RISKS AND REAL-WORLD SOLUTIONS FOR CONNECTED MEDICAL DEVICES

In this article, Tom Oakley, Director of Drug Delivery Device Development at Springboard, discusses the risks surrounding the use of connected drug delivery devices – and the real-world solutions that have either been proved or are being trialled.

Modern medical devices, including drug delivery devices, are being connected to other devices and the internet at an increasing rate. Every organisation we have talked with that is developing drug delivery devices either has a connected device strategy in place or is forming one. An example application is a glucose sensor (perhaps integrated into a smart watch) which communicates with an insulin pump or injector pen to set or advise the correct dose (Figure 1).

It may become normal for high-value chronic diseases to have some sort of connected support story around them. This is already the case for some people living with diabetes, multiple sclerosis or growth hormone deficiency. For examples, see the Medtronic Minimed 670G (Figure 2) or Merck Serono's RebiSmart and easypod (Figure 3).

The potential benefits of connected drug delivery devices have been discussed a great deal in conference presentations and literature, and are summarised in Table 1.

We have all heard about the terrible adherence rates that beset much of the pharmaceutical industry – approximately 50% of all medicines are not taken as prescribed.[1] One of the most common justifications for developing connected drug delivery devices is that it will solve the problem of poor adherence, so let us look at this in more detail.

CAN CONNECTED DEVICES REALLY SOLVE POOR ADHERENCE?

Some people tout connectivity as solving the adherence problem. However, there are issues with this view. The main issue is that the people who are not adherent to their drug regime are also likely to be not adherent to using the connectivity features of their device. Those people would only be helped by connected devices which are completely automatic. For example, to be completely automatic, there must be:

- No installing apps on phones or computers
- No Bluetooth pairing
- No connecting to Wi-Fi
- No logging in or set-up
- Certainly, no entering data
- Ideally, no charging of batteries.

> "People who are not adherent to their drug regime are also likely to be not adherent to using the connectivity features in their app."

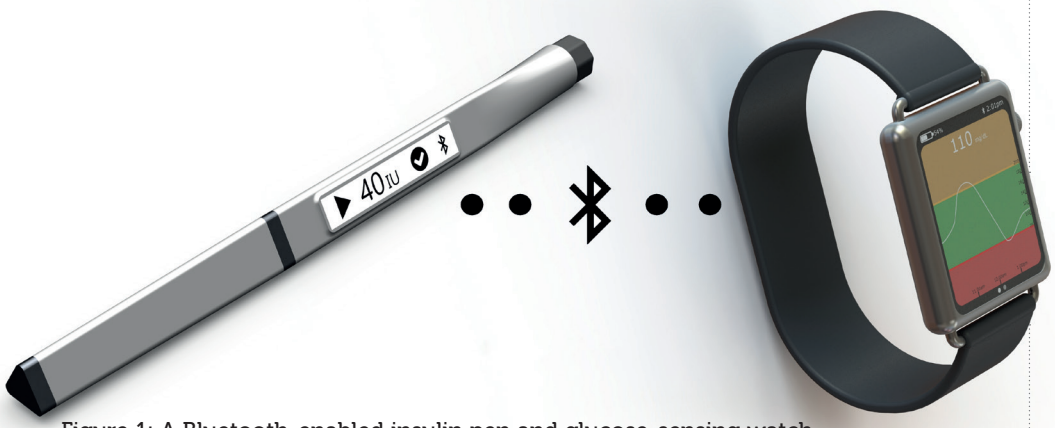

Figure 1: A Bluetooth-enabled insulin pen and glucose-sensing watch.

Tom Oakley
Director of Drug Delivery Device Development
T: +44 1223 607450
E: tom.oakley@springboard.pro

Springboard
St John's Innovation Centre
Cowley Road
Cambridge
CB4 0WS
United Kingdom

www.springboard.pro

Figure 2: The Medtronic Minimed 670G.

Figure 3: Merck Serono's RebiSmart and easypod.

If we look at fitness apps on smartphones, many of the popular apps have retention of only around 55% and that is after only one week.[2] We should not expect to increase adherence to medicines by using technologies which have lower adherence than medicines!

The best way in which connected devices can help with adherence is to understand who is non-adherent. Healthcare resources can then be directed to helping those people become adherent. I think that is where the true value of connectivity lies in addressing the adherence problem.

USABILITY RISKS

Usability (human factors) is already a major part of the device development process, and the regulatory bodies rightly expect it to be. Connectivity brings additional considerations. For example, there are:

1. Risks associated with additional user steps such as identification, connecting and recharging.
2. Risks with how we indicate status to the user. For example, does a flashing light mean "ready to use", or "low battery"?
3. Risk of disengagement as mentioned above.

The solutions are to:

1. Keep the requirements simple so that the solution can be kept simple.
2. Develop and communicate clear benefits to the stakeholders so that they are motivated to engage with (or at least not to frustrate) the functions around connectivity.

Patient	Carer	Carer
• Reminders • Training • Evidence for incentives • Hawthorne effect • Peer support	• Reminders • Training	• (Non)adherence data • Reduced costs
Healthcare professional	**Healthcare provider or regulatory authority**	**Pharmaceutical company**
• (Non)adherence data • Additional support for the least adherent • Adverse events	• (Non)adherence data • Adverse events • Clinical trial data (pre- and post-market) • Population trends	• (Non)adherence data • Adverse events • Clinical trial data (pre- and post-market) • Evidence for reimbursement • Market understanding • Product and training improvements • Increased sales by increased adherence

Table 1: Potential benefits of connected drug delivery devices for stakeholders.

3. Perform usability studies on diverse groups of people at each stage of the project. Diversity means across ages, genders, languages, cultures, technology skills and those with comorbidities and issues such as visual impairment.

RISK OF PUTTING CRITICAL FUNCTIONALITY INTO ELECTRONICS AND CONNECTIVITY

Electronics and connectivity are complex and therefore have more opportunities to fail compared with more traditional mechanical devices. There have been several drug delivery devices where recalls were issued due to failures in the electronics, which could have been avoided with a different device strategy. Examples of risk management strategies include:

1. Using a separate add-on to provide the connectivity so that the core critical functionality is not affected.
2. Build the connectivity into the device, but in a way that the critical device functions do not depend on it. Therefore, the connectivity functions could fail but the patient still receives their dose safely.

RISKS WITH SECURITY OF SUPPLY

The current COVID-19 pandemic has underlined the importance of security of supply. The electronics required by connectivity mean that supply chains can be more complex and less transparent than those for mechanical components (such as plastic injection mouldings and their raw materials).

For example, at a company that I used to work for, a colleague had designed a printed circuit board with a given memory chip. During component selection, he had selected a component which had two independent manufacturers. Following an earthquake in Japan, the first supplier was unable to supply for a few months. My colleague contacted the second supplier and they were also unable to supply. Both suppliers purchased the silicon wafer from a mutual second-tier supplier that had gone offline due to the earthquake. In electronics there is a need to be more vigilant against such "diamond" supply chains.

Another risk is that the production lifetime of components in the electronics industry is very short compared with the lifetime of medical devices. It is not uncommon for an electronic component to "go end of life" whilst the medical device is still being developed. The main strategies for mitigating the end-of-life risk are:

1. Engage with suppliers that understand and support the long timescales associated with medical devices so that they can:
   a. Guarantee minimum supply lifetimes
   b. Support engineering change processes
   c. Support any reverification or revalidation that is required.
2. Conduct full supply chain audits
3. Ensure supply chain diversity (such as dual sourcing) and disaster planning
4. Buy and store enough stock to allow enough time to change if necessary.

RISKS WITH CYBERSECURITY

Connectivity, either to the internet or to other devices, brings with it the risks of hacking and malware. We have already seen exploits in the public such as:

- Demonstration of hacking of pacemakers[2]
- Demonstration of hacking of insulin pumps[3,4]
- Hospital infusion systems with a security vulnerability allowing remote control[5]
- Insulin pump hacking over the air[6]
- Recall of insulin pumps due to cybersecurity risks[7].

The regulatory authorities are developing guidance and requirements in the cybersecurity space, such as:

- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (draft 2018)
- Postmarket Management of Cybersecurity in Medical Devices (final 2016)
- Cybersecurity for Networked Medical Devices Containing Off-The-Shelf Software (2005).

The main strategies to mitigate cybersecurity risks are to:

1. Minimise the "attack surface" of the device and the infrastructure supporting

it. For example, the device should have as few vectors as possible through which an attacker could infiltrate the system.
2. Minimise the amount of data collected and transferred.
3. Use good practice such as encryption for storage and transmission of data.
4. Use internal and external "red teams" which are dedicated to testing the effectiveness of a security programme by emulating the tools and techniques of likely attackers in the most realistic way possible.
5. Keep up to date with, and ideally contribute to, international standards, regulatory working groups and industry groups on the subject.

RISK OF DATA SILOS

Multiple organisations are developing diverse devices, server software and data models to create the connected ecosystem, and they will introduce barriers to the outside world to ensure security as described above. An obvious disadvantage of this is that data will be locked away in "silos" so that:

- Devices will not communicate with each other properly
- Devices will not communicate with other organisations' server infrastructure or web portals, etc
- Stakeholders will need to use and maintain multiple systems to manage their conditions.

We must make a concerted industry-wide effort to ensure interoperability. To this end, there are guidance documents and standards on interoperability, such as:

- FDA Medical Device Interoperability strategy[8] and guidance[9]
- UL 2800-1 Standard for Medical Device Interoperability[10]
- Health Level Seven International standards.

However, some stakeholders have decided that the industry is taking too long to provide interoperable devices and are taking matters into their own hands. For example, some people with diabetes and their family members have started the #WeAreNotWaiting movement where they are connecting various devices such as insulin pumps and continuous glucose monitors on their own without regulatory approval.

RISK OF REGULATORY CHANGE

Regulatory authorities are adapting to the rapid pace of development and working on their requirements. The subject is too large to cover in detail here, but the main areas of change are:

- Interoperability
- Cybersecurity
- Data protection
- How to regulate medical devices which are based on non-medical platforms such as consumer smartphone operating systems.

RISK OF ENVIRONMENTAL IMPACT

Like almost everything in life, we should look at the benefits versus the risks and harm caused. Products such as ventilators typically have a lot of electronic components and they are not very easy to reuse or recycle. However, if we are going to use electronics for anything, I would suggest that the sustenance of human life is the best use. We should put our efforts into first removing electronics from musical birthday cards rather than from medical devices.

Nevertheless, we should do what we can to minimise the environmental damage caused by our actions. Sensible guidelines include:

1. Add electronics only where necessary
2. Create long-lasting devices. These could either be devices with a long use life or reusable devices
3. Implement return-to-manufacturer schemes as GSK has done for its inhalers
4. Design products for ease of disassembly to help with recycling processes.

RISK OF BUSINESS MODEL

The drug delivery industry is different from others, such as consumer products or automotive because in those other industries:

- An individual person chooses the product
- The individual pays for it
- The individual gets the benefit.

On the other hand, in drug delivery:

- The healthcare professionals play a big part in choosing the drug and devices
- The payer is often an insurance company or national healthcare system
- The patient gets the primary benefit.

Therefore, the business models to support connected drug delivery devices are different from those in consumer industries. In some cases, the pharma company is paying for the connectivity and infrastructure so that they can protect their market share of drug sales. In others, we have seen new business models, such as:

- Development of predictive algorithms that can identify patients at risk of adverse events before they occur. This can save large costs in the healthcare system. An example is the collaboration between Amgen and Humana which analyses real-world evidence from Humana's members with data from wearable devices, apps and smart drug delivery devices.
- A Fitbit-based rewards programme where patients can earn US$1,500 (£1,200) per annum, by UnitedHealthcare and Qualcomm.
- Deployment of a connected ecosystem to provide the full patient portal which protects sales of drugs in competitive environments. An example is Merck Serono's web-based software platform, MSDialog for people with multiple sclerosis.

We are seeing many different business models being developed and tested so it will be some time before leading business models emerge.

SUMMARY

We have discussed some of the main risks around deploying connected drug delivery devices, including:

- Expecting connectivity to solve adherence alone
- Usability
- Critical functions
- Cybersecurity
- Data silos
- Regulatory change
- Environmental impact
- Business models.

For each set of risks, there are real-world solutions that have either been proved or are being trialled. Connected drug delivery

devices are here already; they are here to stay and they are likely to become more common. By managing the risks well, we can bring distinct benefits to the various stakeholders.

ABOUT THE COMPANY

Springboard specialises in developing devices from concept to manufacture for regulated markets. It is expert at creating innovative yet robust designs and solving difficult technical problems quickly. Springboard does not have internal projects so it is as fast and cost effective as possible, and the intellectual property belongs to its clients.

REFERENCES

1. *McCarthy, R, "The price you pay for the drug not taken". Bus Health, 1998, Vol 16 (10), pp 27–28, 30, 32–33.*
2. *"US Smartphone Health App Usage". SurveyMonkey Intelligence, July 2016.*
3. *Halperin D et al, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses". IEEE Symposium on Security and Privacy, 2008.*
4. *"Insulin pump hack delivers fatal dosage over the air". The Register, October 27, 2011.*
5. *"Medtronic Insulin Pump Security". Blog, Medtronic, August 9, 2011.*
6. *"FDA warns of security flaw in Hospira infusion pumps". Reuters, 31 July, 2015.*
7. *"J&J warns diabetic patients: Insulin pump vulnerable to hacking". Reuters, October 4, 2016.*
8. *"Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks". US FDA, June 27, 2019.*
9. *"Medical Device Interoperability". US FDA, September 27, 2018.*
10. *"Design Considerations and Pre-market Submission Recommendations for Interoperable Medical Devices". US FDA, September 6, 2017.*

ABOUT THE AUTHOR

Tom Oakley leads engineering and scientific teams developing new injection devices, pumps and inhalers. He has been the named inventor on dozens of patents throughout his 20 years' experience in industry. Mr Oakley is a regular speaker at various international conferences on innovation and medical device development, and mentors engineering and MBA students on innovation and device development at the Cambridge University Engineering Department and the Judge Business School. He read Engineering at Cambridge University before becoming the Choate Fellow in Human Physiology and Pathology at Harvard University.