OVERCOMING HAZARDS IN CONNECTED HEALTHCARE

The future of healthcare is very much up in the cloud, with more and more medical devices integrating with the Internet of Things. We spoke to industry experts about the challenges that medical device manufacturers now face and the ways that they can overcome them.

Medical professionals have a whole new world of data right at their fingertips, while patients can be monitored from home, potentially making routine check-ups a thing of the past.

This is changing healthcare as we know it, but it also exposes the people who use connected devices to hazards that did not exist before.

Manufacturers must take these risks very seriously. A design flaw can be the difference between life and death.

WHY CONNECT MEDICAL DEVICES TO THE INTERNET?

Whether wearable or stationary, connected medical devices allow medical professionals to access and analyse **vast amounts of data** in order to improve future healthcare.

WHAT IS A MEDICAL DEVICE?

A medical device is designed to be used specifically for **diagnostic** and/or **therapeutic** purposes.

Medical devices can be **wearable, implantable, stationary** and even exist as **standalone software.**

Connected devices allow medical professionals to **monitor more of their patients remotely**.

Hospital readmissions have dropped by 64% for patients who have their blood pressure and oxygen saturation levels monitored remotely, according to some estimates.

THE SHARING OF DATA

Modern medical professionals have **instant access to more data** than ever before.

1 User
2 Services
3 Networks

The data stored on a medical device can be shared through **these three levels**.

Each additional level of connectivity increases the chance of the data becoming **unlawfully accessed** or **corrupted**.

TYPES OF CONNECTED DEVICES

Insulin pump – Dosage instructions can be entered into the device remotely and insulin is injected into the body directly.

Asthma inhaler – A small sensor attached to the inhaler wirelessly syncs usage data to the user's smartphone.

Pacemaker – Data is downloaded and automatically assessed by a remote monitor, before it is uploaded to a central server.

Glucose monitor – Provides painless blood sugar monitoring for diabetics. Results are shown on an LCD display and smartphone app.

Infusion pump – 'Smart pumps' read barcodes on IV bags and patient wrist bands to deliver controlled amounts of medications or fluids.

Blood pressure monitor – Bluetooth technology allows users to monitor their blood pressure at any time on their smart phone.

THE FUTURE OF HEALTHCARE

Better patient care – Medical professionals say that new technology increases their knowledge of their patients' conditions and access to data can improve care and device performance in the long-term.

Patients can stay at home – Remote monitoring reduces hospital visits, saves costs and reduces the risk of a patient being misdiagnosed through doctor-induced stress.

Improved insights – Big data analysis can help anticipate seasonal developments and future outbreaks.

Quicker response time – Devices trigger an emergency alert if the health of a remotely-monitored patient drops to a dangerous level.

Instant results – Data can be offered in real-time by simply downloading or uploading it straight from a device.

Automatic supply control – Supplies can be monitored and replenished without human intervention.

EXTRA FUNCTIONALITY BRINGS EXTRA RISK

As with all product design, the combination of **new technology** and added **complexity** brings a **greater risk** for both device manufacturers and users.

It is vital that manufacturers take **full responsibility** for the quality of their products and not only when this is driven by legal requirements.

The hazards that come from connecting medical devices to the internet fall into three categories:

DEVICE SECURITY
SOFTWARE SAFETY
DATA PRIVACY

DEVICE SECURITY

There could be fatal consequences if a hacker with fraudulent or malicious motivations succeeds in attacking a device such as a pacemaker or an insulin pump.

MACHINES THAT CAN KILL

Jerome Radcliffe, a security researcher suffering from diabetes, showed it was possible to **hack his own insulin pump** within a 200 ft radius to deliver a lethal overdose in 2011.

The FDA in the US warned hospitals to disconnect an infusion pump made by Hospira, Inc. after discovering cyber-security vulnerabilities:

"An unauthorised user [could] control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies."

CYBER EXTORTION

An increase in "injury and possible deaths" from cyber attacks was forecasted by Europol in 2014.

However, industry expert Dr. Royth von Hahn says it is more likely that a hacker would attack a medical device to **extort the user** than to simply cause harm.

Tech companies such as **Feedly, MailChimp** and **Meetup** have all been targeted by cyber extortionists

Hackers blocked access to the websites and demanded payment to lift the restrictions.

A small medical practice in Chicago had its server attacked in July 2012.

The hackers encrypted medical records and emails and demanded a ransom to decrypt them.

SOFTWARE SAFETY

Systematic failure is a hazard for any kind of software. What seems like a small mistake in a line of code can sometimes be the **difference between life and death.**

ACCIDENT PRONE

The **more complex** a piece of technology is, the **harder it is to prevent failure** from occurring.

Manufacturers of connected devices can either use **commercially available software** – which can be vulnerable to viruses and worms – or build **new software** from scratch.

SYSTEM FAILURE

All software is as **prone to error** as the **person** who wrote the code that strings it together.

An error in radiation therapy software overexposed 28 patients in Panama to radiation, resulting in **five fatalities** in 2000-2001.

BEWARE OF THE BUGS

Bugs in new software

Medical devices that rely on new software may be prone to bugs as less is known about the quality of the software. Without thorough testing, bugs can remain undetected even after the launch of a product.

Bugs in existing software

Using older, proven software is often assumed to avoid some of the problems of building new software.

This approach can still result in disaster; an Ariane 5 rocket self-destructed less than one minute after take-off when software used on a previous rocket tried to convert a 64-bit value to 16-bit.

DATA PRIVACY

The digitisation of medical data has made it **easier to illegally access confidential information**, meaning that device manufacturers, hospitals and clinics must take care to protect the privacy of their users.

THE PRICE OF DATA

Medical data can be worth **10 times** as much as a credit card number, making hospitals, insurance providers and universities a frequent target for hackers.

If stolen, this information can be **sold on the black market** to identity thieves.

FOR SALE
Patient data can include:
- Names
- Addresses
- Birthdates
- Telephone numbers
- Social security numbers

Medical identity theft costs the US **billions of dollars** each year according to the National Institute of Standards and Technology.

The proliferation of connected medical devices vastly increases the number of potential attack vectors on the network.

Hackers may try to gain control of a medical device – often infecting it with malware – as a way of **penetrating the network** that it is connected to.

FAMOUS DATA BREACHES

4.5 MILLION

4.5 million patients had their private data accessed in at least two cyber-attacks on Tennessee's Community Health Systems in 2014.

The system was hacked through a test server that was never intended to be connected to the internet and was therefore missing key security features.

4.5 MILLION

Another 4.5 million people connected to the UCLA's network – including staff and patients – had their records exposed in late 2014.

UCLA said it was under "near-constant attack" by hackers and blocked millions of attempts each year.

PREVENTING DISASTER

Manufacturers must overcome many challenges to make medical device connectivity a safe and viable reality.

This can be achieved by first **identifying potential safety and security threats**, and then defining counter measures to prevent them from becoming a problem.

Finally, manufacturers must establish proper processes for **testing, certification** and **maintenance**.

DECODING THE REGULATIONS

- Medical device manufacturers are regulated by the Medical Device Directive in Europe and the Food and Drug Administration (FDA) in the US.
- Data privacy and security aspects are addressed in specific standards such as IEC 60601-1 and IEC 62304, which are harmonised in both the US and EU.

The FDA provides non-mandatory guidances for manufacturers of medical devices in the US:

Manufacturers should develop a set of cybersecurity controls.

Ongoing maintenance should be conducted by manufacturers throughout the product life cycle.

TESTING, TESTING…

It is crucial that manufacturers carry out a **rigorous testing** and **risk assessment** process before launching a product.

Manufacturers are recommended to engage a **third-party expert for independent testing** to ensure the safety of their medical devices.

Functional safety testing assessment, in particular, provides confidence that the safety-related systems in the device will reduce the severity and probability of harm in the event of a malfunction.

ANTICIPATING PROBLEMS

Timely software patches can reduce the risk of developing a problem associated with a cyber-security vulnerability and correct newly discovered flaws.

However, software patches to third party software – such as the operating system on which a device runs – can create new vulnerabilities that can be difficult to control.

In the event of a breach, medical data which is identifiable must be rendered unusable through **encryption** or **segregation**, according to the Health Insurance Portability and Accountability Act (HIPAA).

IS CONNECTIVITY THE FUTURE OF HEALTHCARE?

Medical device connectivity shows no sign of slowing down and promises to have huge potential to **revolutionise the healthcare industry**.

Medical device standards are starting to catch up with technology, but do not yet comprehensively cover the potential security issues of connected healthcare.

It is vital that manufacturers **protect their patients** from any device vulnerabilities in order to make the future of healthcare a connected one.

REFERENCES

bbc.co.uk/news/technology-29737540
cbsnews.com/news/black-hat-hacker-can-remotely-attack-insulin-pumps-and-kill-people
cisco.com/c/en/us/products/collateral/wireless/aironet-1200-series/prod_case_study0900aecd80609954.html
computerworld.com/article/2897622/premera-blue-cross-says-data-breach-may-affect-11m-customers.html
computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-createbackdoors-in-hospital-networks.html
computing.co.uk/ctg/opinion/2390029/security-threats-of-connected-medical-devices
fastcompany.com/3000470/medical-cybercrime-next-frontier
fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf
fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm
ft.com/cms/s/0/4f90671c-55e9-11e3-b6e7-00144feabdc0.html
hhnmag.com/Daily/2015/June/internet-of-things-health-care-glaser
ibm.com/cz/public/pdf/The_Future_of_connected_health_devices_GBE03398USEN.pdf
ihealthlabs.com
independent.co.uk/life-style/gadgets-and-tech/news/first-online-murder-will-happen-by-end-of-year-warns-usfirm-9774955.html
informationweek.com/healthcare/security-and-privacy/what-healthcare-can-learn-from-chs-data-breach/a/d-id/1317696
insidemedicaldevices.com/2015/08/11/cybersecurity-risks-with-connected-devices
money.cnn.com/2015/07/17/technology/ucla-health-hack
nemauramedical.com
nursezone.com/nursing-news-events/devices-and-technology/Smart-Pumps-Get-Smarter_24020.aspx
popsci.com/scitech/article/2009-08/first-patient-implanted-pacemaker-communicates-wirelessly-her-doctor
reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924
reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022
safetyresearch.net/blog/articles/toyota-unintended-acceleration-and-big-bowl-%E2%80%9Cspaghetti%E2%80%9D-code
trusteemag.com/display/TRU-news-article.dhtml?dcrPath=/templatedata/HF_Common/NewsArticle/data/HHN/Daily/2015/June/internet-of-things-health-care-glaser
washingtonpost.com/news/the-switch/wp/2015/08/03/connected-medical-devices-the-interet-of-things-thatcould-kill-you
wired.com/insights/2014/06/connected-medical-devices-apps-leading-iot-revolution-vice-vesa
ww2.kqed.org/futureofyou/2015/08/03/millions-of-americans-use-medical-devices-that-are-vulnerable-tohacking

Get ready for the Internet of Things in healthcare
www.tuvsud.com/mhs
2021 © TÜV SÜD AG