

Coordination or Collision? The Intersection of Diabetes Care, Cybersecurity, and Cloud-Based Computing

Journal of Diabetes Science and Technology
2017, Vol. 11(2) 195–197
© 2016 Diabetes Technology Society
Reprints and permissions:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/1932296816676189
journals.sagepub.com/home/dst


Scott Thiel, MBA¹, Jennifer Mitchell, JD², and Jim Williams, BA¹

Abstract

Diagnosis and treatment of diabetes changed little from the Middle Ages through the early 19th century, when the first chemical test for the condition was developed. In the 20th century, advances in diabetes management gained momentum with home-use diagnostic devices and mass-produced insulin. In the 21st century, technological developments around diabetes are advancing so rapidly that a small, discrete system of medical devices that serve as an artificial pancreas are now possible. In this article, we assert that medical device interoperability and cyber security are necessary preconditions for safe, effective, and reliable widespread use of the artificial pancreas system.

Keywords

diabetes, interoperable, interoperability, cybersecurity, data privacy

Being a doctor before the 20th century was not an enviable job, especially when treating people with diabetes. There were no labs with analyzers, latex-free exam gloves, or sanitizing hand gel. In 1776, a physician's tools were a cup and taste buds, because physicians tasted a patient's urine to see if it was sweet, just as doctors had in the Middle Ages (the first chemical tests for diabetes were not developed until the early 19th century). This diagnostic method led to the phrase we use today to refer to the chronic disease: diabetes (siphon) mellitus (honey). Diabetes mellitus is most common form of the disease. It is caused by a deficiency of the pancreatic hormone insulin, which results in the body's inability to metabolize sugars and starch. Sugars therefore accumulate or "spill over" into the blood and urine. The buildup of sugar in urine led to the sweetness detected during the unenviable taste test.

Insulin as a treatment for diabetes was shown to be a viable option in the early 1920s, and Eli Lilly and Company began bulk manufacturing of insulin later that decade. Dip strips to test for sugar in urine (generically known as "clintrips" or "clintix") were introduced in the 1940s. Blood glucose monitoring for home use did not reach the market until the 1960s and 1970s, with fairly bulky and complex devices such as the Ames Reflectance Meter that relied as much on technique as on science to obtain a valid result. Fortunately for patients, today the market is awash in small, discrete, battery-powered diagnostic devices and disposable test strips that take very little technique to use and provide a reliable result.

The blood glucose monitoring systems used today are able to automatically determine blood glucose levels from a sub-microliter amount of blood placed onto a disposable chemistry pad. The results are time-stamped and stored, often with additional user-entered contextual information. The devices are able to store hundreds of results and later upload the results wired or wirelessly to external software. There are also continuous glucose monitors (CGMs) that use subdermal sensors connected to small electronic devices contained inside a patch adhered to the abdomen. CGMs typically measure glucose in the interstitial fluid to estimate the amount of glucose in the blood and the rate and direction of change in glucose levels.

Similarly, delivery of insulin has transitioned from reusable glass syringes with hypodermics the user had to sharpen to high-tech insulin infusion pumps capable of near-continuous delivery of minute amounts of fast-acting insulin. Insulin pumps today are also small and discrete, and are capable of collecting and sharing large amounts of the user's health data.

¹Navigant Consulting, Inc, Indianapolis IN, USA

²Navigant Consulting, Inc, Los Angeles, CA, USA

Corresponding Author:

Scott Thiel, Navigant Consulting, Inc, 9001 Wesleyan Rd, Ste 200, Indianapolis, IN 46268, USA.

Email: scott.thiel@navigant.com

Current ongoing development of the various devices used in the monitoring and treatment of diabetes mellitus includes continued efforts to increase the precision and accuracy of the handheld and CGM devices as well as insulin delivery. However, current methodologies are likely near the limit of what is technologically possible, especially in the home environment.

Flexible circuit boards, better and smaller batteries, and glucose-sensitive inks are some of the concepts typically mentioned when discussing future diabetes management technology leaps. The more likely next step, however, is the interconnection of diabetes management devices. Interconnection of the devices takes advantage of the information collected by spot-monitoring blood glucose (SMBG) devices, CGMs, and insulin pumps. Each of these devices already collects a vast amount of a diabetic's health information at various points in time during the day, week, or month. Most of these devices already contain hardware and software capable of transmitting the stored information wirelessly using either Bluetooth (BT) or Wi-Fi technologies. The question for the near future concerns the risks and benefits associated with the collection and connectivity of all of that information.

The tie that binds the devices and information into a system is software: software in the devices (firmware or embedded software), mobile apps, Fog software, and cloud (a network of remote servers hosted on the Internet) software. A good deal of software exists already that graphs data from these devices, generates mealtime or titration recommended amounts for insulin delivered, alerts users of current or predicted hazardous situations based on results, and allows clinicians to have a better patient history record. Tightening the bonds between the various devices and software leads us closer to the elusive goal of an artificial pancreas.¹ Realization of an artificial pancreas, while not an implant, could bring people with diabetes closer to a life where daily interaction with each device is minimized: the CGM and insulin pump exchange information with software that analyzes the information and sends insulin delivery adjustments to the insulin pump, all with little interaction from the user.

But there are costs and risks associated with such a useful system. Additional research and development (via use of mathematical modeling) to improve use of CGM and SMBG data in relation to the body's reaction to glucose and insulin are necessary. The ability to tailor a software application to each individual patient is also needed. Furthermore, success for such a system hinges on reliable communication infrastructures; reliable, accurate, and correct data inputs; and the ability to seamlessly swap out disposables and worn out equipment during the life of the user. The devices in an artificial pancreas system must be interoperable.

Interoperability is the ability of 2 or more systems to interact and exchange usable electronic data. For the current article, interoperability is further defined as the concept of demonstrating a system is safe with a user performing and verifying

configuration and connections, while using the device within the manufacturer's original intent. Interoperability allows for information and devices in the system to be shared and interchanged seamlessly. Information about the patient, status of therapy, and status of devices can be shared within the system and with anyone who has access to the system. For systems with a cloud-based component, the sharing is limited only by the number of individuals with access to the data.

Regardless of whether there is a cloud-based aspect to an artificial pancreas solution, such a solution will undoubtedly rely on wireless connectivity. One only needs to look at devices offered by Medtronic, DexCom, Roche, Lifescan, and OmniPod to find wireless diabetes management devices. There are also groups such as the Personal Connected Health Alliance providing a framework and guidance on use of wireless communication standards to aid these manufacturers in developing interoperable devices.² The advent of inexpensive and energy efficient communication components like Bluetooth Smart (or low energy) facilitate the creation of wireless devices and, thus, wireless networks.³ Within the user home, wireless data hubs such as the Qualcomm Life 2Net hub provide a common point for collecting data and passing it to cloud-based software or databases.⁴ In short, the future of wireless health networks is already here.

With a system of networked devices that have direct impact on daily (and sometimes hourly) health of a person with diabetes, security of the network and the associated information becomes critical from a safety perspective. A wireless or cloud-based system can be hacked to control the connected devices or the data from the devices. Ransomware is a newer form of hacking and may spread more widely than remote control of devices.⁵ In these malicious ransomware attacks, the devices in a system or the associated data could be made unusable until a ransom is paid. As yet, there are no known cases of ransomware associated with medical devices. Furthermore, the most likely targets of ransomware attacks are devices connected to hospital networks (consider all hospital infusion pumps suddenly shutting down).⁶⁻⁸ The failure of manufacturers to incorporate adequate cyber and physical security measures in home use medical devices could lead to the artificial pancreas system becoming a viable target for hackers.⁹ But designing and developing these systems consumes resources—measured in both time and dollars—and consumes even more if addressed reactively rather than proactively.

Should the dream of an artificial pancreas be dropped due to fear or should researchers and manufacturers simply plow full ahead? Neither. A reasoned, risk-based approach incorporating continual learning and improvement can help find acceptable risk associated with an artificial pancreas. As with any medical device, risks are inherent; continually driving risks to a level accepted by supporters and users of devices allows us to use thermometers and first aid equipment; provides delivery of lifesaving drugs and immunizations; and

creates the environment and tools to support surgical procedures. All of these medical devices help provide for healthier and longer lives—despite the risks associated with each. Cyber threats are simply another risk that must be considered and thoughtfully addressed in the development and delivery of interoperable and interconnected medical devices.

The US Food and Drug Administration (FDA) has increased its consideration of cyber risks during its pre-market review of medical devices. The FDA also has provided guidance associated with cyber risks and suggestions for how manufacturers should address them.^{10,11} Application of existing cyber security practices and standards in the medical device industry can also be useful, especially for the software tying a medical device system together. However, the application of these standards may require careful consideration before use, because in terms of user safety, the health care and life sciences areas in which these devices are used is less forgiving than typical consumer electronics.

The rate of change in how diabetes mellitus is diagnosed, monitored and treated has increased significantly since the 1940s. The near-term future of these devices likely includes some of the first artificial pancreas systems comprised of wireless interoperable devices and associated cloud-based software. For these first-time systems to be successful, cyber and physical security measures must be included in the design from the beginning; otherwise, manufacturers will pay much higher costs in terms of patient safety, regulatory agency enforcement actions, lawsuits, reputational damage, and system remediation costs. Perhaps in another 50 years these early systems will be looked on and considered about as palatable as tasting urine is considered today. To support the evolution of these systems, we must ensure the systems of today and the near future provide consistent, reliable, and accurate performance and information. Cyber security is pivotal in ensuring these goals.

Abbreviations

BT, Bluetooth; CGM, continuous glucose monitor; FDA, Food and Drug Administration; SMBG, spot-monitoring blood glucose.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. Juvenile Diabetes Research Foundation. Artificial pancreas. 2016. Available at: <http://www.jdrf.org/research/artificial-pancreas/>. Accessed September 12, 2016.
2. Personal Connected Health Alliance. 2016. Available at: <http://www.pchalliance.org/>. Accessed September 12, 2016.
3. Bluetooth. Low energy. 2016. Available at: <https://www.bluetooth.com/what-is-bluetooth-technology/bluetooth-technology-basics/low-energy>. Accessed September 12, 2016.
4. Qualcomm. 2net™. 2016. Available at: <https://www.qualcomm.com/products/2net>. Accessed September 12, 2016.
5. Ossola A. Hacked medical devices may be the biggest cyber security threat in 2016. *Popular Science*. November 23, 2015. Available at: <http://www.popsoci.com/hackers-could-soon-hold-your-life-ransom-by-hijacking-your-medical-devices>. Accessed September 12, 2016.
6. Murdock J. How a security researcher easily hacked a hospital and its medical devices. *International Business Times*. February 15, 2016. Available at: <http://www.ibtimes.co.uk/how-security-researcher-easily-hacked-hospital-its-medical-devices-1544002>. Accessed September 12, 2016.
7. Niccolai J. Thousands of medical devices are vulnerable to hacking, security researchers say. *PCWorld*. September 29, 2015. Available at: <http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html>. Accessed September 12, 2016.
8. Radcliffe J. Hacking medical devices for fun and insulin: breaking the human SCADA system. n.d. Available at: https://media.blackhat.com/bh-us11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Accessed September 12, 2016.
9. Mann M. This diabetes activist hacked her medical device and made an artificial pancreas. *Vice Motherboard*. May 23, 2016. Available at: <http://motherboard.vice.com/read/this-diabetes-activist-hacked-her-medical-device-and-made-an-artificial-pancreas>. Accessed September 12, 2016.
10. US Food and Drug Administration. Postmarket management of cybersecurity in medical devices. Draft guidance. January 22, 2016. Available at: <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf>. Accessed September 12, 2016.
11. US Food and Drug Administration. Cybersecurity. Updated May 10, 2016. Available at: <http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>. Accessed September 12, 2016.