An NCC Group Publication

Connected Health: Security Landscape Review

Research team:

Katharina Sommer
Katy Winterborn
Matt Lewis
Stuart Kurutac

Contents

1 Introduction

Connected health is a much bigger area than the 'security theatre' reports that are often released for connected devices.

There is scope for much more in-depth work in combination with many other bodies and groups, alongside cutting-edge research.

Modern day healthcare is a rapidly changing landscape. Computers are in widespread use where paper was once the only means of record keeping, while the demands on connectivity, information sharing and data retention are ever-increasing so as to provide various healthcare organisations with insightful data about people and their health.

From this vast amount of data, new insights can be obtained, such as improved diagnosis and optimised treatments. Many benefits can also be derived such as remote diagnosis and healthcare, taking the strain away from doctors and hospitals, and allowing for improved, prioritised healthcare.

The innovative possibilities here know no bounds, however one can quickly imagine the implications of getting connected health wrong in terms of security, particularly if that security is overlooked, or simply bolted on at the last minute.

Connected health can be rather nebulous to define. One article in the Telegraph [1] described it as being **"about linking every aspect of healthcare, ensuring professionals and individuals have access to all the information they need. This isn't just a trendy new way of looking at things. It's a necessity."**

Security concerns in connected health can differ to those in environments traditionally tested by the security community, although many of the issues are still applicable. Traditionally, penetration tests in standard environments focus heavily on remote code execution and privilege elevation in order to fully compromise a network.

While these techniques are still important and valuable in connected health, there is a slight emphasis shift. Data privacy is a concern, however loss of life is a very real possibility if connected devices are not secure, hence attacks such as denial of service, traditionally assigned a lower level of interest, become a major concern in the context of connected health.

It is standard practice to assess risks to a system using the acronym 'CIA' considering the Confidentiality, Integrity and Availability of a system and its data and assigning risk based on which is the most important. In terms of connected health all three are significant, and example concerns include:

- **Confidentiality** – patient records contain sensitive details, including personal information, such as religion as well as medical information such as diagnoses. Patients typically expect that these sensitive records are kept private
- **Integrity** - if medical test results can be tampered with, the integrity of data can be called into question. This may lead to misdiagnosis and either unnecessary treatment or missing critical treatment that could save a life
- **Availability** – medical care is a fairly visible example of a set of critical systems, where timely action can be vital for saving a life. If a piece of equipment, such as a defibrillator, is vulnerable to a Denial of Service attack that compromises its availability, then this can have serious consequences.

With the above factors in mind, connected health is a much bigger area than the 'security theatre' reports that are often released for connected devices. There is scope for much more in-depth work in combination with many other bodies and groups, alongside cutting-edge research.

Traditional penetration testing also has a role to play and should not be discounted as it may provide a useful contribution alongside more in-depth research and strategic discussions. This was highlighted in a Reuters article, exploring connected health which indicated that "privacy should be a bigger worry than the potential for hackers to manipulate devices to intentionally harm patients" and that despite the news indicating hacking medical implants is the next big thing, an equally valid concern is "boring things like an old computer virus that unintentionally shuts down global operations of remote cardiac telemetry for hundreds of thousands of patients at once" [2].

Technical issues and potential attacks are one area of interest, but another equally important concern is privacy. A report in The Independent [3] indicated that **"medical records are worth more than credit card details on the dark web because they contain personal identifying details that can be used to open bank accounts, obtain loans or acquire a passport"**, going further to state how attractive a target the NHS is due to its **"unique store of millions of medical records providing an unparalleled resource"**.

A recent case in Singapore highlighted that this is a real threat and that user data is being actively targeted [4], according to the article **"hackers targeting Singapore's largest health care institution, SingHealth, stole the personal profiles of some 1.5 million patients along with the details of prescriptions for 160,000 others.**

Included in the latter group was Singapore's prime minister, Lee Hsien Loong, who the Ministry of Health said was targeted 'specifically and repeatedly.'" Breaking into the network is one obvious method to obtain this data, however the insider threat and accidental leaks are equally valid threats to user records.

Although security research in connected health is vital, and has a lot of positive consequences, one potential hazard to bear in mind from the traditional hacking of medical devices is the unintended public backlash.

There have been reports of patients refusing potentially lifesaving devices, such as pacemakers, due to the fear of them getting hacked, when the risk is very small compared to not having the device. A report in the Financial Times [5] indicated this kind of fear is a concern in the industry; in an interview it was described as follows: **"the worst consequence of a vulnerability disclosure... could be a public panic. There is a risk that someone might decide not to have a pacemaker implanted because of something they have heard in the media, which did not perhaps provide the sufficient benefits versus the risks"**. In terms of real world consequences, in the United States **"in 2013, former US vice president Dick Cheney revealed that his doctor had ordered that the Wi-Fi functionality of his cardiac pacemaker be disabled owing to fears it might be hacked in an assassination attempt"** [6].

It is clear that research into devices such as pacemakers is useful and an important component of connected health, however the cybersecurity community has a responsibility to avoid too much 'security theatre'. Care must be taken to avoid fuelling fears for the purposes of headline grabbing conference talks. One comparable example is the current 'anti-vax' movement, which is different in that the claims made in the original paper crediting vaccinations for causing autism have been completely discredited. However, care must be taken not to create a similar effect. In the case of vaccinations parents are refusing to have their children immunized, leading to a rise in diseases that should have been eradicated.

While not fuelling ungrounded fears is a major concern, another equally valid problem is the trade-off between security and privacy and necessary speed when saving someone's life. It is easy in the security world to consider problems in isolation, without understanding the real-world consequences.

For example, recommending the use of strong passwords and encryption is typical within a cybersecurity context, however this could cause delays in a scenario where speed is critical and lives are at stake. An Infosec Institute report noted, in a discussion relating to why implantable medical devices were open to attack, that **"alternative methods like passwords would not prove time-efficient in the event of emergency, for instance, if the person with the device is unconscious"** [7]. It is important to strike an appropriate balance and to understand the complications with otherwise standard suggestions.

The approach to research in the United States, which appears to be ahead of the UK in variety and numbers of connected health devices, alongside growing legislation, has also led to an increase in adopting new technologies and innovation. Healthcare organisations are working with leading technology companies to explore emerging digital solutions. There are instances where deeper collaboration is taking place to ensure off-the-shelf products are customised in meaningful ways and not just as a best fit or using default settings. Historically, the trend in the UK has been to convert paper-based processes into digital versions without improving those processes by taking advantage of technology [8].

While connected hospitals are the most obvious area considered when thinking of connected health, a number of other potential areas of interest have come to light. These include safety devices in the mental health industry, personal health monitors, age-related devices and monitoring for babies in all stages of developments.

Taking personal responsibility for health and testing, particularly as a means to bypass long waiting times for doctor appointments, has become more prevalent in recent years, particularly with the ability to self- diagnose via the internet. Personal testing kits exist, such as the 'Medichecks Tiredness & Fatigue Blood Test' available at Boots [9]. However, this still requires a sample to be sent off and analysed, and there appears to be no guarantee of how data is used or stored; this is an area where attackers may be able to leverage a weaker third party to gain information before proceeding to bigger targets. It also highlights a severe lack of standardisation and legislation around who can perform tests and the safeguards on the data they generate.

As a final example, a scientific American paper [10] described a recent vulnerability "affecting approximately 300 medical devices, including drug infusion pumps, ventilators and external defibrillators. It warns that hard-coded passwords that normally allow service technicians to gain access to myriad machines could be used to make nefarious changes if they fall into the wrong hands" but also gave the following warning: "Medical device companies remain hesitant to market their products as being secure, because they do not want to invite attacks on their systems from hackers who like a challenge".

This latter point is a real risk, and although this should not deter companies from attempting to improve security, this is where standards and legislation may play an important role in normalising security across the industry. As the cybersecurity industry matures and grows towards practice-based security with a view towards working closely with vendors and helping produce more secure products, this may help to alleviate these concerns.

The rest of this whitepaper is split into four main sections, followed by a conclusion. Firstly, existing areas of research into connected health will be chronicled, then an exploration of technical areas that may be of interest in connected health in the immediate future. Following this is a description of current standardisation and legislation in both the United Kingdom and United States, before finally considering long-term developments that do not seem viable at the moment, but may play a big part in the future of the industry.

2 Existing Research

Generally, existing security research in the connected health industry seems to be focussed on three key areas: implantable medical devices, security of equipment and networks in hospitals and methods by which implantable devices can be defended while still remaining accessible to medical staff in an emergency.

2.1 Implantable Medical Devices

Implantable medical devices seem to be the key focus for security-related research, with a number of high-profile vulnerabilities discovered and presented at key conferences. The main devices used in the research seem to be insulin pumps and pacemakers.

While it should be noted that this is not a recent attack vector, an article from The Register in 2008 [11] described an attack on pacemakers, the main body of research into implantable medical devices. The most well-known was performed by Barnaby Jack, a researcher for McAffee and IOActive [12]. In 2011 he demonstrated an attack against a Medtronic insulin pump [13] which allowed him "to locate and seize control of any device within 300 feet, even when he didn't know the serial number." The vulnerability allowed for a number of attacks to be executed including forcing the device to "dispense its entire reservoir of insulin, which is about 300 units." In 2013 Jack was due to give a presentation at Black Hat USA on "how to kill a man at 30 feet by hacking his pacemaker", however the presentation was cancelled as sadly Barnaby Jack died a few days before his talk.

Similar attacks were disclosed in an insulin pump manufactured by Johnson & Johnson in 2016 [14] and in 2017 a number of vulnerabilities were reported by ICS-CERT in the Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump [15]. The pump was made by a UK-based company and the vulnerabilities included a classic buffer overflow and numerous cases of hard-coded credentials and passwords in a configuration file. According to the bulletin successful exploitation could lead to remote code execution. In the same year Medsec, a company that specialises in medical security, released a report into a vulnerability in St Judes pacemakers [16].

In 2018 further vulnerabilities were discovered in Medtronic products, a talk at Black Hat USA [17] demonstrated that "attackers could remotely install malicious firmware on a device used by doctors to control their patients' pacemakers" by intercepting and manipulating the firmware update process. It is also worth noting that the software in this case ran on Windows XP. At Defcon in the same year a different talk discussed an attack due to a lack of authentication "in the RWHAT protocol, one of the networking protocols used by medical devices to monitor a patient's condition. This protocol is utilised in some of the most critical systems used in hospitals". A successful attack could be used to modify patients' vital signs.

New research reported in nature.com [18] is attempting to reduce the risk that current wireless implantable devices incur through the size of the electro-magnetic field they generate. To do this the researchers are utilising the body's own conductivity to transmit data from the implantable device to a receiver such as a smart wearable. According to the article, the reduction in the field area is 5 metres down to 0.15 metres. However, this has led to some potentially false beliefs that the data is fully secure due to the proximity requirements needed to extract data or compromise the device and that as a result, encryption could be optional.

2.2 Hospital Equipment and Networks

The second offensive area that has emerged from our literature review is around the security of hospital networks and the devices used, such as x-ray machines, that may one day be networked and may even be connected to the internet.

An Ibtimes article from 2016 [19] details an assessment by Kaspersky into hospital infrastructure. It was possible to connect to an MRI scanner from the hospital's Wi-Fi. In 2017 Trend Micro conducted a study that **"found over 100,000 records relating to medical equipment and hospital computers worldwide that are openly exposed and potentially vulnerable to attack."** [20]

In terms of vulnerabilities in the medical equipment, this does not seem to be as popular within the industry, possibly due to difficulties in access. However, one case study worth noting from the 1980's, was the Therac-25, a "computer-controlled radiation therapy machine". Between 1985 and 1987 it was the cause of a number of deaths due to a logic error which resulted in patients receiving a radiation dose over a hundred times more than they were supposed to receive. This was due to incorrect software checks, which had replaced earlier hardware safeguards that did not work correctly when the device entered an unexpected state due to rapidly switching modes. There were a number of additional errors and investigation found the code had not been independently reviewed or rigorously tested. [21]

In the above case, the issue was categorised as safety rather than security and was not used deliberately or maliciously, however it is an example of how logic errors can cause serious flaws in medical equipment that could be used by an attacker in the right circumstances.

In 2013 researchers for Cylance found a vulnerability in the Phillips 'XPER' medical information system [22] which interfaces with x-ray machines. The article did not provide specific details, but the issue was found via fuzzing as the machine had **"inherently weak remote authentication."**

More recently, researchers discovered a method whereby attackers could modify CT scan results to display tumours that were not present, compromising the integrity of scanning devices and causing significant, unnecessary upset to patients and at a significant cost if this was not swiftly discovered and treatments started [23].

2.3 Defensive Techniques

The third main area of existing research in connected health that we found from literature review was defensive in nature and seemed to be more academic than other research. This comprised techniques to prevent malicious activity, mainly in implantable medical devices, while ensuring they could be accessed quickly in the case of an emergency.

A good overview of defensive research is given in an Infosec institute article on implantable medical device security [7]. One of the main focuses of this research is into pacemakers, as security must be balanced with availability in an emergency.

Previously devices were reprogrammed with a 'wand' which had to be within a certain distance of the patient to "start up a software switch for passing on instructions", however modern devices operate wirelessly with a much greater range.

The same article makes reference to an initiative by RICE University and RSA to develop a system called 'heart to heart' which uses heartbeat as a biometric. Apparently it is possible to use an ECG as a reliable identifier as it retains the same characteristics even at different levels of exertion. It is not clear how this would be effective if the heart had stopped in the case of heart failure.

The process is described in one article [24] as "a doctor holds a device against the patient's body, and takes a direct reading of the heartbeat. The device reads the patient's heartbeat and compares it to one relayed in a wireless signal from the implant, and then confirms that the signals match. The wireless exchange of the heartbeat signal is encrypted, thwarting any attempt to hijack the communications during the exchange." A number of articles further explore this idea [25], [26] however the information all dates from 2012/2013 and does not seem to appear in any articles written more recently other than a mention of its existence.

In addition, Princeton University NJ and Purdue University have developed a prototype firewall called the 'MedMon' firewall, which uses anomaly detection to prevent attacks. This was first referenced in the infosec institute article, but further details can be found on the mddionline website [27].

3 Current Connected Health Technical Landscape

Connected health is a broad and varied topic, with many potentially interesting areas. There is a move in the general population towards taking care of personal health through connected devices, as well as a number of industries that are not currently the focus of connected health research, such as age related health care and mental health.

This section will explore the connected health technical landscape and current areas where there is scope to think about the intersection between security and healthcare, expanding upon previous research while considering new research areas.

3.1 Connected Hospitals and Medical Devices

The main area that comes to mind upon first thinking about connected health is related to hospitals and implantable medical devices. The speed with which automatic healthcare and computer-controlled devices can react compared to a human, and the accuracy that can be delivered, means this is likely the future of healthcare, as described in an article by the Infosec Institute [7]: **"Modern IMDs are entrusted with vital tasks in terms of medical care: delivering insulin or painkillers at proper rates, measuring and collecting data on the vital signs and passing it on to doctors and nurses, and direct stimulation of an organ's critical function, as the case is with pacemakers."**

One report in the Financial Times [20] claimed **"US hospitals currently average between 10 and 15 connected devices per bed".** Even the beds themselves might often implement connectivity, such as those equipped with wireless sensor networks for auto-adjustment aimed at reducing bedsores for immobile patients [28].

There is still a large amount of research possible in this field; hospitals are becoming more and more interconnected and it is likely that evermore-connected healthcare devices will become a reality in the UK as the benefits become apparent.

The obvious area to consider in this arena is internet/network-connected machines and devices, such as x-ray machines, MRI scanners and monitoring equipment for example. Equally important is the data that will be passing between locations. Digital medical records and test results will likely be uploaded with very little human intervention in the future, ensuring this data is protected, cannot be disclosed to an unintended recipient or modified, and is accessible when needed should be a part of an investigation into connected health security.

The technology used in medical devices can be incredibly complex, which makes securing such devices effectively a difficult task. According to the Infosec Institute [7] **"A pacemaker may depend on more than 80,000 lines of code to keep it going, and a magnetic-resonance imaging (MRI) scanner more than 7m lines."** It is very hard to ensure safety, never mind security, in devices as complex as this. An example case took place in the 1980s in which code "supporting one kind of radiotherapy machine caused emission of massive overdoses of radiation rays on several patients, taking the life of at least five of them." This was due to a previously undiscovered logic error [7].

Currently, tracking and remediating security issues seems to be confusing and ad-hoc at best, non-existent at worst. There is a database of medical device issues, known as MAUDE, however it is **"nearly useless from an information security standpoint since 90+% of the entries are related to user experience issues"** [10], this gives an indication of how security is not considered as its own separate issue and makes the job of securing medical systems difficult. In addition, hospitals are often in a difficult position as a standard security recommendation is patching, however **"the medical device vendors may refuse to support the device if the original configuration is changed".** In order to ensure security in these environments a standards and legislative change will likely be needed.

A level of security is possible due to legislation, as evidenced in US Department of Defence hospitals; there is a **"requirement for every device, including medical devices, attached to a military network to comply with the DIACAP (Department of Defense Information Assurance Certification and Accreditation) process, any medical device which is networked must be evaluated and certified from an information security standpoint before being used"** [10]. So such standardisation and legislation is clearly possible, just not desirable from a manufacturer's viewpoint.

Implantable medical devices are a hot topic for research, however there is a risk that too many scare stories in this area will lead to the general public avoiding using lifesaving equipment because of a fear of someone hacking the device, without an understanding of the risks involved, as mentioned in the introduction. Despite this, there is probably still value in research around the security of these devices. However, this should be done with care, the cybersecurity industry has a responsibility to ensure that research in this area is done with a view to helping the security of these devices and an understanding of the potential risks involved.

3.2 Electronic Health Records

Perhaps one overarching concern is the security and integrity of patient data, independent of how it is acquired.

A core technology to consider would be the ubiquitous EHR (Electronic Health Record), EPR (Electronic Patient Record) or EMR (Electronic Medical Record). Whilst similar in name there are differences, which are succinctly described in one article [29]. For the purposes of this document, they will be collectively referred to as EHR.

The EHR should be considered a high-priority target for attackers as each would contain an enormous amount of patient data. The adoption of the EHR is widespread but, as with any technology, different EHR vendors offer differing solutions. EHR's are complex systems that provide a significant amount of functionality, not only this but a number of different EHR platforms may be found in the same hospital. Adding to this, the fact that some platforms cannot communicate with each other may mean that some hospitals utilise additional middleware or mechanisms to transfer data between the disparate systems.

3.3 Healthcare in the Cloud

Some healthcare organisations have already been using the cloud for certain functions. One key emerging area appears to be for research purposes due to the availability offered when collaborating and the scalability to meet the need for big data analysis [30]. More recently in the UK, the NHS has released guidance to help with transitioning from on-premises solutions to cloud services [31]. Along with the UK Government "cloud-first" policy for public sector IT, released in 2003, it is likely that more and more services will be migrated to the cloud.

Migrating to cloud services has the potential to significantly reduce overheads and can provide additional incentives for IT departments of public health organisations. One of these benefits would be the removal of the need to continually maintain, patch and update the underlying infrastructures operating systems. This would arguably be the single greatest contribution to the security posture of an organisation beyond user education.

Companies such as Google, Microsoft, AWS and more are offering healthcare-specific cloud solutions that conform to various regulations to ensure that access to and storage of patient data is compliant with legal requirements. These services are advertised as secure but if there is a lack of experience or misunderstanding from the organisations that utilise these services when they are configured then there is a possibility that sensitive data could be at risk.

3.4 Personal Health Apps

Personal health apps and wearable devices are a big industry in the current market.

Devices such as the Apple watch or Fitbit collect data relating to a number of metrics, such as heart rate and activity levels throughout the day and store these on a central server. Users are generally required to provide personal details that may be sensitive upon signing up to these applications.

While big players in the market such as Apple will generally have taken security into account, there are a number of health-related applications made by smaller teams or individuals that may not have the same level of security rigour.

On a broader, public scale the NHS has announced the NHS-App as a "simple and secure way for people to access a range of NHS services on their smartphone or tablet." [32] The app will allow patients to book appointments, order repeat prescriptions, view their medical records and register as an organ donor. This shows the rapid growth of technical solutions to meet challenges in the medical industry and how connected health will affect most people within the country, regardless of whether they choose to use personal health apps.

3.5 Connected Devices in the Mental Health Care Industry

While the first thought when considering connected health are hospitals and doctors' surgeries, there are other areas of the healthcare profession which receive less attention but may have security concerns.

The mental health industry is an example of this. At a recent CENSIS conference Safehinge [33] were discussing the zero suicide alliance, an initiative to reduce suicide rates to 0%. Some of the statistics they shared indicated that a significant percentage of suicides occur in mental health facilities and so they had produced a prototype solution to detect ligatures around the door as part of the Symphony Doorset range. The prototype was effectively a concealed weighing scale that detected any type of pressure and sent an alert to the staff. This is an area of growth and involves very innovative, technical solutions, however privacy and security issues are of obvious concern in the mental health industry and areas such as this are where the cybersecurity industry can add value.

3.6 Age-Related Healthcare

Personal wearable devices are generally associated with health and fitness and lifestyle, however a related branch of devices aids with monitoring for vulnerable demographics, with the largest consideration appearing to be given to age-related healthcare.

A number of devices are available including fall monitors and cameras for elderly relatives with dementia, allowing an aging population to remain at home for longer periods of time and live independently for as long as possible. One range which fits in with a suite of products has been developed by Philips [34] and includes fall detection and connection through to medical centres in the event of an emergency.

Any vulnerabilities in devices that fall into this category, including denial of service, could have serious consequences as a failure to report a fall or other health concern which could lead to loss of life.

3.7 Telehealth

Related to, but a distinct category from age-related healthcare is telehealth, which is the ability to provide care remotely, allowing people to receive care at home by utilising technology to triage, monitor, or for general practice appointments in a more convenient way. Telehealth has the potential to reduce the burden on primary care facilities and hospitals by for example, facilitating care to vulnerable demographics that may not otherwise attend appointments at a GP's office due to travel difficulties.

Even though there are apparent benefits to telehealth, a few barriers exist in the uptake but not due to a lack of capability. According to a report conducted by the Center for Connected Medicine (CCM) [35], the main concern in the United States is the current lack of reimbursement. Similarly, an older study in the UK [36] concluded that telehealth would increase the costs of standard care by 10%. However, it was also noted that there were limitations in the study and that further work should be carried out. Contradictory to this was a more recent article [37] that states telehealth "could save the NHS billions".

Regardless of the financial outlay when telehealth mechanisms are implemented, consideration needs to be given to the increase in risk by introducing devices and applications into people's homes on untrusted devices and in untrusted networks. Ensuring sufficient physical and network restrictions are implemented to prevent any unwarranted access to remote devices that could have a negative impact on a patient or the hospital network it may communicate with will be paramount.

One concern in this area is the lack of human interaction in telehealth, as an extreme example there was a report recently on a patient who was told he was dying via a 'video-link robot' [38]. Although not specifically linked to security, this is an example of digitisation going too far. There is also a security element, if these video links could be compromised to cause unnecessary distress to patients.

3.8 Baby and Pregnancy Monitoring

An interesting and potentially sensitive topic, in a similar vein to age-related healthcare, is in the area of baby monitoring. Traditional devices, such as babycams, have been on the market for many years, however even these familiar devices are becoming more connected, with the option to view footage from the internet, which has obvious privacy-related concerns.

However, an additional type of application has been developed which allows for the tracking of child development, even down to sleep patterns and growth rate in the case of the Philips ugrow application. According to an article in the Telegraph [39] the system "uses information that is collected anyway, such as height, weight and feeding patterns, alongside data drawn from a connected baby monitor and thermometer to allow parents to track temperature, sleep pattern and the progress of the child. This data can be shared with doctors, or used to get personalised support".

Taking this a step further, according to the same article, Philips has developed an 'embryoscope', which has been called "CCTV for embryos" and "takes a live recording of the embryo and presents the results in the form of a graph that highlights any abnormal behaviour that the embryologist can then go backand analyse". This is clearly a highly sensitive area where security and privacy could be a major concern. The Ugrow system is available online [40], however there is no mention of the embryoscope outside of the Telegraph article, so this may be a future development or research may have been paused or stopped entirely at the time of writing.

3.9 Other Sensitive Areas

The same Telegraph article cited above [39] described a number of other connected health areas and devices, mostly designed by Philips that do not neatly fit the previous category, but nevertheless contain sensitive information and have serious consequences if a security flaw were exploited. These include:

- "Implants beneath the surface of the skin now allow diabetics to continuously track their glucose levels."
- "A self-adhesive wearable biosensor that can be used in hospitals to monitor patients in need of frequent observation."
- An app "AlcoChange, which helps patients with alcoholic liver disease drink within safe limits, using a breathalyser attached to their phone, and also nudges them away from places where historically they may have struggled to control their alcohol intake."
- "A range of connected health devices and programs designed especially for people who are susceptible to, for example, heart disease or diabetes."

4 Standards and Legislation in Connected Health

Although purely technical solutions are of vital importance in connected health security, enforcing secure solutions or making security a priority will be difficult without agreed standards throughout the industry and government legislation.

4.1 Standardisation Overview

In order to improve security and safety throughout any industry, standardisation, regulation and legislation is vital. Connected health does not currently have any official standards or mandated government legislation, or any generally agreed upon security approaches across the industry. There is short-term work with regards to what could be considered now in terms of standardisation; this is also likely to be a long-term issue that will require many years' work.

There are some attempts at standardisation in North America, but these do not appear to be enforced yet. A Tripwire article [41] states **"The FDA (Food and Drug Administration) has issued final guidelines for manufacturers to consider cybersecurity risks as part of their medical device design and development. Its guidance contains voluntary recommendations and does not establish any legally enforceable responsibilities".**

It is worth noting that medical devices are often made by similar manufacturers to industrial control systems, where there will be standards adhered to even if they relate to safety more than security. According to [42] Siemens, Philips, Honeywell, and GE all provide products to both industries, and vulnerabilities in medical devices appear to be reported by ICS-cert [43]. There may be a possibility of taking existing standards and expanding upon them rather than there being a necessity to start from scratch.

All media attention around the issue of connected device security has been largely scaremongering or questions of 'what-if?' However, the WannaCry infections in May 2017 demonstrated the real-world impact of a wormified ransomware on a connected health network; the outbreak impacted severely on the UK's NHS, impacting up to 70,000 devices which included computers, MRI scanners, blood-storage refrigerators and theatre equipment. Patient health was impacted from inability to administer certain treatments and needing to cancel many appointments and medical procedures while needing to deal with the incident, which is estimated to have cost the NHS £92m in remediation [44].

A further related case, outside of the medical arena took place in 2013 - **"the Federal Trade Commission (FTC) filed a complaint against TRENDnet Inc., a producer of wireless cameras that can be installed wherever people need a video feed. The wireless cameras produced by TRENDnet can send motion-captured video to computing devices, such as iPhones or laptops. The complaint stated that TRENDnet failed to provide reasonable and appropriate security for the wireless cameras, which resulted in hacking attacks. The hackers posted Internet links to compromised feeds for nearly 700 wireless cameras."** [45] Although the domain in this case was different, parallels can clearly be drawn to security and privacy failures in the medical industry.

The use and widespread adoption of standards can help assist with public confidence in connected health, by guaranteeing a base level of security has been taken into account. The absence of concrete security standards however, is unsurprising considering the lack of operational compatibility between the myriad of vendors that exist in this sector. Efforts to reduce interoperability and issues that occur because of a lack of standards is another focus in the healthcare world. There are frameworks in place from the NHS [46] and HL7 [47], most notably FHIR [48] from the latter, to help overcome a number of these problems.

4.2 Current Standards and Legislation in the United Kingdom

The situation in the UK seems to be some way behind the United States. A review of the existing regulatory and legislative standards for connected health in the UK presents a fragmented and complex landscape comprising multiple standards and requirements, split responsibilities for compliance and enforcement and a seemingly limited whole-system approach that comprehensively covers all elements of connected health or digital healthcare.

There has been much focus on the secure storage of patient data, but less emphasis on developing regulations for medical devices that blend safety, security and resilience, or provide specific requirements for IoT components in hospitals.

From a standardisation perspective, a 2015/16 report [49] on the 'Smart Hospital' by the European Network and Information Security Agency (ENISA) breaks down the elements of connected health as 'smart hospital assets'. A slightly simplified version of this for the UK ecosystem includes:

1. NHS trusts and healthcare providers, and the systems, processes and equipment they use including digital patient records, MRI and radiotherapy equipment and wider IT infrastructure.
2. Individual patients' health and care management technologies, including medical devices such as insulin pumps and pacemakers and wearable devices such as fitness trackers and blood pressure cuffs.

The current situation in the UK should be viewed in the context of future ambitions for the country's health service, as set out in the current Health Secretary's tech vision [50], and the NHS Long-Term Plan [51] which set out:

- Large-scale digital upgrades including digital access to NHS services, a seamless digital journey through single and secure NHS sign-on; embracing digital tools such as mobile monitoring devices, the use of connected home technologies, and frictionless APIs; and digital patient records becoming the norm.
- Plans to set national, mandated open standards for data, interoperability, privacy and confidentiality, real-time data access, and cybersecurity and access rules, moving to prioritising compliance at the point of procurement so that innovators and commissioners have clear rules to adhere to when selling and buying products.

A new organisation to lead this work, NHSX [52], will work with the NHS and the wider digital economy to build world-class digital services, using experts in technology, digital, data and cybersecurity to deliver the Health Secretary's tech vision and the Long-Term Plan for the NHS, including through setting national strategy and mandating cybersecurity standards so that NHS and social care systems have security design in from the start.

Going forward, there are a number of different regimes and standards that apply depending on category.

For NHS trusts and healthcare providers:

- NHS organisations will be required to complete the Data Security Protection Toolkit (DSPT) [53] by 31 March 2019 which acts as the national assurance framework for data security and protection in health and care. The DSPT is a self-assessment tool to help organisations audit their own systems against the National Data Guardian's 10 data security standards, and also incorporates the provisions and requirements of the Network and Information Security (NIS) Regulations 2018 and the Data Protection Act 2018.
- The DSPT framework covers the secure handling, storage and transmission of data, access management, and avoidance of unsupported systems across the estate, incident reporting and accountability, annual security training, and continuity planning and testing.
- From April 2019, minimum cybersecurity standards will be fully incorporated into the DSPT; by summer 2021, there will be 100% compliance with mandated cybersecurity standards across all NHS organisations (the Will Smart review post-WannaCry also recommended that all organisations move to comply with the Cyber Essentials Plus standard by June 2021).

For individual patients' health and care management technologies:

- The safety and quality of medical devices in the UK is regulated and assured by the MHRA.
- The (about to be overhauled) 2017 Interim Cybersecurity Science and Technology Strategy [51] finds that **"there is a mature legislative and regulatory framework for medical devices"** but warns that **"the extent to which connected medical devices and other emerging technologies fit into this framework is a developing issue"**.
- A 2017 update to the Medical Device Regulations 2002, covering general and active implantable medical devices and in-vitro diagnostics medical devices requires that software is developed and manufactured according to state-of-the-art lifecycle processes, including information security measures protecting against unauthorised access [54].
- It is said that the current regulatory framework for medical devices aims to ensure safety but has failed fully to consider the possible impact of poor cybersecurity on patient safety or privacy. In addition, while software for medical purposes is explicitly included in medical device regulation, critical components of information and communication infrastructure are not usually covered.
- Further to the EU-derived medical device rules, there are a range of international ISO and EIC standards covering medical device software e.g. BS EN ISO 62304.
- In addition, device manufacturers, predominantly in the US (though they are internationally operating) have developed their own approaches to cybersecurity. For example, Philips Healthcare has committed to the deployment of comprehensive security plans that assure the safety of medical devices, business enterprise information and personal data; Abbott has established a cybersecurity multifunctional group to ensure cybersecurity is part of its design process; and Draeger has a dedicated product security team that considers cybersecurity throughout every stage of its product development cycle.
- For wearable devices, such as health trackers, for example, the consumer IoT Secure by Design Code of Conduct is relevant. While IoT products in scope are primarily intended to be employed in manufacturing, with those in healthcare not necessarily in scope, wearable health devices are mentioned as one type of product to which the Code should apply.

In addition, the NHS Long-Term Plan makes the case for embracing digital tools so that e.g. people with long-term conditions are supported through mobile monitoring devices such as digital scales or blood pressure cuffs and the use of connected home technologies.

4.3 Current Standards in the United States

In recent years the FDA appears to be taking the security of medical devices much more seriously and assigning it a much higher priority and, according to [5], **"spoke at Defcon for the first time this year. The regulator has issued guidelines to push device makers to take security seriously, and it is encouraging them to work with the "white hat" hackers".**

An interesting paper [55] considered some guidelines for medical device security. Two useful takeaways are the properties recommended that medical device software must satisfy, these include **"safety, security, reliability, resilience, and robustness among others."** Alongside this a list of FDA recommendations that manufacturers of medical devices should provide:

- A specific list of all cybersecurity risks that were considered in the design of a device;
- A specific list and justification for all cybersecurity controls that were established for a device;
- A traceability matrix that links actual cybersecurity controls to the cybersecurity risks that were considered;
- The systematic plan for providing validated updates and patches to operating systems or medical device software, as needed, to provide up to-date protection and to address the product lifecycle;
- Appropriate documentation to demonstrate that the device will be provided to purchasers and users free of malware
- Device instructions for use and product specifications related to recommended anti-virus software and/or firewall use appropriate for the environment of use, even when it is anticipated that users may use their own virus protection software

Another consideration should be from a global perspective. Medical device manufacturers need to certify their products through various regulations if they want to have a presence in different geographical locations, which is often an expensive process especially considering any changes to the device means certification may need to be re-evaluated.

A single globally approved process would simplify and potentially improve the overall standard of devices. If manufacturers only need to adhere to one standard that incorporates safety and cybersecurity, then this could save money and potentially encourage a proactive approach rather than meeting baseline requirements of multiple regulatory bodies. Enabling the healthcare industry to meet agreed objectives by simplifying the method to reach those objectives could start with a single security standard.

5 Future Considerations

There are a number of areas that are likely to be of interest in the future of connected health, yet do not seem viable at the moment. These include AI, use of robot doctors and ambient computing.

5.1 The Role of Artificial Intelligence (AI)

Speculating on the future of the healthcare industry as a whole, one area that seems to be mentioned frequently is AI and machine doctors that can, among other things, perform diagnoses.

While this does not appear to be an immediate development and for the foreseeable future human doctors will be the main point of contact, it does seem that this may one day become a reality.

The security requirements of AI and machine learning is broadly not well understood, in particular how can any level of assurance around purity of training data and the training process be demonstrated? When there is a possibility that the data may become tainted (as occurred in the case of Microsoft's chat bot [56]), extremely unintended consequences can occur, in the Microsoft example, the chat bot 'learned' strong prejudices and alarming viewpoints, leading it to be pulled from public interaction.

Research is also ongoing into robot-assisted surgery [57]. There are obvious advantages to automated systems in this space – better processing, possibly improved accuracy during surgery and thus reduced risk of error. However, when robotics and AI go wrong, there tends to be extreme consequences due to the cyber-physical aspect. We are already seeing these issues and concerns presenting themselves in the world of autonomous vehicles [58].

5.2 Ambient Computing

Following on from AI is the concept of Ambient Computing. This is essentially utilising technology in a way that is more natural by responding to the environment around it. For example, using voice recognition and processing in conjunction with AI to complete various jobs without requiring additional interaction from the end user. This can simply be for an improved patient experience or to potentially revolutionise tasks that currently involve a significant amount of manual data input.

Virtual assistants such as Alexa, Google Assistant and Siri have allowed many users to control a number of smart devices in their homes for a while. Such usages are appearing in the medical world for example, a program currently being piloted by Cedars-Sinai hospital [59] allows patients to interact with nurses and control entertainment systems in their room hands free. This solution uses Aiva, which is built with Amazon's Alexa for Business.

At the HIMMS18 conference, Eric Schmidt, former CEO of Google, presented an idea for ambient computing called "Dr Liz". An article reporting on the prevalence of AI at HIMSS18 quoted the presentation of "Dr Liz" stating, "This system listens to the conversation, disambiguates the voices, follows the consultation, and gives suggestions to the clinician in his or her earpiece. It transcribes the situation so everyone has a record of the complete conversation, and then it fills out and navigates the EHR." [60].

Although companies like Amazon and Google might seem like the obvious pioneers for integration of voice assistants in medical facilities, there is already, at least one, well-established company in this space. Nuance recently announced their ambient computing solution [61], stating that it will drastically reduce administrative burden on medical staff and therefore contribute to the reduction of physician burnout. Physicians tire due to a number of factors including the increasing demand on administrative tasks and this is a very real problem. According to one study, medical staff are spending more than half their working day inputting data into EHR systems [62]. If solutions such as this can deliver on these promises, then the uptake would likely be significant.

There are a number of privacy concerns surrounding digital assistants currently [63], [64]; this is especially true given the security of patient data is a primary concern and mimics privacy concerns about the use of such digital assistant devices in the home. This is an area that is likely to come under the spotlight in future debates around the use of digital assistants.

6 Conclusion

Connected health is a vast and varied domain with many potential avenues for research, and many demands for pragmatic security advice from the cybersecurity industry. It is clear that many new and innovative solutions are coming onto the market but which may not have the correct or desired focus on security.

The current industry focus appears to be on implantable medical devices such as pacemakers and insulin pumps. Academic research seems to be focused on secure ways to access such devices without impacting lifesaving work while the cybersecurity industry in general has focused on just a small subset of the medical industry.

There is much scope for teams from both industries to work together across the full range of security disciplines; from novel, cutting edge research, through to penetration testing and aiding in the development of much needed standards and legislation.

7 References & further reading

[1] www.telegraph.co.uk/wellbeing/future-health/connected-healthcare/

[2] www.reuters.com/article/us-health-heart-pacemaker-cyber/pacemakers-defibrillators-are-potentially-hackable-idUSKCN1G42TB

[3] www.independent.co.uk/voices/hackers-medicine-nhs-cyber-attack-medical-device-pacemaker-wifi-a8032251.html

[4] www.theverge.com/2018/7/20/17594578/singapore-health-data-hack-sing-health-prime-minister-lee-targeted

[5] www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691

[6] www.independent.co.uk/voices/hackers-medicine-nhs-cyber-attack-medical-device-pacemaker-wifi-a8032251.html

[7] resources.infosecinstitute.com/hcking-implantable-medical-devices/#gref

[8] www.healthcareitnews.com/news/digital-transformation-healthcare-remains-complex-and-challenging

[9] www.boots.com/health-pharmacy/electrical-health-diagnostics/dna-test-kits/medichecks-tiredness-and-fatigue-blood-test-10256015

[10] www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/#666870321f8e

[11] www.theregister.co.uk/2008/03/12/heart_monitor_hacking/

[12] en.wikipedia.org/wiki/Barnaby_Jack

[13] www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

[14] www.bbc.co.uk/news/business-37551633

[15] ics-cert.us-cert.gov/advisories/ICSMA-17-250-02A

[16] www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

[17] www.csoonline.com/article/3296633/security/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html

[18] www.nature.com/articles/s41598-018-38303-x

[19] www.ibtimes.co.uk/how-security-researcher-easily-hacked-hospital-its-medical-devices-1544002

[20] www.ft.com/content/75912040-98ad-11e7-8c5c-c8d8fa6961bb

[21] en.wikipedia.org/wiki/Therac-25

[22] www.darkreading.com/attacks-breaches/security-researchers-expose-bug-in-medical-system-used-with-x-ray-machines-other-devices/d/d-id/1138984

[23] www.computing.co.uk/ctg/news/3073636/malware-that-can-inject-fake-cancerous-nodes-into-ct-scans-created-by-security-researchers

[24] www.technologyreview.com/s/519266/encrypted-heartbeats-keep-hackers-from-medical-implants/

[25] www.livescience.com/23656-logging-in-with-your-heartbeat.html

[26] www.medicaldaily.com/keeping-hackers-out-your-body-heartbeat-password-protects-pacemakers-implanted-insulin-pumps-cyber

[27] www.mddionline.com/prototype-firewall-could-prevent-malicious-medical-device-hacking

[28] www.ncbi.nlm.nih.gov/pubmed/26929768

[29] www.masters-in-health-administration.com/faq/what-are-the-similarities-and-differences-between-an-ehr-epr-and-emr/

[30] www.level3.com/~/media/files/ebooks/en_cloud_eb_healthcare.pdf

[31] digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services

[32] digital.nhs.uk/services/nhs-app

[33] www.safehinge.com/

[34] www.lifeline.philips.com

[35] www.connectedmed.com/blog/content/top-of-mind-2019-interoperability-cybersecurity-telehealth?utm_source=pressrelease&utm_medium=media&utm_campaign=tom2019-upmc-pressrelease

[36] www.nhs.uk/news/medical-practice/are-benefits-of-telehealth-care-worth-the-cost/

[37] www.healthcareitnews.com/news/digital-health-apps-could-save-nhs-billions-says-report

[38] www.bbc.co.uk/news/world-us-canada-47510038

[39] www.telegraph.co.uk/wellbeing/future-health/connected-healthcare/

[40] www.philips.co.uk/c-m-mo/ugrow-baby-development-tracker

[41] www.tripwire.com/state-of-security/security-data-protection/medical-device-security-standards/

[42] www.darkreading.com/attacks-breaches/security-researchers-expose-bug-in-medical-system-used-with-x-ray-machines-other-devices/d/d-id/1138984

[43] ics-cert.us-cert.gov/advisories/ICSMA-17-250-02A

[44] www.digitalhealth.net/2018/10/dhsc-puts-cost-wannacry-nhs-92m/

[45] resources.infosecinstitute.com/privacy-implications-internet-things/
[46] digital.nhs.uk/services/interoperability-toolkit
[47] www.hl7.org/implement/standards/index.cfm?ref=nav
[48] www.hl7.org/implement/standards/product_brief.cfm?product_id=491
[49] www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals
[50] www.gov.uk/government/news/matt-hancock-launches-tech-vision-to-build-the-most-advanced-health-and-care-system-in-the-world
[51] assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf
[52] www.gov.uk/government/news/nhs-long-term-plan-launched
[53] www.dsptoolkit.nhs.uk/
[54] www.vde.com/en/dgbmt/working-areas/cybersecurity-requirements-medical-device-manufacturers
[55] www.csl.sri.com/users/neumann/cacm231.pdf
[56] www.technologyreview.com/s/610634/microsofts-neo-nazi-sexbot-was-a-great-lesson-for-makers-of-ai-assistants/
[57] en.wikipedia.org/wiki/Robot-assisted_surgery
[58] www.theguardian.com/technology/2018/mar/22/self-driving-car-uber-death-woman-failure-fatal-crash-arizona
[59] www.cedars-sinai.org/newsroom/cedars-sinai-taps-alexa-for-smart-hospital-room-pilot/
[60] healthitanalytics.com/features/ehr-users-want-their-time-back-and-artificial-intelligence-can-help
[61] www.nuance.com/about-us/newsroom/press-releases/2019/Nuance-Unveils-ACI.html
[62] www.annfammed.org/content/15/5/419.full
[63] www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation
[64] www.businessinsider.com/amazon-sends-alexa-shower-recordings-to-wrong-person-2018-12?r=US&IR=T