Making Trade-Offs for Safe, Effective, and Secure Patient Care

Dan Lyon¹

Journal of Diabetes Science and Technology
2017, Vol. 11(2) 213–215
© 2016 Diabetes Technology Society
Reprints and permissions:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/1932296816676281
journals.sagepub.com/home/dst

Abstract

As the health care model evolves to deliver on demand care, patients are becoming more responsible and interested in their data. The security of the medical devices and connected systems becomes increasingly more important because it plays a significant role in achieving better patient outcomes. Diabetes patients are at the forefront of this evolution and yet on the receiving end of diabetic equipment manufacturers delivering systems that support secure care. In order to deliver the best patient outcomes, complex trade-offs are required, including (1) usability, (2) cost, (3) time to market, (4) device life cycle, and (5) patient privacy. These trade-offs for security cannot be made without a comprehensive informed development process.

Keywords

cybersecurity, security, development process

In many ways, diabetes patients are leading the way for the shifting paradigm in medicine. Patients are directly benefiting from automation replacing manual processes through devices like continuous glucose monitors. They are also benefiting from increased availability of their data for self-management, as well as access to historical monitoring data by caregivers and health care professionals through the Internet. Integration of consumer technologies like mobile phones means that patients and caregivers can have on demand access to data and use that information to make informed decisions. All of these items are intended to increase the quality of life for patients.

However, items like increased access over the Internet and use of mobile phones present significant security concerns. Recent articles on cybersecurity in pacemakers and defibrillators highlight how security can take front and center in the media. One such report was from Muddy Waters Research, where a security researcher made claims that a line of St. Jude pacemakers is missing basic security protections such as encryption. While the report has had some critical responses from independent organizations like Virta Labs that show patient safety may not be at risk, events like this can still produce concern and worry among patients. In the worst case scenario, patients may even decide to forego beneficial therapies because of an incorrect perspective on security risk. Decisions like that are not helping deliver better outcomes.

This article describes the challenging topic of cybersecurity, medical devices and the balancing act that is required to deliver diabetes patients new therapies using secure systems.

It is well known that security is an emergent property of systems. Today systems that monitor patients with diabetes and provide anytime, anywhere access to medical data are complex. For those designing these systems, delivering a secure system is a bit like solving a Rubik's cube; many different sides of the problem exist, and must be solved concurrently. A solution that solves only for usability is missing the side of the Rubik's cube that represents security.

One of the challenges with security is that it is an attribute covering the entire system. Users and their password choices, communications and back end systems never seen by users are all important for the security of the system. The trade-offs of usability, cost, time to market, device life cycle, and patient privacy are some of those that must be balanced when designing a secure system.

Usability

One of the items that can be particularly challenging to design adequate security around is usability. Some aspects of usability are driven by the patient population that will be using the device. For example an older patient population has a different foundation for using technology than a younger one, and a system that is usable by younger patients may not be usable by older patients.

¹Cigital, Inc, Dulles, VA, USA

Corresponding Author:

Dan Lyon, Principal Consultant, Cigital, Inc, Dulles, VA, USA.
Email: dlyon@cigital.com

One example of the intersection of security and usability is provided by passwords. Password-based systems have technical security controls that can provide the necessary security, but only under certain conditions that are directly influenced by the person selecting the password. This is the reason that web sites ask for passwords of a certain length, with numbers, letter and special characters.

From a security perspective, very long and completely random passwords offer the best protection. From a usability perspective, a very long and completely random password cannot be remembered. On traditional computer systems, there are technologies that can help to solve this called password managers. They allow storage and retrieval of long, random passwords so that a user does not need to remember the password. Security experts consider use of a password manager a requirement for people to securely use any password-based system. That presents a problem however, because medical devices do not allow users to install additional software like a password manager. The result is that users will use a weak password which can be easily guessed, circumventing all the security controls within the system.

Finding the appropriate balance in this type of problem is essential to maintaining both usability and security. The patient population, use scenarios, and use environment all affect the kinds of security controls that are reasonable.

Cost

Adding cost to medical devices translates to increased costs for patient care. For manufacturers that produce medical devices, there is tremendous pressure to make products and therapies more cost-efficient, both from insurers as well as patients.

A secure solution requires some fundamental technologies to support the security triad of confidentiality, integrity, and availability. But the addition of new security technologies raises the cost to produce and purchase the medical device. There is tension between adding features and delivering value that can be difficult to balance.

At a time when there is a lot of pressure to make health care more affordable for patients, these increased costs provide little perceived value for both providers and patients. Thus, security is often viewed as something which is in direct competition with providing better care for patients.

However, the opposing view of the security technology (increasing costs and detracting from the availability of new patient therapies) is the question of how can patients have the right care, at the right time, from the right care provider? A system that can be manipulated by someone with malicious intent cannot be trusted to provide the right care. A secure system provides the foundation for enabling the right care for the patient. Safe and effective care has always been the goal of medical devices, and now achieving that goal requires the therapy systems to maintain data confidentiality, integrity, and availability.

Time to Market

Patients living with diabetes are looking for a better quality of life that medical technology can provide, and from their perspective the sooner the better. Patients desire the best and newest therapy; however it can take a long time to bring new solutions to market. This can be seen by the fact that solutions for diabetes are moving into a new treatment paradigm that involves mobile phones and the Internet. Moving the functionality of a process like monitoring blood sugar levels to the Internet and a web browser seems like a simple task because it is now so common to have things connected to the Internet. Patients and caregivers can imagine the benefits these systems would bring, and are asking for them because they can help increase patients' quality of life.

Along with patient demand for new technologies are the business drivers for delivering a product to market faster than the competition. When a product is first to market, significant market share can be obtained which increases profits.

Business leaders often do not understand the security investments necessary to adopt new architectures such as one that uses mobile phones and Internet communications. As a result there can be significant resistance to investing into secure system architecture because it takes longer and costs more to develop. The drivers of patient demand and business opportunity present a perfect storm that puts pressure on short development cycles.

Device Life Cycle

Even for those that are not in the security industry, it is hard to miss the frequent media articles around data breaches and security vulnerabilities. Users of computers and phones are constantly asked to upgrade software that includes security fixes, as often as once a month for some of the major operating systems.

The release and patch development cycle, where vulnerabilities are discovered in released software and then patched on a regular basis is in direct competition with devices like insulin pumps. Medical devices do not follow the rapid update cycles of consumer technologies like phones, and they are intended to be used for longer periods of time. For evidence, look at warranty periods—a Medtronic MiniMed insulin pump warranty is 4 years, while an Apple iPhone warranty is 1 year.

There are many reasons why updates are done differently with medical devices. The primary one is that every time a software update is installed, it may cause problems. I've seen security patches on operating systems that break existing software applications, and it is frustrating to have systems quit working unexpectedly. For life-sustaining therapies the risks are much higher than just frustration. The increased risk requires more development and testing to ensure safe and effective behavior. This increased effort translates to a higher cost for delivering the security update.

While leveraging mobile technologies and consumer platforms is attractive for both the patient and the manufacturer, it introduces risks around update cycles and how those are managed.

Patient Privacy

Patients not only want their data, but it is increasingly important for self-management of chronic diseases like diabetes for patients to have access to the data. With mobile lifestyles, access from a patient's phone or computer is a definite benefit. However that means that data is now accessible over the Internet.

Privacy is something that used to be a lot easier to manage. There were physical paper records in a doctor's office, not electronic copies in the cloud. With current systems, anyone with access to the electronic records system could potentially view patient private data, if the appropriate controls are not in place.

But then if too many restrictions are in place the data may not be available to some when they need it. And how about caregivers and others that patients may want to have access to their data because they help manage their disease state? This could be people in the same household or across the ocean. Patients need a way to not only have access to their data, but also to have some control over who else may have access to their data. These are the kinds of problems a strong security architecture can help solve.

Conclusion

All of the trade-offs discussed are challenging to address and intentionally presented without solutions. The key takeaway is that *what* is built is not as important as *how* it is built. Each system and product will have a unique combination of patient population, use environment, and therapy objective that comprise the risks and benefits. What is important is that all of these trade-offs are made intentionally with security being an equal stakeholder in the decision process. This can only be done correctly if the development processes used by the device manufacturer incorporates security as a fundamental design input. A secure development process is one that can identify and balance security needs with all the other system needs.

And the patient benefit? A trusted system that delivers the right care.

Declaration of Conflicting Interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: The author is employed by Cigital, Inc, one of the largest application security consulting firms.

Funding

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