeasures.
» FDA now requires focus on cybersecurity in device development.
» Risk management evaluations are a key tool for device development.

Johnson

Thiel

Mitchell

Miles Johnson *(miles.johnson@navigant.com) is a Consultant and* ***Scott Thiel*** *(scott.thiel@navigant.com) is a Director in the Indianapolis office of Navigant Consulting.* ***Jennifer Mitchell*** *(jennifer.mitchell@navigant.com) is a Director in Navigant's Los Angeles office.*

In recent years, the management of diabetes has benefited tremendously from advanced technology and innovation. Indeed, it won't be long before manual insulin injections and finger-stick blood glucose monitoring are forgotten practices. However, the new concepts and products coming to market bring certain risks, particularly from cyber criminals and hackers. We hope that raising awareness about this vulnerability will encourage the medical device industry to make secure technological design an integral part of every new innovation.

Connected medical devices and cybersecurity

Consider this: The question is no longer if an artificial pancreas is possible, but when it will become commercially available. With every major insulin pump company working in this area, along with many startups, patients will not have just one system, but several from which they can chose.

Devices using advanced automation technologies generally give users peace of mind, because patients, caretakers, and family members can monitor real-time glucose level data and ensure wellbeing. Importantly, the mobile device and cloud-based aspects of any artificial pancreas solution will likely rely on wireless connectivity for delivering a continuously variable solution. Although the overall benefits of connected health technology for diabetes care are significant, it is also important to recognize the vulnerability of the technology and plan for sufficient security countermeasures at all steps of product development and deployment.

Connected medical devices, like all other computer systems in the healthcare universe, incorporate software that is susceptible to hackers and internet viruses. The implications

of software-controlled systems and the threats to device security and, consequently, patient wellbeing and privacy weigh heavily on everyone in the connected health and device industry.

Unfortunately, many stakeholders lack the tools to assess the clinical impact and risk of these vulnerabilities. Still others fear that real fixes to problems might not occur until there is a patient death. However, companies that incorporate effective cybersecurity measures and quality systems at the outset will be better prepared to mitigate cyber breaches and reduce legal risks if they occur.

Vulnerabilities of medical device security

Although the advances in information transmission can facilitate patient care, the exploitation of connected medical devices via cyber hacking poses two real concerns to privacy and safety.

Privacy

Cyber criminals constantly target the $3 trillion US healthcare industry,[1] whose many companies and hospital groups still rely on aging computer systems that lack adequate security. Hackers normally search for the weakest link in the system, and medical devices represent the soft, vulnerable underbelly of healthcare networks. According to a recent *Reuters* article, "Your medical information is worth 10 times more than a credit card number on the black market," because the information obtained from a medical record cannot be cancelled and re-issued easily, unlike a credit card.[2] The personal data from medical records can be used over and over again, and patients may not be aware that they have been victimized for years.

It is clear that hospitals and health insurance companies have become a hot target for ransomware attacks. Hackers threaten to permanently encrypt (or release to unauthorized users) stolen patient records unless hospital management teams succumb to paying a ransom. Recently, there has been an uptick in frequency of these crimes, given the inherent vulnerabilities of connected devices. The devices require the wireless transmission of stored patient data either via Bluetooth or Wi-Fi technology. Hackers penetrate the networks, invade the devices and servers, and then steal the valuable electronic health record (EHR) information.

Despite the industry's general awareness of the cybersecurity issue, regulators and the industry itself have been slow to respond or anticipate the constant threats. The 1996 Health Insurance Portability and Accountability Act (HIPAA) and the HITECH Act in 2009 established fairly straightforward rules about medical providers' obligations in the event of a breach of patient or customer data.[3] But the rules in these Acts are not always the best stewards for protecting EHR data. HIPAA does not require that patient data be encrypted, and most companies see the extra security step as an expensive complication. Plain text records in hospitals are tempting targets for hackers. HIPAA does provide a framework for handling risk, but does so without offering explicit guidance. Furthermore, the requirements fail to secure company data in today's ever changing environment. Unless organizations realize the severity of the issue and step up to the challenge, limited cybersecurity measures will continue to plague the vulnerable networks and misconfigured Web servers (and patient records) of hospital IT systems.

Safety

A more critical concern in the cybersecurity war zone is patient safety in all environments. Selling hacked EHR data may seem mundane compared to the deadly risks associated with a cybersecurity breach into an insulin infusion

device connected to a critical care patient. And the cyberbreach may have completely unintentional consequences. For example, malware leaks, with codes designed to steal credit card details, can inadvertently cause chaos in the medical device arena.

This is the world of the Internet of *Medical* Things. One reason patient care centers suffer frequent malware attacks is because they house a large number of Internet of Things (IoT) devices. The devices have wireless capabilities, but often lack robust security features. Users may fail to change a default password from 0000 and, therefore, leave their connected medical devices vulnerable to malware threats that probe Internet-connected devices for such weaknesses. Many connected insulin pumps and continuous glucose monitoring (CGM) devices run the same operating systems as consumer devices and larger information systems, and automated hacking tools cannot tell the difference between a tempting target full of credit card details or EHRs and a life-saving medical device attached to the Internet. A malware attack on a very sensitive, glycemic-controlled patient could cause serious problems by rendering a device unresponsive or causing it to deliver hazardous drug loads.

There is ample proof that this safety threat is real:

- In 2011, a group of researchers (or researchers operating as hackers) demonstrated security attacks on popular CGM and insulin delivery systems. Their study showed "both passive attacks (eavesdropping of the wireless communication) and active attacks (impersonation and control of the medical devices to alter the intended therapy) can be successfully launched using public domain information and widely available off-the-shelf hardware."[4]
- In October 2011, in Miami, Florida, with the support of McAfee (now a division of Intel), famed late hacker Barnaby Jack made a presentation at the Hacker Halted conference, exposing security vulnerabilities that allowed an insulin pump to be remotely commandeered via radio frequency.[5]

And the implications are beyond malicious: Imagine cyber terrorist hackers wirelessly exploiting vulnerabilities in pacemakers to carry out untraceable assassinations against political targets or create a widespread panic by making deadly adjustments to insulin pumps of a large user-group across the nation. Healthcare facilities and patient homes remain vulnerable in the crosshairs of an attack, because most of these settings depend on infrastructures that haven not been securely updated. Manufacturers are insufficiently aware of the risks of exposure in the clinical environment and are often new to the regulatory environment. There are benefits to integrating the latest technologies within medical products, but manufacturers and providers should acknowledge these possible breaches and provide more robust security options to minimize risks in their software and networks.

Government regulations and guidance

The good news is that both the healthcare industry and the U.S. Food and Drug Administration (FDA) are paying greater attention to the cybersecurity risks of "diabetes" medical devices. The increased network integration of these devices is leading to new patient safety risks, and the FDA is working hard to raise awareness about the issue. The FDA has increased its consideration of cyber risks during its premarket review of medical devices. The FDA also has provided industry guidance associated with cyber risks and suggestions for how manufacturers should address them.

In June 2013, the FDA released draft guidance about managing cybersecurity in medical devices, with the final guidance being released in October 2014.[6] Drawing on many of the experiences and much of the associated research presented here, the FDA guidance emphasizes the need to consider device security during the design and development stages of medical devices. Specifically, the guidance recommends:

- Identifying assets, threats, and vulnerabilities;
- Assessing the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessing the likelihood of a threat and of a vulnerability being exploited;
- Determining risk levels and suitable mitigation strategies; and
- Assessing residual risk and risk acceptance criteria.

In January 2016, the FDA released draft guidance for post-market management of cybersecurity in medical devices. The final guidance of this draft was released in December 2016.[7] The 2016 guidance expands upon the 2014 guidance to provide insights into monitoring and maintaining cybersecurity of devices after they are introduced into use. Of key importance is risk management and understanding the use of the devices and the risks associated with a compromise of cybersecurity.

The FDA's guidance documents expand upon the general information under 21 CFR 820.30 (Design Controls) to require more consideration of cybersecurity by establishing a cybersecurity vulnerability and management approach as part of the software validation, risk analysis, and post-market management plan.

In addition, in September 2016, the Government Accountability Office (GAO) reviewed the U.S. Department of Health and Human Services' (HHS) security and privacy oversight and published a report identifying significant gaps in the cyber security guidance provided by HHS to entities regulated by HIPAA.[8] The report's primary criticism emphasized that though HHS prepared a crosswalk with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the crosswalk lacked many of the cybersecurity requirements identified by NIST in the framework. These gaps unnecessarily expose EHRs to security threats.

Cybersecurity standards

In addition to these governmental efforts, the work of the Diabetes Technology Society (DTS), a non-profit promoting the development and use of technology to fight diabetes, is another step in the right direction. DTS recently released a cybersecurity standard (DTSec) whose goal is to raise confidence in the security of network-connected medical devices through expert security evaluation.[9] DTSec is a technical community composed of clinicians, manufacturers, cybersecurity experts, academia, and government members. The DTSec program focuses on four device classes: blood glucose monitors, CGMs, insulin pumps, and artificial pancreases. DTSec is a significant advance for medical device safety, because this standard has the ability to evaluate and ensure security that will enable new—and secure—therapeutic breakthroughs.

The ISO/IEC 80001 series of standards also provides a framework specific to the medical device ecosystem by defining roles and responsibilities, activities, risk and lifecycle management, security capabilities, and guidance on specific topics (e.g., guidance for wireless networks). During the Obama Administration, there were even pushes from Executive Orders (13636 & 13691)

and Presidential Policy Directives (PPD-8) designed to strengthen cybersecurity infrastructure and information sharing in the private sector.

These steps in advancing regulation will largely define the future of medical device security. However, security is an unstable game of trade-offs, and current political stakes could drastically alter the healthcare market.

What's ahead in 2017

The Trump Administration has already sparked tremendous discussion around regulatory policy changes in Washington. His pledge to have Congress repeal the Affordable Care Act (ACA) has been on the forefront of his agenda. Trump and Congress appear to be backing away from the initial plans to immediately repeal ObamaCare, because it is too cumbersome of a task to replace it while also repealing it. The ObamaCare medical device excise tax of 2.3%, which taxes device sales, has gathered significant attention. A Congressional bill in December 2015 suspended the tax for two years. When this article went to press, the device tax was still in place, although a bill is under consideration that would permanently repeal the tax.

In terms of his First 100 Days Action Plan, Trump claims he will ease regulation at the FDA to expedite drugs awaiting approval. Although most of the restrictions Trump is targeting apply to drugs, some will affect the medical device industry as well.

The "21st Century Cures" legislation won House approval in early December with a 392–26 vote. Many Senate Democrats oppose the bill, but the White House strongly supports the passage. The bill authorized $4.8 billion to the National Institutes of Health (NIH) and $500 million to FDA over 10 years. The 21st Century Cures legislation also contains provisions to accelerate the approval of new medical treatments, especially devices. Funding for new research and breakthrough treatments deserves praise, but more attention ought to be shifted to the growing issue of cybersecurity, too. It is difficult to know where to draw the line for accelerating the approval of breakthrough devices while also considering the risks for patients.

Conclusion

Security has been an afterthought for many medical providers and device manufacturers, whether in setting budgets or in building encryption into software to protect patient records and information. But as increasingly sophisticated threats are detected each day, the solutions need to be upgraded constantly to provide adequate firewall security and prevent cyber breaching. Unfortunately, the big-picture problem of unsecure medical devices will take a decade or more to solve. That is because the time-to-market for most medical devices is usually 5–10 years, sometimes longer. This means a securely designed medical device submitted to the FDA for approval today will not see the inside of a hospital (or the inside of a patient) until the 2020s. And that is assuming medical device manufacturers decide right now to make cybersecurity a priority, built in by design and not "bolted on" in version upgrades after the fact.

It is difficult to know where to draw the line for accelerating the approval of breakthrough devices while also considering the risks for patients.

In the world of the Internet of *Medical* Things, networked medical devices are worth

the risk. Automating hospital systems relieves medical staff of rudimentary duties, such as monitoring delivery of medicine intravenously to patients, and can help prevent human error, a common cause of injury in hospitals. Medical device manufacturers, hospitals, and regulators, however, need to collaborate more systematically and effectively. These groups will be better off incentivizing the correct behavior to manage cybersecurity. To this end, they must incorporate a risk-based approach to ensure that the pending hacker risks to public health are addressed appropriately. Manufacturers, providers, and payers need to align with the frameworks put forth by FDA, Presidential Executive Orders, DTSec guidelines, and other regulatory controls. Companies need to be held responsible to existing quality system regulations and post-market authorities.

1. Caroline Humer and Jim Finkle: "Your medical record is worth more to hackers than your credit card" *Reuters*; September 24, 2014. Available at http://reut.rs/2nxZKw0
2. Dan Lowe: "The Growing Threat of Malware within Medical Devices" *Bitdefender OEM Hub*, Insights into Antivirus Technology. 2016. Available from: http://bit.ly/2nHaYP7
3. Aaron Sankin: "The real reason hackers want your medical records" *The Kernel*; April 26, 2015. Available at http://bit.ly/2mpJ2PE
4. Chunxiao Li, Anand Raghunathan, and NK Jha: "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system" *ResearchGate*; June 1, 2011. Available at http://bit.ly/2n4DbfB
5. AJ Burns, M Eric Johnson, and Peter Honeyman: "A Brief Chronology of Medical Device Security" Communications of the ACM; October 2016;59(10):66–72. Available at http://bit.ly/2naDKGl
6. Idem.
7. U.S. Food & Drug Administration: Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and FDA Staff. December 28, 2016. Available at http://bit.ly/2nOYGB8
8. Lynn Sessions and Suchismita Pahi: "GAO Report Criticizes HHS' HIPAA Cybersecurity Guidance and Program" *Health Law Update*. 2016. Available at http://bit.ly/2nPdOOY
9. Diabetes Technology Society (DTS) press release: New Standard to Raise Confidence in the Security of Network-Connected Medical Devices through Expert Evaluation. May 23, 2016. Available at http://bit.ly/2njMeMb