Imperial College London

Institute of Global Health Innovation

Improving Cyber Security in the NHS

Saira Ghafur
Gianluca Fontana
Guy Martin
Emilia Grass
Jonathan Goodman
Ara Darzi

Contents Page

Imperial College London
Institute of Global Health Innovation

Foreword

The last few years have seen a surge of new digital technologies being used in healthcare, and as a consequence, ever-larger quantities of data are being generated. With this digital evolution comes a wealth of opportunities to improve the health and care of patients, and to prevent, cure and manage illness. Over the past century, health system leaders have progressed toward these goals, aided by significant advances in science and technology: new vaccines, medicines and surgical techniques; technologies, such as telehealthcare, which can dramatically improve access, and analytics to better measure the costs and variations of care provision. These factors contribute to improvements in life expectancy across the globe.

However, there are also enormous risks. The NHS holds large amounts of sensitive and valuable data in vulnerable systems. Effective cyber security is not just about protecting data, it is fundamental for maintaining the safety, privacy and trust of patients. The global cyber attack, WannaCry, in 2017 compromised IT across the NHS, starkly demonstrating the vulnerability of the NHS. There is no quicker way of undermining the public's trust than by allowing essential systems to be compromised or personal data to be lost.

Imperial College London has established a new interdisciplinary collaboration for cyber security in healthcare between the Institute of Global Health Innovation (IGHI) and the Institute of Security Science and Technology (ISST). This collaboration will serve as a leading hub for translational research in cyber security for healthcare, both in the UK and globally and will aim to provide a powerful engine to support the incubation and transformation of research through academic excellence, aligned objectives, funding and resources.

This report identifies some key insights for the UK health and care sector to consider for future cyber security practices, policies and protocols; this includes increased investment, improved governance and greater accountability, which are essential to protect the NHS from future attacks.

I would like to take the opportunity to thank all those who have contributed to the production of this report, with a special thanks to our advisory board who have in-depth knowledge across academia, industry, healthcare and government.

Professor the Lord Darzi of Denham OM KBE PC FRS

Advisory Board

Imperial College London
Institute of Global Health Innovation

Professor Chris Hankin, Co-Director of the Institute for Security Science and Technology, Imperial College London
Professor Hankin's research is in theoretical computer science, cyber security and data analytics. He leads multidisciplinary projects focused on developing advanced visual analytics and providing better decision support to defend against cyber attacks for both enterprise systems and industrial control systems. He is Director of the UK's Research Institute on Trustworthy Inter-connected Cyber-physical Systems (RITICS). He is Chair of the UK's Academic Resilience and Security Community (Academic RiSC) and sits on the ministerial oversight group of the Security and Resilience Growth Partnership. He is Chair of the Association for Computing Machinery (ACM) Europe Council. He is also a member of the ACM Publications Board.

Professor Nick Jennings CB FREng, Vice-Provost (Research and Enterprise), Imperial College London
Professor Nick Jennings, CB FREng, is responsible for promoting, supporting and facilitating Imperial College London's research performance and for leading on the delivery of the Research and Enterprise Strategy. He also holds a chair in Artificial Intelligence in the Departments of Computing and Electrical and Electronic Engineering. Before joining Imperial College London, Professor Jennings was Regius Professor of Computer Science at the University of Southampton and the UK Government's Chief Scientific Advisor for National Security. Professor Jennings is an internationally-recognised authority in the areas of artificial intelligence, autonomous systems, cyber security and agent-based computing.

Rachel Dunscombe, CEO of the NHS Digital Academy and a strategic advisor for Salford Royal NHS Foundation Trust
Rachel additionally works with KLAS Research building a rigorous evidence base for success factors in the implementation of digital health and care solutions. As part of her role at Salford Group she has delivered the Global Digital Exemplar and two NHS Vanguards. She is also an Ambassador for the ECHAlliance / Digital Health Society and an ambassador for CHIME, the professional body for global healthcare CIOs. She currently holds a Visiting Professorship at Imperial College London and is a certified CHCIO - a US healthcare CIO certification.

Cal Leeming, Founder & CEO, River Oakfield
Cal Leeming is a cyber security expert and co-founder of several startups, including The Zebra and PixelMags, and recently appointed to the Healthcare Cyber security Advisory Board for Imperial College London. The story behind Cal's journey is remarkable. After a nefarious start where his natural curiosity and obsession to understand how things work led him astray, he was caught hacking at the age of 12, making him the youngest child ever to be prosecuted under the Computer Misuse Act in the UK. Now in his early 30s, Cal's ingenuity and ambition have earned him the reputation of a trusted industry icon.

1
Executive summary

Ineffective cyber security is a clear and present danger to patient safety in the UK and worldwide. As the recent WannaCry attack on the NHS showed, cyber incidents can significantly disrupt health and care systems and directly contribute to patient harm. The NHS was found to be vulnerable and not adequately prepared to respond, with limited capability and uncertain accountability for cyber security. In the future, the threat and consequences will inevitably grow due to an increased reliance on technology in healthcare, and evolution in the motivation and sophistication of malign actors.

Technology is expected to "transform" the NHS. Innovations like the increased use of artificial intelligence, cloud computing and connected devices can support more effective care. However, as healthcare relies more on technology, the risk of cyber disruption will also significantly increase, unless appropriate actions are taken. In addition, cyber attackers are becoming more sophisticated and focused on the health sector.

Key Insights

1. A culture of risk awareness and good cyber security needs to be embedded across the NHS and this needs to be effectively communicated to the public.

2. The oversight and governance of cyber security and risk needs to be streamlined and simplified.

3. An approach to developing sustainable minimum cyber security standards is needed for the design, build and procurement of medical devices.

4. Research is needed into the development of future data architectures that allow permeable boundaries of access and control to meet the specific context of healthcare; the need to widen access whilst putting in place features to restrict the ability of cyber damage to propagate.

5. The NHS Digital Data Security programme needs to be expanded and appropriately resourced to provide a single strategic cyber forum.

6. The mapping of interdepencies across the IT landscape and the consequences of shared infrastructure in the face of a cyber attack need to be better understood. There is a need to effectively model the impact of IT incidents across local, regional and national systems.

7. A mandated framework for cyber security should be further developed, tested and implemented along with operational resilience testing and assurance in the healthcare sector.

8. The infrastructure required for interconnected networks needs to be better understood to ensure the healthcare system is secure at scale.

9. Research into a better understanding of how and with what speed attacks propagate is needed order to design time-relevant responses.

10. Cyber security attacks need to be viewed as a fundamental threat to patient safety and not just an IT issue.

Imperial College London
Institute of Global Health Innovation

While WannaCry was a wide-ranging attack that happened to impact health systems including the NHS, in 2018 hackers specifically targeted the Singapore healthcare group SingHealth and stole the information of 1.5 million patients. In addition, WannaCry blocked access to NHS systems, but was very visible. The threat to patients would have been even bigger if data had been subtly manipulated, for example changing a patient's blood type in the Electronic Health Record, without being detected. This highlights that any cyber attack in healthcare is a threat to patient safety.

In examining the opportunities, threats and challenges of emerging technologies in the context of cyber security, this report aims to identify some of the actions that can and should be taken at the policy and research level now and in the near term in order to ensure they are successfully exploited.

Addressing the future threat effectively will require appropriate actions to decrease vulnerability and improve resilience in the event of an attack.

It is critical to understand and manage the underlying risk factors, by addressing unclear governance, vulnerable security architectures and modifying cultures and behaviours that lead to increased risk. It is also vital to take preventative action in order to reduce the risk of an attack being successful.

2
Introduction

Emerging technology has the potential to transform healthcare. Artificial intelligence will make it possible to accurately diagnose complex conditions with economy at scale and speed; networked devices will allow the remote monitoring and dosage of drugs; the proliferation of wearable devices will allow patients to augment their health records with "pattern of life" data; robotic surgery will replace the conventional variety for many procedures, and improved communications will drastically reduce the need for patients to travel long distances for consultations.

Given the well-reported pressure on health services, every effort should be made to harvest the benefits that technology can bring, but in order to do this it is essential that it be done not only safely, but also securely with the understanding that technology is not safe unless it is secure.

In recent years, the number and severity of cyber attacks against healthcare systems and hospitals has increased significantly, compromising the health information of millions of people. In May 2017, the WannaCry ransomware programme encrypted data and files on 230,000 computers in 150 countries and devastated the NHS.[1] Key systems were blocked, preventing staff from accessing patient data and critical services; thousands of appointments and surgeries were cancelled, necessitating, in some cases, care diversion to other hospitals.

The WannaCry attack was not, however, targeted at the NHS, though it was allegedly state-sponsored. Other major organisations were affected, including: Telefonica, FedEx, Nissan, Russian Railways, and the Bank of China. Yet the biggest impact was undoubtedly felt by the NHS. As health systems worldwide watched on, it became apparent how vulnerable healthcare is to any cyber threat.

Prior to this, there were already well-publicised and alarming examples of cyber attacks targeting healthcare organisations, such as the Anthem Insurance hack in 2015, which has cost over $100 million in settlements and much more in costs to date after 79 million records were breached, or the ransomware attack on the Hollywood Presbyterian Medical Centre in 2016 which cost $17,000 in Bitcoin payment to bring to an end, having effectively shut down the hospital for many days.[2,3] More recently, in 2018, SingHealth, the largest healthcare provider in Singapore, suffered a cyber attack which resulted in the breach of 1.5 million records.[4]

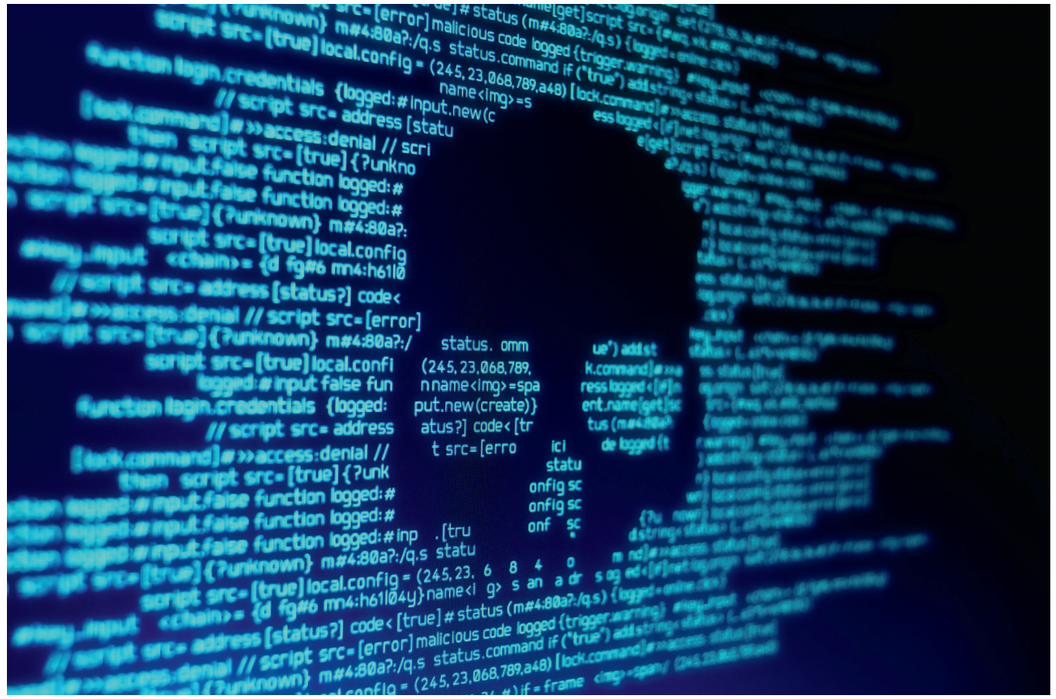
Healthcare is one of the most frequently targeted sectors by hackers, in part because security among particular institutions is variable and because private health data can be valuable on the dark web.[2,5] Given the size of the population the NHS serves, major breaches represent a significant threat.

Cyber attacks can also have a significant impact on patient safety. As modern technology has become indispensable in healthcare operations, the vulnerabilities to cyber threats are increasing exponentially. This can happen a number of ways: data can be stolen; data may be deleted or, even worse, corrupted in a way that is not obvious until years later; medical devices such as magnetic resonance imaging (MRI) scanners, computed tomography (CT) scanners, or implantable cardiac defibrillators can be hacked, causing direct harm to patients. Maintaining the security of healthcare is not only vital to ensure the safety of patients, but also to maintain their trust in those securing their health.

Notwithstanding the ongoing strategies to tackle cyber security within the NHS, the current healthcare landscape makes the attainment of a cyber secure future challenging. Healthcare networks are vulnerable as cyber security has not been prioritised as part of corporate strategy and investment. Current governance of medical technology is orientated towards clinical safety despite increased device connectivity. This complex governance structure is further complicated by the plethora of legacy infrastructure and practice throughout the healthcare sector.

3
What does cyber security entail?

Imperial College London
Institute of Global Health Innovation



The UK's National Cyber Security Centre (NCSC) defines cyber security as how individuals and organisations reduce the risk of cyber attack from malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.[6] While this definition is largely comprehensive given how cyber security is practiced today, the world of information technology has and continues to evolve. As technology changes and what counts as 'cyber' becomes broader, defining cyber security, and the growing number of terms that fall into cyber security studies, will become increasingly difficult.

The salient issue in cyber security is, however, always protection from different modes of undesirable or unpermitted access, but as more systems and devices become reliant on increasingly complex digital technologies the potential for exploitation will rise. Our goal in this section is to discuss what qualifies as a cyber security incident, and to describe the varying types of cyber security incidents currently seen across industries and their effectiveness.

A moving target

As the types of attacks launched in cyberspace have become more sophisticated, the terminology has in turn become more complex in an effort to account for the changing nature of attacks and the varieties of interfaces and networks that require protection. In healthcare, while data privacy and its associated security risks are a crucial issue that governments and members of the public focus on, medical device security is an under-appreciated issue that may become a pressing concern in the coming years.[7]

The increasing complexity of the subject does not, however, preclude the categorisation and classification of important aspects. Indeed, any discussion of cyber security 'necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualise and ultimately respond to a security threat.'[7] While offering a comprehensive definition for each aspect of cyber security may be akin to hitting a moving target given that technologies and incidents are always changing and new threats emerging, the critical notions of protection should remain constant.

Types of breaches

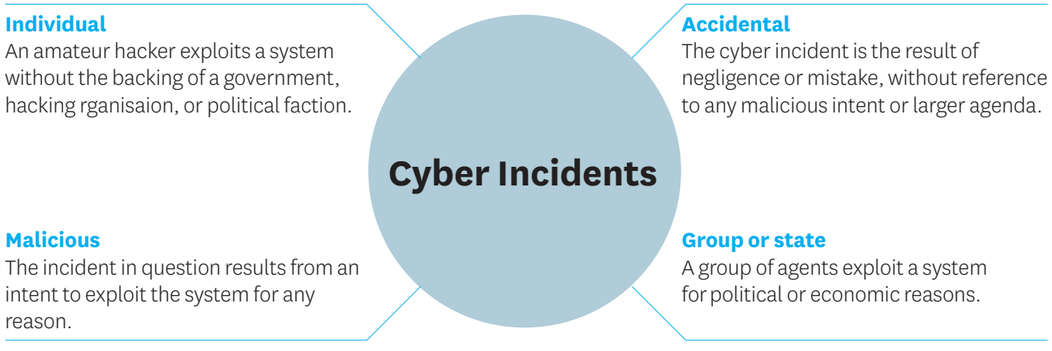
Table 1 gives common types of cyber security breaches. A group of primary distinctions should, however, be made among them, which is set out in *Figure 1*. While breaches often have identical or similar consequences for the system affected, i.e. the loss of data, loss of control or access to the system, and so forth, the causes of those breaches vary significantly, both in source and intent. Distinguishing between causes, sources, and intentions of the actor directly causing the breach can help to predict and prevent future breaches, either through technological or behavioural interventions.

This is not an exhaustive list, and other, more innovative forms of malicious attack will undoubtedly become more common over the coming years. The key distinctions among these terms — and probably among all possible varieties of cyber breach — is in the source and/or cause. *Figure 1* portrays these distinctions, which rest on whether a breach is intentional or accidental, state-sponsored or amateur.

These sources and causes of cyber incidents are logically distinct, though there is often overlap among them: with social engineering, for example, the malicious intent of an individual or group may overlap with the accidental contributions of a well-intentioned user. An individual may similarly exploit a cyber security system with the backing of a political group.

Regardless of the type of attack or the intention of the individual causing the data loss, cyber security measures involve protection of data and the prevention of unauthorised access, whatever its cause. The purpose of cyber security protocols are therefore to prevent and minimise the damage from all types of breaches. Awareness about how breaches occur, and how malicious attacks are changing with the advent of new technologies, is necessary for doing so.

Figure 1: Root causes of cyber incidents



Imperial College London
Institute of Global Health Innovation

Table 1: Common terms relevant to cyber security [9,10]

Credential reuse
This type of attack relies as much on a malicious hacker's intentions and abilities as it does on the frequency with which users use identical passwords when logging on to different websites. If one website's database containing user logon credentials are leaked, hackers attempt to use this information, which usually appears on the dark web, to access user data from other websites. For example, if all credentials for a badly protected gaming forum are stolen, hackers will use these usernames and passwords to try to log on to banking websites with the same details.

Cross-site scripting
In this type of attack, a malicious hacker targets a specific website's users by injecting a legitimate website's content with code that can infect users' browsers. Any information the user communicates through the website is then funnelled directly to the hacker.

Cyber attack
Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Denial of service
While this type of attack does not lead directly to loss of data, it can disable users from accessing the page; when financial institutions, for example, are targeted, this type of attack has the potential to damage a country's economy.

Dictionary attack
A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

Download attack
The unintentional installation of malicious software or virus onto a device without the user's knowledge or consent. May also be known as a drive-by download.

Exploit
May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

Human error
From forgetting to log off a public machine to forgetting USB drives on the bus, human error accounts for an enormous amount of data loss per year. Fifty-three percent of all cases of data loss may be due to mistakes or neglect on the part of the healthcare organisation in question.[8]

Malware
One of the most common sources of breach, malware is an amalgamation of 'malicious' and 'software.' Malware can be used to steal data, monitor machine usage, or control devices, but almost always requires that an authorised user, mistakenly or otherwise, installs the programme onto his or her machine.

Pharming
An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

Phishing
Phishing is a particular type of email scam, whereby victims are targeted from seemingly genuine persons or services, with the aim of tricking the recipient into either providing personal details or clicking on something that will allow the attacker to do something the user may not be aware of such as stealing credentials or installing malware.

Ransomware
Malicious software that makes data or systems unusable until the victim makes a payment.

Session hijacking
In this case, a malicious hacker takes control of communication between a user and server, enabling him/her to steal the data flowing between the two parties.

Smishing
Phishing via SMS: mass text messages sent to users asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.

Social engineering
Manipulating people into carrying out specific actions, or divulging information, that are of use to an attacker.

Spear-phishing
A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

SQL injection attack
This type of attack specifically targets databases built using the SQL programming language. In this case, a malicious hacker may breach the database through the language the database is built with; this can lead the database to reveal information contained within it to unauthorised users.

Sources: National Cyber Security Centre, UK, and NHS Digital; 'human error' is an original definition.

4
What makes the health sector particularly vulnerable?

Summary Points

- Investments to cyber security are not given priority
- Untrained staff constitute (unintentional) internal threats
- Outdated and unsupported IT infrastructures and medical devices increase NHS vulnerabilities
- Inefficient incident response capabilities exist due to lack of cyber security specialists
- Complex structures hinder fast and efficient responsiveness in the face of a cyber attack

Healthcare is one of the most frequently targeted sectors by hackers, in part because security among institutions is variable and because private health data can be valuable on the dark web.[2-5] Given the size of the population the NHS serves, major breaches, such as 2017's WannaCry attack, represent a significant threat.

The scale and availability requirements for sensitive data

As other sectors aim to limit access to data, the nature of healthcare and its sheer scale dictates that patient records need to be available to multiple staff members and now to patients as well. The personal and financial information included in medical records not only contains some of the most sensitive aspects of a person's life, but may also be as valuable on the dark web as credit card data, making records attractive targets to malicious hackers.[11,12] Recent cyber incidents in the healthcare industry showcase this: in 2015, 78 million records were stolen from the Anthem Blue Cross Insurance System in the United States, and over 1.5 million records were stolen from the Singapore health system, including that of the country's prime minister in 2018.[2,4]

Outside healthcare, records can be used for blackmail or, as is becoming increasingly common, in the United States, for identity theft: according to *Forbes*, about 1% of the US population filed some kind of credit card complaint in 2016, 13% of which concerned identity theft.[13] As much as 10% of the US population had medical records breached in the same year and these records can be found on the dark web selling for a mere $100 each.[13] As health records often contain enough information to steal a patient's identity, their value can be a great deal more in the wrong hands.

The competing demands of investing in IT and direct patient care

There has been chronic underinvestment in healthcare IT, especially compared with other market sectors; NHS organisations spend only 1-2% of running costs on IT services compared with 4-10% elsewhere.[14] To embed a security culture, there needs to be progressive investment in IT and an economic impact assessment to understand what is working. With limited budgets, health systems are faced with difficult choices in allocating resources, and cyber security investment is often not a priority when organisations struggle to meet minimum requirements for IT provision. This is often seen as a trade-off in all sectors, though the potential consequences for healthcare, both economic and in terms of patient safety, may be catastrophic.

While the UK government has invested heavily in cyber security measures, a year after WannaCry none of the 200 NHS hospitals inspected by the Care Quality Commission and NHS Digital met the criteria for Cyber Security Essentials Plus certification, a basic standard for security within the UK.[1] While no organisation had passed an assessment commissioned by NHS Digital, the purpose was to create a baseline and gauge improvement. (See page 16)

The extended legacy IT estate

Besides the complexity of the NHS, the IT landscape within the system is highly heterogeneous and inconsistent. For instance, different networks like the Health and Social Care Network (HSCN), local authority Public Services Network (PSN), or direct internet connections are in place, requiring differing security approaches. Although the Department of Health and Social Care (DHSC), NHS England, and NHS Improvement have defined the Data Security and Protection Requirements (DSPR) based on the National Data Guardian's 10 data security standards, no detailed specifications are provided.

Therefore, it is not unusual that old software is used as long as it is regularly patched or not connected. In fact, all 80 NHS organisations that were affected by WannaCry had failed to apply the Microsoft update patch that had been recommended by NHS Digital.[15]

Although important steps are being taken to resolve these issues, much work remains to be done. Without accurate asset inventories of what is on a network, organisations will face the challenge of not being able to patch that which they don't know exists. To date, no catalogue exists to systematically list all software and hardware deployed within the NHS. This leads to a severe lack of visibility of NHS vulnerabilities. Hence, it is not easily possible to evaluate the NHS's resilience against cyber attacks.

Skills and capability

Hiring trained cyber security staff is difficult for the NHS, as it is unable to compete with commercial salaries. In December 2018, about 1.5 years after WannaCry, a Redscan freedom of information (FOI) request showed that as much as 25% of NHS trusts had no employees with cyber security qualifications.[15] It also highlighted that among trusts with 3000 to 4000 employees annual cyber security training expenditure may be as little as £500. Financing shortages also reputedly make it difficult for the NHS to hire competent cyber security personnel given the large pay gaps between public sector and private sector wages for similar work.[16]

Employee behaviour and culture

Most sectors aim to reduce their cyber risk by locking-down systems and limiting access to records. In healthcare however, this is difficult as access is required by multiple users to ensure safe delivery of care. In fact, there is a renewed drive to widen access across providers, share even more data and give patients and staff alike access to health records across a range of devices and settings.

Healthcare is actively widening access and opening up systems whilst simultaneously collecting an ever-greater range and depth of data. Furthermore, the increasing dependency on agency and temporary staffing within the health sector adds greater vulnerabilities and risk. Staff may be unfamiliar with systems and dependent upon the sharing of credentials to support the delivery of care, whilst the use of temporary staff increases the inherent challenges of tracking and monitoring access and use of systems and data.

Employee behaviour is a crucial aspect of healthcare cyber security that is frequently overlooked. Easy access to the most personal aspects of a patient's life means that the potential for malicious activity is ever-present, particularly if data belongs to high-profile patients. There are publicised examples of such behaviours of staff being disciplined and hospitals fined following inappropriately accessing and sometimes leaking the medical records of celebrities.[17-18]

Currently, it is mandatory for all NHS staff members to complete online training on information governance (including cyber security), though recent evidence suggests that only 12% of trusts reached the NHS Digital target of 95% compliance.[15]

Highly complicated governance structures

The NHS, like all other health systems, is a complex behemoth of many organisations that provide leadership and governance for services across the board. The oversight for cyber security is led by the DHSC and different accountabilities have been assigned to the Arm's Length Bodies (ALBs; see *Figure 2*).

One main problem is the lack of clarity and transparency leading to partly overlapping competencies. Such uncoordinated processes result in higher costs, inefficiencies and waste of resources. Complicated interrelationships prevent the NHS from responding to cyber attacks in as fast and agile way as possible. In the field of cyber security, efficient responsiveness is critical for ensuring smooth-running operations, fast recovery from disruptions and mitigating negative impacts on patients.

Several key vulnerabilities, with particular emphasis on patient safety, are endemic to the healthcare industry and require immediate intervention to enable a safe and secure future for healthcare. While the UK government has, in the wake of WannaCry, begun to take steps to mitigate the risks these vulnerabilities pose, more work is needed to determine the specific risks unique to the NHS, which will in turn lead to improved cyber resilience.

***Figure 2*: National Accountabilities for Cyber Security of DHSC (black box) and ALBs (grey boxes)**

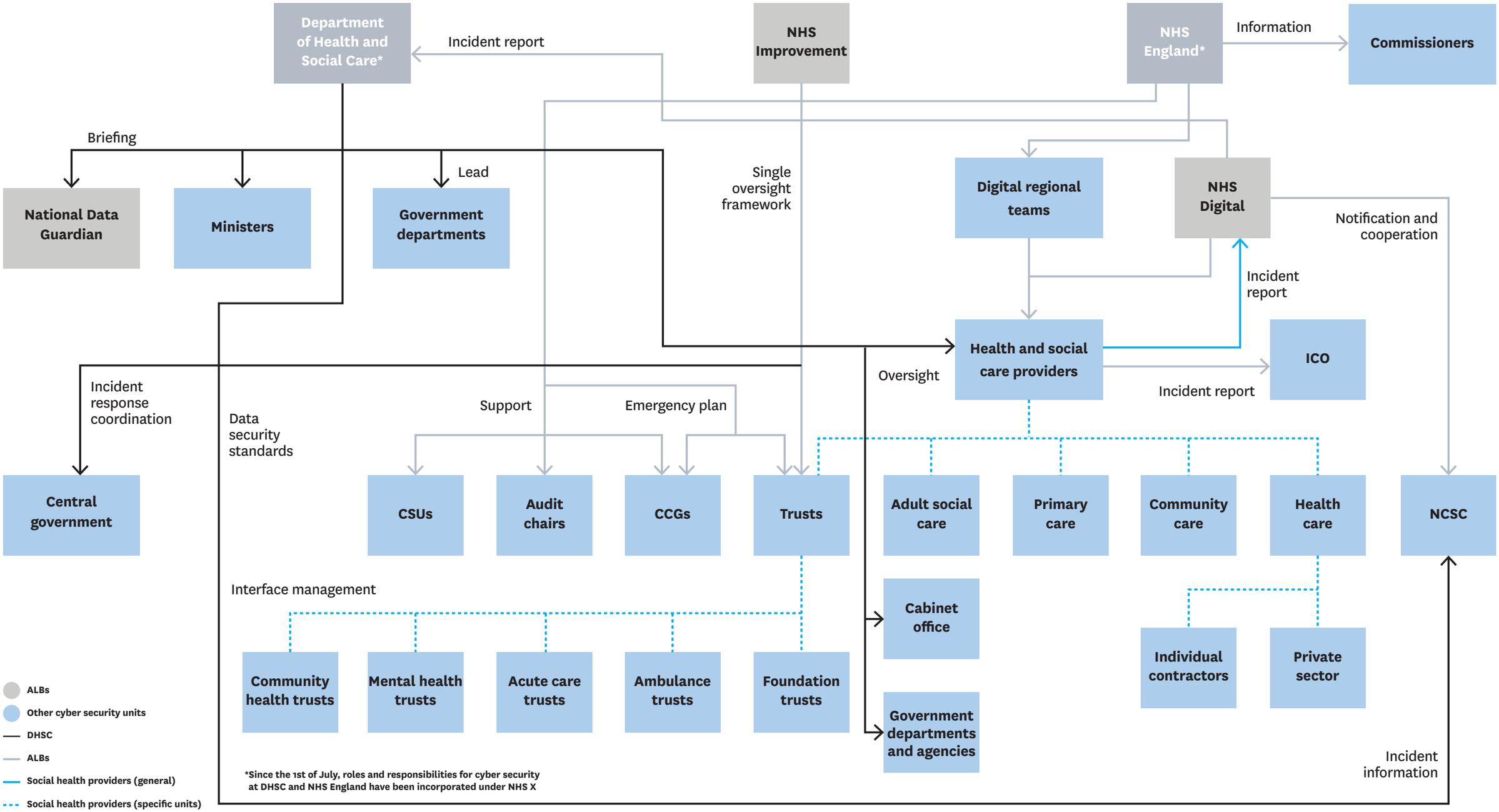


Figure reprinted with permission from the Lancet Digital Health (Ghafur et al. 2019).[19]

5
NHS cyber security accountabilities

Imperial College London
Institute of Global Health Innovation

Summary Points

- This section highlights the different national and local bodies accountable for healthcare cyber security and their roles
- NHS cyber security accountabilities are complex and interrelated
- Newly introduced NHS incident response processes aim at improving cyber resilience, e.g. through CareCERT
- It is hoped that through the launch of NHS X will help streamline NHS cyber-security accountabilities

The Government Communications Headquarters (GCHQ) is an intelligence and security organisation responsible for providing signals intelligence and information assurance to the government and armed forces of the United Kingdom. The NCSC, part of GCHQ, was established in October 2016 to be the UK's national authority for cyber security advice and incident management. It has a mandate to help bring coherence and transparency to UK cyber security, in support of the government's commitment to make the UK the safest place to live and work online. As part of GCHQ, it can draw on the unique capabilities of the UK's intelligence agencies to help us do this.

GCHQ and NCSC provide intelligence and support for all critical sectors in the UK, however, DHSC and the ALBs are responsible for operationalising services across the NHS. Since the WannaCry attack, the NHS has taken several steps to increase its cyber resilience, and accountabilities have been assigned to the DHSC and ALBs, as shown in *Figure 2*. This figure highlights the significant complexity of NHS organisational structures due to the large number of ALBs and sovereign organisations.

The DHSC is accountable for the regulatory oversight of Trusts and Foundation Trusts under the Network and Information Systems (NIS) Regulations as well as for the compliance of the data security standards applying to all health and care providers. [12] It also takes on the role as an interface manager between the Cabinet Office, health and social care providers and other government departments and agencies.

NHS Digital plays a central role in threat detection, response and recovery. As an example, the launch of the cyber security operations centre (CSOC), has seen an increased threat intelligence capabilities; this has resulted in several nationwide potential cyber attacks intercepted and prevented and has blocked 1.4 million communication attempts with malware botnets.

Based on the Single Oversight Framework, NHS Improvement monitors data security standards of NHS trusts and provides support to achieve required security levels. It ensures that health and social care providers take the recommended measures for improving cyber resilience. Similarly, NHS England is accountable for ensuring that cyber security standards of, for example, the NHS Standard Contract are implemented and that emergency plans exist in case of a cyber emergency. In addition, Commissioning Support Units (CSUs), audit chairs and Clinical Comissioning Groups (CCGs) are supported by NHS England on how to increase cyber security. NHS Improvement and NHS England act as information providers concerning cyber security to healthcare providers and commissioners, respectively.

In the case of a cyber incident different processes and measures take place. For instance, NHS Digital, the Information Commissioner's Office (ICO) and the NCSC have to be informed as soon as an attack is detected. As indicated by *Figure 2*, NHS Digital pass the information onto the DHSC as the Competent Authority for the health sector. The Department provides incident information to NCSC and is responsible to brief the Ministers and the National Data Guardian at the same time. In turn, NCSC provides intelligence information and the National Data Guardian advises how to share and secure data.

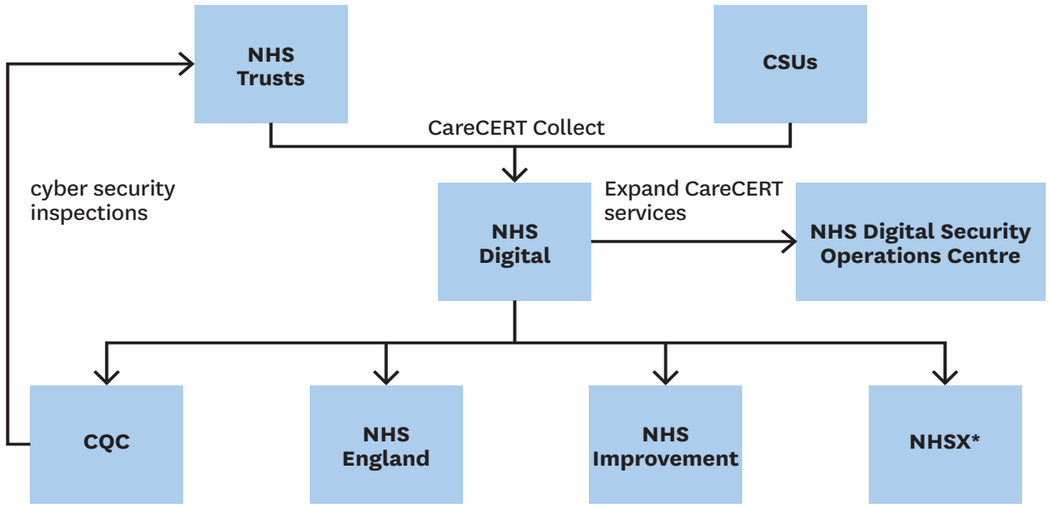
After a cyber attack ALBs coordinate and provide support in terms of response actions. In particular, NHS England acts upon its Emergency Preparedness, Resilience and Response (EPRR) framework, coordinating and managing all efforts to mitigate and control the negative impacts. In the case of a major attack NHS England guides the response activities of the overall system. In collaboration with NHS Improvement communication about the respective incident to all health and social care organisations is established. NHS Digital, supported by NCSC, is a further adviser helping the healthcare system in responding to cyber incidents on a national and local level.

Complexity of accountabilities

Figure 2 highlights the significant complexity of NHS organisational structures due to the large number of ALBs and sovereign organisations. One main problem is that some bodies have partly the same accountabilities and competencies, leading to multiple and not necesseraly uniformed response activites. As shown in *Figure 2*, NCSC receives information about a cyber attack directly from NHS Digital and additionally through DHSC, making the information transfer cumbersome and complex.

Different networks like the Health and Social Care Network (HSCN), local authority networks or direct internet connections are in place, requiring different security approaches. Although the DHSC, NHS England and NHS Improvement have defined the Data Security and Protection Requirements (DSPR) based on the National Data Guardian's 10 data security standards, no detailed specifications are provided. As commissioners of GP IT services, CCGs must ensure commissioned GP IT providers are contractually required to comply with these requirements.

***Figure 3*: Securing Cyber Resilience**



*NHSX will combine teams from DHSC, NHS England and NHS Improvement.

Incident response

In the case of an incident, all health and care organisations have to inform NHS Digital through the Information Governance (IG) Toolkit and the Information Commissioner's Office (ICO) if the incident exceeds level 2. In this instance, the IG Toolkit has been replaced by the Data Security and Protection (DSP) Toolkit, which is an online self-assessment tool measuring the performance of health and care organisations against DSPR.

Performance against the DSPT standards is the baseline used to inform progress, is monitored by NHS England, and applies to all NHS organisations, Local Authorities and bodies commissioned or contracted to provide services who process personal confidential health and adult social care data. Over 27000 DSPT self-assessments have been completed with over 97% meeting the DSPT standard and 532 organisations exceeding it.

A new version of the toolkit was released by NHS Digital in June 2019 incorporating a broader range of external security standards Cyber Essentials, EU NIS, Minimum Cyber Security Standard (MCSS) and the NCSC Cyber Assessment Framework. It is a requirement for large NHS organisations' DSPT self-assessments to be independently audited annually. Additionally, NHS Digital is working with the CQC on providing expertise and specialist Cyber advisors for their 'Well Led' Inspections.

Although cyber incidents are reported and registered in a database, the data are not systematically processed or statistically evaluated. Therefore, the fundamental understanding and awareness of potential risks and threats are missing. Since NHS Digital does not measure risks or vulnerabilities on a local level, it is not possible to assess the impact a cyber attack would have on the NHS's IT infrastructure, data, and patients in advance.

Efforts have been made to improve the NHS's responsiveness to cyber threats. In 2016 NHS Digital was commissioned by the Department of Health to develop a Care Computer Emergency Response Team (CareCERT).[20] CareCERT consists of three key services, which support stronger cyber security across health and social care: a national cyber security incident management function, good practice guidance on cyber security for the health and social care system, and national level threat advisories which are broadcast to organisations across the health and social care sector.[20] *Figure 3* gives an overview of how CareCERT is used to improve cyber resilience.

If an alert is triggered by the CareCERT Collect system all NHS trusts and Commissioning Support Units (CSUs) have to report what they have done in response, e.g. implementing security patches or updating anti-virus software within 48 hours. New initiatives like the NHS Digital Security Operations Centre are intended to increase NHS Digital's monitoring and cyber security capabilities.

The development of CareCERT into the Cyber Security Operations Centre (CSOC) will support NHS Digital in offering enhanced services across the sector. The deployment of over 900,000 instances of Advanced Threat Protection (ATP) has improved both the protection of end point devices, and the capability the CSOC has to hunt and identify threats across the sector.

This is complemented by centrally funded interventions at a local level designed to increase cyber resilience and improve security postures, as well as providing services, e.g. vulnerability scanning and protected domain name system (DNS) ,launching in 2019, that health organisations can utilise.

NHS Digital have performed on-site cyber security assessments on all Trusts and a number of primary care providers based on the Cyber Security Essentials Plus certification. The Data Security Protection Toolkit has increased the capability to better assess the broader system with supporting services for on-site assessments. As a result, NHS Digital is able to provide tailored advice to NHS organisations on the cyber security capabilities and how to mitigate future threats.[21]

One recommendation from the NHS CIO's WannaCry report is for all large NHS Organisations to achieve CE+ certification by June 2021. NHS Digital have performed On-Site Cyber Security assessments including CE+ on all Trusts and a number of primary care providers. As of March 2019, 38 organisations are already CE+ certified, 27 months before the target date. Achieving CE+ is a pass/fail assessment, as organisations improve security controls the more will become CE+ certified.

DHSC plans for cyber resilience

In October 2018, the DHSC published a report outlining its plans to improve cyber resilience within the NHS.[22] The report, part of the Data and Cyber Security Programme being developed by the DHSC along with the aforementioned ALBs, details current and planned spending on cyber security in the NHS, the estimated costs of WannaCry overall, and plans for decreasing the risks associated with cyber security in the short and long term.

In addition to outlining spending and software plans, the DHSC provides 22 recommendations for the NHS, and its constituent trusts and practices, to mitigate technological vulnerabilities throughout the country. In addition to a new agreement with Microsoft to ensure all systems are updated appropriately and as needed, the department plans to spend £150 million over the next three years to 'protect key services from the impact of cyber attacks.'[22] These methods of protection include, primarily, improvement of infrastructure, interventions to address weaknesses often found in the NHS, and investment in NHS Digital's Cyber Security Operations Centre. Site assessments are planned, over the coming years, to determine whether individual sites are doing enough to prevent cyber incidents.

NHSX

A new ALB, NHSX, was launched on the 1st of July, 2019. NHSX brings teams from the DHSC, NHS England and NHS Improvement together to drive digital transformation and lead policy, implementation and change. It is headed by Matthew Gould, who previously served as the UK government's Director of Cyber Security.[22] Among other responsibilities, NHSX will mandate cyber security standards across health and social care, to ensure that all organisations related to the NHS have security protocols from inception.

It is hoped that the launch of NHSX will help streamline and simplify the national cyber security accountabilities for the NHS by integrating the roles and responsibilities of the cyber security teams at NHS England and the DHSC. This will be key to help front line NHS IT teams in implementing any national and local protocols.

6
Emerging challenges

Summary Points

- This section looks at the cyber security challenges of emerging tools including: connected medical devices, algorithmic decision making, Electronic Health Records, robotics, cloud computing and precision medicine
- Connected medical devices can have dramatic cascading effects in the case of cyber attacks
- Deficient monitoring mechanisms of cloud services imply complete reliance on third-party organisations
- Implications of decisions made by artificial intelligence algorithms are not yet well understood in the healthcare context
- Discrimination and manipulation of DNA data can have far-reaching consequences for the individuals and their relatives
- Secured access to patient data and records is essential to mitigate the risks of manipulation and theft of data as well as disruption of care operations due to unauthorised actions

The NHS, along with health systems across the world, is becoming ever more reliant on technology to deliver safe patient care. There are exciting new innovations that have the promise to change the way care is delivered and offer new treatments and discoveries. Some of these technologies such as artificial intelligence (AI) and robotics are already in use at relatively small scale and in some trusts. However, their widespread and combined use is likely to generate a step-change in quality and nature within this sector. The challenge will be to adopt technologies safely and securely and appreciate the emerging cybersecurity challenges that become more apparent as these technologies are more commonplace.

Imperial College London
Institute of Global Health Innovation

Connected medical devices

Opportunity
If a method of assuring the cyber security of connected medical devices can be achieved, it will be possible to deliver a fully integrated and scaled ecosystem of connected medical devices across healthcare providers and patients. The data captured by connected medical devices, if fully integrated, will provide real-time information and open new opportunities for understanding diseases and treating patients.

There are currently small-scale test beds of this type of device integration being conducted. For example, Imperial College Healthcare Trust are currently piloting the integration of monitoring devices with its EHR. The monitoring devices capture observations and this data automatically flows into the patient's EHR. It produces an early warning score for the patients which can incite early medical intervention.

Threats/challenges
If nothing is done and adoption of medical devices continues at pace and scale there could be mass introduction of poorly regulated or unsecure medical devices that are hyper-connected and vulnerable to cyber threat. At present, healthcare providers are unable to effectively and consistently risk assess the adoption and integration of emerging technologies and there is a persistent lack of agreed minimum standards for security.

Current landscape
There is a lack of procurement policy to monitor and regulate devices being used in care delivery. Additionally, there is little incentive for suppliers of medical devices to provide appropriate levels of cyber security due to the high cost, with a lack of mandate to do so. The consensus among experts, both within the cyber security and medical areas, is that this risk is real, pressing, and that high security standards are needed more than ever, with the advent of advanced medical devices.

Whilst robust regulatory standards for safety exist there is a lack of explicit cyber security equivalents that medical devices must meet to be released to the market. Most now recognise that a set of security guidelines must be developed. The US Food and Drug Administration (FDA) is leading in this space; while the EU's medical device regulations are less well-defined than those of the FDA, two publications in May 2017 introduced strict rules around post-market surveillance of all medical devices approved for use in member states.[23] All member states are required, since the publication of these papers, to maintain close surveillance of all approved devices, to monitor any hazardous incidents, and to report all corrective action taken thereafter.

A report from British Standards Institution (BSI) notes, however, that these documents do not deal closely with the subject of security, and instead focus on the safety of medical devices approved in EU member states. The EU regulations specify only that all devices should maintain 'state of the art' security which will require time (and potentially the accumulation of case law) to credibly evolve into a commonly understood baseline.

The Department of Culture, Media and Sport (DCMS) launched a Code of Practice for consumer internet of things (IoT) security in 2018.[24] This Code of Practice sets out practical steps for IoT manufacturers and industry stakeholders to improve the security of consumer IoT products and associated services in the home, through a set of 13 guidelines.[24] Despite this code of practice being introduced, there is still not an equivalent guide for medical devices.

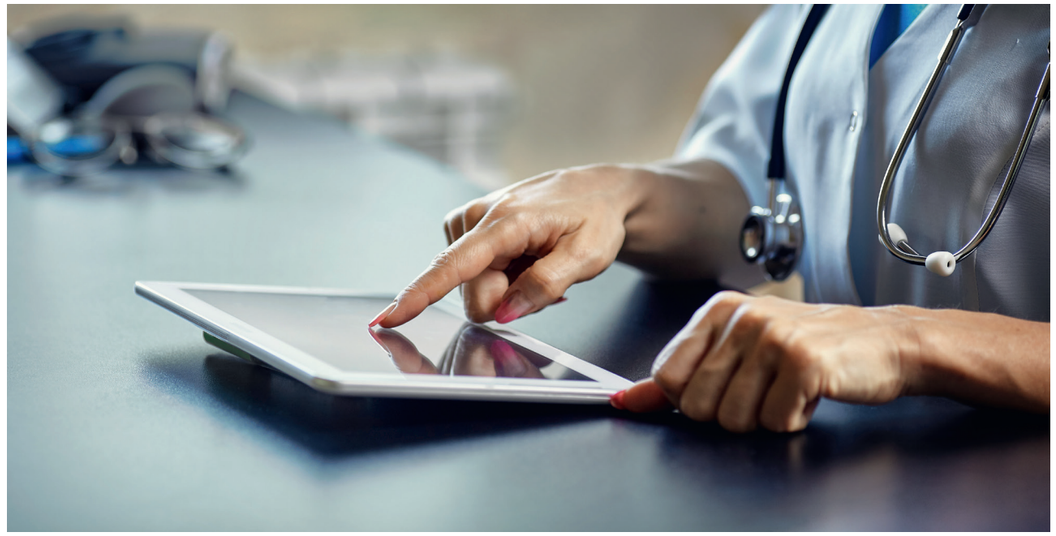
Artificial intelligence: algorithmic decision making

Opportunity
Clinical decisions may be delegated to algorithms including AI and machine learning. There is the opportunity to use data collated by a plethora of medical devices to provide data-driven, real-time diagnostics and care management decisions. The accuracy and efficiency of algorithmic decision-making will allow for early intervention of medical care, personalised treatment and real-time monitoring for patients. Ultimately, appropriate and managed use of algorithmic decision-making will save time, improve accuracy and reduce cost for the NHS.

Threat/challenges
As the healthcare sector begins to introduce algorithmic decision-making into clinical settings, significant consideration must be given to the implications they may have upon patients or practitioners. If an algorithm makes the wrong decision, who will be held responsible and how will this be managed? A recent study demonstrated how attackers can use deep learning to add or remove evidence of lung cancer from medical scans that in turn could not be differentiated by the reporting radiologists[25]. It is evident that, at present, processes are not yet established to effectively manage algorithmic decision-making in healthcare. Soon the delegated decision will be much more complex (e.g. diagnosing chronic medical conditions). In addition, the impacts of AI algorithms upon clinical liability, as the human is removed as the authoritative decision-maker, have not been considered.

The nature of AI means that it is often trained locally by the data that is inputted into the machine. This means that the machines quickly become specialised, easily adaptable and significantly divergent from those supplied by the same manufacturer. The implication of this is that traditional fixes such as 'patching' will become redundant as a singular fix will not be suitable for all machines that have been trained using different data and it cannot be proven that it is better than before the fix. The adaptability and specialist capabilities of AI can be favourable, but they also present a challenge from a governance and assurance perspective as the machines have the ability to change momentarily and cannot be treated in an identical manner.

Current landscape
The DHSC launched a code of conduct for data-driven health and care technology (February 2019) with 10 key principles.[26] There is a small-scale pilot of a mobile phone-based application using AI technology to alert staff to patients at risk of deterioration and death through kidney failure.



Electronic Health Records (EHRs)

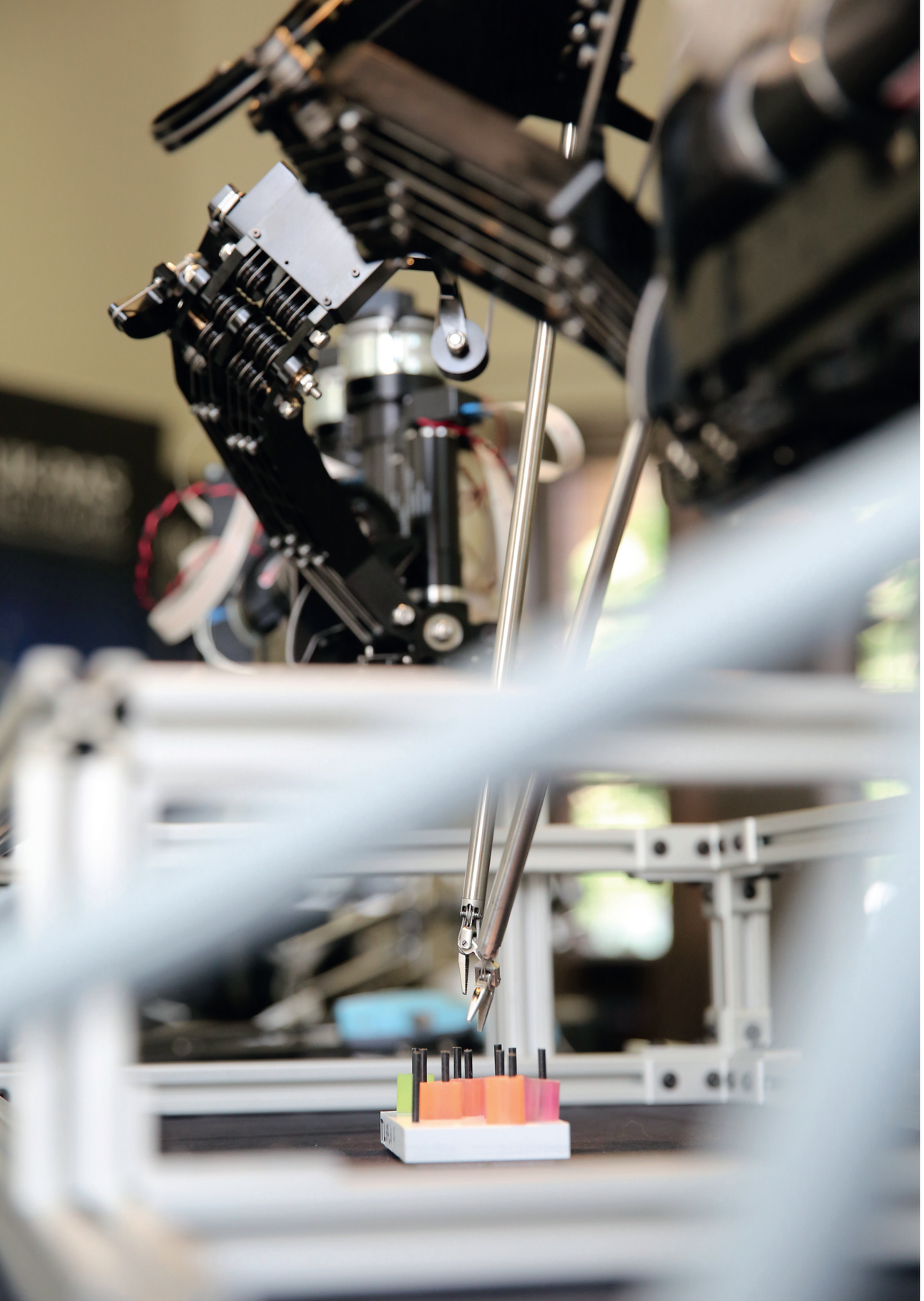
Opportunity
EHRs will be the foundation of a digital healthcare system that configures data from medical technology. Patient access to their own data in the future will enable them to better understand and manage their own medical data and give them greater autonomy in their healthcare decisions.

Salford Royal NHS Foundation Trust is currently exploring how to integrate medical devices so that the data generated can provide real-time information and decision-making. The trust is working with Marand from Slovenia on an open EHR platform. A patient portal allows patients to share their blood glucose and blood pressure readings from devices, with a clinician then able to access and review the data.

Threats/challenges
If the parameters of access and control for an individual's EHR are not appropriately managed, then patient data may be vulnerable to misuse and cyber threat. The supporting infrastructure for EHRs must provide secure flexibility to service the need of each user and the healthcare sector needs to establish a data architecture that would set the appropriate parameters of access and control for different users of EHRs.

Current landscape
The WannaCry attack showcased the vulnerabilities posed by EHR systems when clinical staff cannot get access to critical information. Even if an attack is determined to have been accidental, any disruption that removes access to EHRs has the potential to disrupt care, preventing treatment, congesting care pathways and impacting patient safety. Removing access is one thing; another consideration is a malicious attempt to corrupt data over a period of time where it is difficult to detect, creating a lack of confidence and reliability in the data. Over-reliance on badly connected EHR systems may leave the NHS vulnerable to a widespread shutdown in the event of an intentional attack.

The ambition for the healthcare service is for patients to have access to their medical records. This again adds another layer of risk in terms of cyber security and if the parameters of access and control are not appropriately managed then patient data may be vulnerable to increasing cyber threats. As patients begin to have systematic access to their own data, the government must find ways to educate the public on how to safely store and share their personal data.



Imperial College London
Institute of Global Health Innovation

Robotics

Opportunity
Robotics in healthcare have the potential to transform the delivery of care in a variety of ways, such as carrying out repetitive tasks (e.g. patient observations), aiding a human surgeon or executing operations independent of human intervention. Robots will significantly impact delivery of care for the elderly either through assisted living or end-of-life care by prolonging personal independence. For healthcare, the ambition is that this will reduce the pressure put on the NHS in the face of an ageing population.

Threats/challenges
Robotics use a complex mesh of AI algorithms to make decisions. As previously discussed, there is a risk that removing the human factor from the decision-making process drastically changes clinical liabilities for which the healthcare sector is not currently prepared to manage safely, securely and at scale. The successful adoption of robotics to realise potential benefits to the healthcare sector is reliant on effectively managing the human interaction with them.

Current landscape
Current investment into developing robotics is underpinned by the UK government's plans to invest £300 million in RAS (Robotics and Autonomous Systems) research between 2012 and 2020. Additionally, GrowMeUp is an ongoing project endorsed by the EU that is developing a robot that has the capability to respond to changes in an individual's routine and environment.[27]

As observed by the Parliamentary Office for Science and Technology, 'Many of the robots and robotic devices developed for social care appear to still be at the conceptual or design phase'.[28] The real challenge is understanding whether or not robotics can be integrated into clinical environments alongside existing technologies and governance practices.

Cloud computing

Opportunity
Cloud computing will allow large-scale analysis of medical data to support healthcare services, especially when combined with AI. According to the 2017 Healthcare Information and Management Systems Society (HIMSS) Analytics Cloud Survey, 65% of hospitals had been utilising cloud services in some capacity, and it is expect that the majority of EHRs will be cloud-based by 2020.[29] The UK NHS Blood and Transplant, for example, has been using IBM Cloud to optimise its organ allocation scheme by analysing medical records in the cloud to identify potential transplant recipients.[30] In 2018, Arthritis Research UK launched a cognitive virtual assistant, powered by IBM Cloud and AI, which was trained by specialists to provide personalised 24/7 support for arthritis patients.[31]

When integrated properly, the security of cloud-based solutions has the potential to exceed that of local servers alone.[32] Furthermore, the operational costs of on-demand cloud computing and storage are low, which is supportive of the push for increased access to EHRs, digital health solutions and the analysis of medical data for research purposes.[33-35]

Threats/challenges
While progress is being made to adopt cloud computing solutions, there is still a lack of awareness and education around the technology, which could be exacerbated by a culture wary of putting trust in servers they cannot directly control.[36] Cloud services are supposed to be monitored 24/7 by specialist third-party IT staff and alert clients of any suspicious behaviour. There are some instances where this has failed to happen. As of January 2019, 416 cases were investigated by the US Department of Health and Human Services' Office for Civil Rights involving security breaches of health information, 47% of which were caused by an IT incident or hacking.[37]

These incidents highlight another challenge of cloud computing: healthcare providers are completely reliant on third parties to store and protect their data. Healthcare providers need to have, at least, some degree of oversight to ensure that their cloud service supplier is complying with regulatory frameworks. They also need mechanisms in place to continuously monitor the company's compliance through using security tools and audit logs.

Current landscape
NHS Digital has issued a guidance document approving healthcare organisations' use of cloud computing, provided that appropriate safeguards are put in place.[38] The challenge, however, is to navigate the fragmented structure of the NHS in order to implement adoption of cloud computing, as well as overcome cultural resistance. Local service agreements should also outline what the scope of the cloud services are, who is responsible for what, who holds insurance, who's indemnifying whom and what the healthcare provider's rights are to access the data.[39]

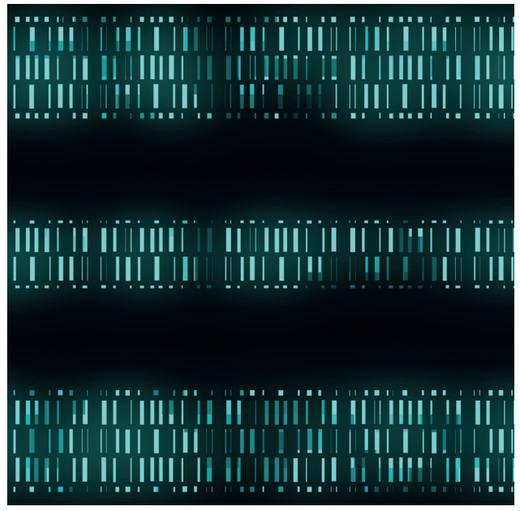
Precision medicine

Opportunity
Precision medicine has the potential to facilitate more effective treatment options for rare as well as noncommunicable diseases. The concept of using a person's genomic data to design treatments tailored to that person is no longer a far-fetched concept, because of the decreasing cost of genome sequencing and its availability through research initiatives.[40]

The 100,000 Genomes Project was first announced in 2013 through the establishment of a private company, Genomics England, owned by the DHSC. The aim of the project was to sequence the DNA of 75,000 patients with cancer as well as families affected by rare disease. There has been success in treating patients based on their genomic data.[41,42]

The UK Biobank has collected over 500,000 medical records, DNA samples, as well as other biological samples and health and wellbeing data from volunteers. If volunteers consented, these data could be anonymised and linked to their EHR to correlate them with hospital statistics. By 2020, the organisation is hoping to make these anonymised records publicly available.[43,44]

Threats/challenges
While precision medicine is more accessible than ever to the general public and has had various success stories, there are still concerns about research participants, as well as their relatives, becoming victims of hacking or DNA discrimination. In December 2018, Genomics England were forced to address reports that, because of multiple cyber attacks on their database of 85,000 individuals' genomes, they had to move participants' data to a secure Ministry of Defence (MoD) base. Genomics England maintained that there was "no evidence" that it had been targeted by any cyber attacks, that patient data had never been moved and in fact resided in a secure government-owned facility based in the UK.[45,46]



Even the suspicion that participants' data could be compromised is enough to generate scepticism of genomic sequencing schemes. Unlike social security or national insurance numbers, credit card information and other data subject to fraud, DNA data of an individual cannot be changed and are shared, to some extent, with their relatives.[47] However, there is little to no privacy protection in place for the extended relatives of individuals who take part in uploading their DNA to open databases or taking part in genomic research. Therefore, as the popularity of seeking health and ancestry insights grows, so does the threat to relatives' privacy and their risk of being affected by a hacking incident.[48]

Current landscape
To protect the data of participants of genomic research, policymakers have restricted access to pools of anonymised biomedical genetic data.[49,50] If hackers were able to match genetic information with personal information, there are a myriad of malicious uses for that combination of information. These include exploiting people in positions of power, identity theft, framing a person for criminal activity and holding genetic data ransom in return for a steep price and in a worst case scenario, using mass data to develop bio-weapons.[51]

7
Key practice priorities

Imperial College London
Institute of Global Health Innovation

Summary Points

- Key practice priortities include: awareness, education, regulation, creating secure infrastructure and research to support practice
- Incentives and regulations for medical device manufacturers are needed to ensure security-by-design
- Raising awareness at all levels leads to a better understanding of potential implications of cyber threats
- Having secure IT infrastructures in place is a fundamental prerequisite for better cyber resilience
- Cultivating a security culture throughout the healthcare sector can help significantly to improve patient safety
- Cyber incident response and recovery processes have to be tested and business continuity planning has to be part of the board agenda
- Developing a clear and comprehensive support and oversight framework is necessary to facilitate complex decision-making processes

Awareness

There is a need to improve individual, organisational and system-wide awareness of future threats, vulnerabilities, and the potential impact of cyber security incidents. Health and social care must ensure the adequate provision of comprehensive advice, guidance and communication to support organisations in the adoption of emerging technology safely and securely.

All organisations need to develop and promote a security culture and ensure that the message being filtered is that cyber security is not just an IT concern, but a patient safety concern. Improving staff training and awareness of the implications of cyber attacks as well as what can be done to mitigate the risk is vital.

Leadership is also key and the fragmentation of organisational structures — local, regional, and national — must be avoided to ensure a consistent message is being delivered, resources are not being duplicated, and that senior leaders have the authority and responsibility to effect positive change and be held account for failures.

Recommendations:

1 Strengthen, expand, and appropriately resource the current NHS Digital CareCERT programme to provide a single strategic cyber forum that brings together a range of experts in order to share best practice, develop guidance for organisations, and build wide capability and resilience

2 Highlight and spread good practice and identify local exemplars of best practice in each region to support all organisations in improving their security awareness and posture. Funding from the Global Digital Exemplar programme should be ring-fenced to support the development of these local security champions

3 Support and encourage open dialogue, scrutiny, and consultation regarding both cyber security concerns, and concerns surrounding data security and confidentiality with patients and staff through a formal process of patient and public involvement and engagement

4 Local NHS Boards need to understand the frameworks to manage cyber risks in the way they manage clinical risk and there should be further educational provision to do this. NHS Digital has delivered GCHQ accredited cyber security awareness training to over 150 boards

5 Security professionals from industry should work with the NHS to support and improve training and expertise in cyber resilience.

Education

Even in security-conscious organisations, the click rate on well-crafted phishing emails can be up to 30%, and it remains true that the most common sources of ransomware are malicious email attachments that are inadvertently opened by staff.

Meanwhile, one of the biggest threats to patient data is the insider threat; with easy and ready access to large amounts of hugely sensitive personal information, the risk of accidental or deliberate compromise by individual staff members is ever present and must be tackled: organisations must be trusted by patients to secure their data and use it appropriately. All organisations need to develop and promote a security culture and ensure that the message being filtered is that cyber security is not just an IT concern, but a patient safety concern and therefore relevant to all staff members.

Recommendations:

1 Require the delivery of annual mandatory training in cyber security awareness and seek to embed a security culture across all organisations and staff, building upon current training modules staff in the NHS are required to undertake

2 Identify and classify the cyber threat as a specific patient safety priority akin to those for infection prevention and control or medication safety to improve awareness, develop shared learning, and change culture.

Governance

There is a need for supporting better decision-making, maintaining trust in the system and ensuring organisations meet their responsibilities to ensure clarity around responsibility, accountability and authority. Additionally, there is a need to develop and spread new methods to evaluate, quantify and report the direct and indirect impact of cyber security incidents or health IT failures on patients and providers.

A pragmatic, comprehensive and standardised framework for cyber security assurance and testing in health and social care must be developed; existing generic tools such as Cyber Essentials are not fit for purpose as the scale and pace of emerging technology adoption creates complexity which is not addressed by these current generic standards.

Recommendations:

1 Develop, test, and implement a mandated framework for cyber security and operational resilience testing and assurance in the healthcare sector; a “CBEST for Healthcare.” Additionally, security preparedness and resilience must become part of the Single Oversight Framework upon which healthcare providers are assessed and regulated

2 Provide specific support, guidance, and funding to enable all organisations to meet existing legislative requirements on data security; specifically, the General Data Protection Regulation (GDPR) and Directive of Security of Network and Information Systems (NIS Directive)

3 Simplify the oversight and governance of cyber security to better enable risk assessment and the adoption of technology at scale. Without clearly defined roles and responsibilities the structure does not support effective decision-making and avoids ownership and accountability

4 The infrastructure required for interconnected networks must be better understood to ensure the healthcare system is secure at scale. This is essential to ensure that flexibility is built into a system that will allow for the significant changes in data capture and retrieval requirements triggered by proliferation of connected medical devices and the introduction of assisted living and remote consultation

5 As the use of medical connected devices expands, there should be an asset management and supply chain system to designate the appropriate and necessary privacy, safety and security requirements of each device. However, the regulation/legislation/policy/guidelines in relation to this should be targeted at the supplier of the device rather than the user (healthcare staff) at the point of use.

Regulation

The UK has an opportunity to establish itself as an exemplar of cyber security best practice in healthcare by mandating 'Secure by Design' and clearly defining a minimum viable tolerance for risk regarding cyber security. This will support the prioritisation of cyber security to be as significant to care delivery as safety.

There is a risk when enforcing regulation that if too stringent, it can stifle innovation and inadvertently act as a blocker to technological and scientific advancement. This is not a desirable outcome as the UK seeks to be world-leading in healthcare. Robust cyber security standards may also increase the manufacturing costs of medical devices. As the healthcare sector does not mandate secure by design there is little current incentive for manufacturers to make the investment into cyber security.

According to a March 2018 report from the Royal Academy of Engineering (RAEng), while digital technologies are quickly improving healthcare throughout the UK, organisations throughout the healthcare sector are not yet able to manage security threats and in many cases, such as with medical devices, are not even aware of the threats they face.[52] It is remarkable that minimum security standards exist through the 'Secure by Design' code of practice for consumer Internet of Things devices such as smart lightbulbs and exercise trackers, but no such guidance exists for medical devices.[24]

Security risks are likely to change as technology advances and malicious hackers are, furthermore, likely to find other means of exploitation of our medical devices that are not yet known. Additionally, there is a need to provide further support, resource, and guidance to ensure compliance with relevant legislation governing information and data security for healthcare organisations.

Recommendations:

1 Modify current NHS procurement rules to ensure that the security and resilience of healthcare IT and medical devices is prioritised: changing purchasing decisions will force industry to improve the products and services on offer

2 Current legislation and regulatory schemes are not sufficient to manage the unknown quantity of unknown device types, conceivably connected to an integrated health records database whilst allowing the user (clinical practitioner) to do their job at the necessary pace

3 As the UK is on course to leave the EU, with unknown repercussions for medical regulation, it is critical that the UK government establish regulatory protocols for medical device cyber security within the next several months. As the EU's regulations are not yet well-defined, now may be an especially important time for the UK to develop its own comprehensive regulatory framework, which other countries, including EU member states, may follow.

Technology: secure infrastructure

There needs to be a progressive increase in the proportion of budgets spent on IT infrastructure and cyber security in particular. Organisations must ensure they have robust perimeter security (firewalls), effective protective monitoring (intrusion detection) and networks that are designed to support robust cyber security from the outset; all systems must be secure by design, not as an afterthought. There must be effective processes in place for the safeguarding and audit of data leaving networks.

Good cyber security 'hygiene' is also vital: effectively managing privileges, ensuring appropriate encryption, utilising multi-factor authentication, and ensuring systems are regularly patched and updated. The challenge of outdated medical devices and hardware running on legacy systems that are no longer supported must be tackled. Connected medical devices create cyber security vulnerabilities and therefore need to be independently assessed and catalogued according to risk they present.

Recommendations:

1 Introduce a programme to incentivise healthcare organisations to replace out-dated and unsafe IT hardware and software in a targeted way

2 Develop and institute an independent registry of medical devices to assess and catalogue their security flaws against an open and transparent minimum standard.

Resilience

Safe organisations are resilient organisations. There is a need to develop and test effective incident management procedures and improve business continuity planning across the entire healthcare sector. All organisations must be able to safely and effectively function whilst under cyber attack. Meanwhile, all data and systems must be securely backed-up and disaster recovery processes tested to ensure that the backup is isolated and cannot be erased or tampered with.

Recommendations:

1 Mandate the regular simulation and rehearsal of major cyber security incidents and IT failures at both a local and national level to test and improve resilience, much like other major incidents such as mass casualty events or fire evacuation drills. Additionally, testing of cyber resilience must form part of the regulatory framework [53]

2 Develop a response to the regulatory, technical, and public attitude barriers that currently prevent the widespread movement of health data and IT services to the cloud. Cloud computing in healthcare can dramatically improve resilience and also support the deployment of new real-time analytical techniques such as AI-enabled risk stratification or alerting

3 There is a need to effectively model the impact of IT incidents across local, regional and national systems, understand how incidents may affect the business continuity of individual organisations, and how this may in turn affect patients and neighbouring healthcare providers

4 Adopt the principles of enterprise architecture into cyber security. The enterprise needs to be controlled and monitored appropriately. The impact of every data end point, be it IoT or EHR, needs to be considered in an enterprise context. This would have helped many organisations with WannaCry as they could then isolate and turn off limited segments where issues occurred, reducing impact on 'Business As Usual'

5 A disaster recovery template should developed centrally to help health and care organisations to develop recovery strategies in the event of a cyber attack or IT failure. The strategy should include information for networks, servers, laptops, wireless devices, data and connectivity and these plans should be reviewed regularly as IT needs grow and increase to ensure that the right infrastructure is in place.[53]

8
Research and innovation priorities

Imperial College London
Institute of Global Health Innovation

Summary Points

- There is limited research to increase the resilience of the NHS in the face of a cyber attack
- There is room to develop new evidence-based interventions including technology, behavioural and educational interventions
- Specific funding should be made available for cyber security in healthcare research
- Effects of cyber incidents on healthcare providers and patients have to be formulated and measured for improved operational resilience and business continuity plans
- There is an increasing focus on the relationship between human behaviours and cyber security, especially in healthcare; further research on behavioural patterns along with education is critical

Research priority 1: Understanding the scale and impact of the problem

Prior to the development of complex research objectives it is first crucial to fully understand the basics of a problem; the first overriding research priority must therefore be to develop a better understanding of the scale and impact of cyber incidents and health IT failings on both patients and organisations. This includes:

- To develop and test a methodology for effectively quantifying the scale of cyber incidents and health IT failings across the NHS. This will require a multifaceted approach to ensure the capture of incidents which are currently recorded across multiple systems and sources (e.g. local IT helpdesks, local or national incident reporting systems such as NRLS or centrally to NHS Digital), or more likely not recorded at all. A robust quantification of the scale of the challenge is required to ensure adequate resource is directed towards tackling the threat
- To develop and test a methodology for robustly quantifying the impact of cyber incidents and health IT failings on patients and organisations. The recording of patient harm is a key facet of patient safety and is effectively performed every day in the health sector. There is however currently no established and validated means of identifying the harm caused to patients by health IT failings or cyber incidents. Evaluating harm is required for estimating the scale of the problem, whilst in-depth analysis of specific adverse events will allow the development of new evidence-based strategies to reduce avoidable harm caused by health IT failures.

Research priority 2: Understanding resilience — mapping organisational inter-dependencies and system flow

The WannaCry attack demonstrated how fragile the system is, and how easily patient care can be disrupted by cyber or IT incidents. There is a need to effectively model the impact of IT incidents across local, regional and national systems, understand how incidents may affect the business continuity of individual organisations, and how this may in turn affect patients and neighbouring care providers.

Health systems are becoming increasingly complex and interdependent, and evermore rely on the integration of digital and physical systems; the failure of a single IT system or disruption in one organisation can have considerable secondary effects. For example: what would be the impact on patient flow, hospital demand, and subsequent knock-on effects to other local services across the system if one of the Major Trauma Centres or a major A&E department were closed for a number of days due to an IT failure?

This modelling information is required to inform effective operational resilience and business recovery plans, and target investment at crucial pinch points or critical weaknesses. Much of the NHS is inter-dependent on shared services and technology such as the N3 National Spine, and there is a paucity of understanding about the threats and opportunities this poses. As such there is a further need to establish and model technological interdependencies across services and systems and model the impact of failures in these; if a number of local hospitals share a single operating system or data server this may be a point of critical weakness and as such additional back-up or redundancy systems may be required to prevent widespread disruption in the event of an incident.

Research priority 3: Behavioural research

In the past five years, following significant cyber attacks on corporations, universities, and healthcare entities worldwide, researchers have focused increasingly on the relationship between human behaviours and cyber security. No matter how sophisticated the algorithms and firewalls, it takes only a click for a phishing attack to dismantle an entire network. By nature of virtue, healthcare is one of the critical sectors where the biggest threat to cyber security is from an insider threat; however, this needs to be taken in the context that the healthcare IT systems are often not designed with both quick access by clinical users and robust security measures in mind. Human error and lack of training is a major contributor, but employees may also be abusing their access to systems or data, although in 13% of cases, it's driven by fun or curiosity—for example, where a celebrity has recently been a patient.

This suggests that, when not accounting for attacks that combine malicious intent with accidental user involvement — such as social engineering — measures that control only for breaches resulting from technological attacks may prevent only half or fewer cyber incidents. Public and staff awareness and education must also be a critical part of cyber security protocols across NHS organisations. As more information and more access to medical records becomes available to patients, this will also need to be taken into consideration.

Conclusions

Imperial College London
Institute of Global Health Innovation

Main Conclusions:

- Innovative technology in healthcare presents both opportunities and risks, requiring responsible secure by design approaches
- Based on identified weaknesses and vulnerabilities key practical and scientific measures are suggested to improve NHS cyber resilience
- NHS current cyber security efforts and financial support are just first steps towards a more cyber resilient healthcare and a comprehensive and overarching cyber security strategy has to be developed and pursued

This report is an overview of the state of cyber security for healthcare in England and focusses on the challenges that make healthcare different to other critical sectors. It has covered the following key points:

- Highlighting reasons for NHS's severe cyber vulnerability, including: lack of investment in IT and cyber security, outdated and diverse IT solutions, the need to train staff in security issues
- Summarising the NHS' efforts to increase cyber resilience, including accountability assignments, introducing incident response mechanisms and new investments to improve cyber security functions
- Showing the opportunities and challenges of technical innovations, including connected devices, artificial intelligence, robotics, cloud computing and precision medicine
- Presenting practical and scientific approaches to increase cyber resilience, including: awareness improvement, staff training, resilience and developing a secure infrastructure.

References

1. Martin G, et al. WannaCry—a year on. *BMJ*. 2018;361:k2381.
2. Abelson R, Goldstein M. Anthem hacking points to security vulnerabilities of healthcare industry. *The New York Times*. Available from: https://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html?_r=0.
3. Chinthapalli K. The hackers holding hospitals to ransom. *BMJ*. 2017;357:j2214.
4. Kwang K. SingHealth cyberattack: Committee of Inquiry appointed, report due end-2018. *Channel NewsAsia*. Available from: https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-committee-of-inquiry-appointed-report-due-10557724.
5. Coventry L, Branley D. Cyber security in healthcare: a narrative review of trends, threats and ways forward. *Maturitas*. 2018;113: 48-52.
6. HM Government. *National Cyber Security Strategy 2016-2021*. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
7. Cavelty MD. Cyber-Security. In: Burgess JP, *The Routledge Handbook of New Security Studies*, 154-162. London: Routledge; 2010.
8. Jiang J, Bai G. Evaluation of causes of protected health information breaches. *JAMA Intern Med*. 2019;179(2): 265-267.
9. National Cyber Security Centre. NCSC Glossary. Available from: https://www.ncsc.gov.uk/glossary.
10. NHS Digital. *Cyber Security Glossary*. Available from: https://digital.nhs.uk/services/data-and-cyber-security-protecting-information-and-data-in-health-and-care/cyber-and-data-security-policy-and-good-practice-in-health-and-care/cyber-and-data-security-resources/cyber-security-glossary.
11. Bai G, Xiang J, Flasher R. Hospital risk of data breaches. *JAMA Int Med*. 2017;177(6): 878-880.
12. Department of Health and Social Care. The Network and Information Systems Regulations 2018: Guide for the health sector in England. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/706613/network-and-information-systems-regulations-2018-health-sector-guide.pdf.
13. Lord R. The real threat of identity theft is in your medical records, not credit cards. *Forbes*. Available from: https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/#2e2b0d2c1b59.
14. Martin et al. Cyber security and healthcare: how safe are we? *BMJ*. 2017;358:j3179.
15. Smart W. Lessons learned review of the WannaCry ransomware cyber attack. London: Department of Health & Social Care, 2018. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-WannaCry-ransomware-cyber attack-cio-review.pdf
16. Halliday J. Sir Alex Ferguson: hospital apologises after staff 'spied' on medical records. *The Guardian*. Available from: https://www.theguardian.com/football/2018/dec/03/sir-alex-ferguson-salford-royal-hospital-apologises-staff-spied-records.
17. Hoeksma J. ICO warns NHS staff that unlawfully accessing patient records is an offence. *Digital Health*. Available from: https://www.digitalhealth.net/2017/08/ico-warns-nhs-staff-that-unlawfully-accessing-patient-records-is-an-offence/.
18. Ornstein C. Celebrities' medical records tempt hospital workers to snoop. *NPR*. Available from: https://www.npr.org/sections/health-shots/2015/12/10/458939656/celebrities-medical-records-tempt-hospital-workers-to-snoop?t=1552824049899.
19. Ghafur S, Grass E, Jennings NR, Darzi A. The challenges of cyber security in health care: the UK National Health Service as a case study. Lancet Digital Health 2019; 1: e10–12
20. https://digital.nhs.uk/services/data-security-centre/threat-advice-and-intelligence
21. Hughes O. NHS trusts fail post-WannaCry cyber security checks. *Digital Health*. Available from: https://www.digitalhealth.net/2018/02/nhs-trusts-fail-post-WannaCry-cyber security/.
22. Department of Health and Social Care. Securing cyber resilience in health and care. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf.
23. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. *Official Journal of the European Union*. 2017;(6): 1-176.
24. Department of Culture, Media and Sport, 2018. Code of practice for consumer IoT Security. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf
25. https://www.medicaldevice-network.com/news/medical-scans-cyber security-study/
26. Department of Health and Social Care. Code of conduct for data-driven health and care technology. Available from: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology.
27. European Commission. GrowMeUp. Available from: https://cordis.europa.eu/project/rcn/194088/factsheet/en.
28. Gaskell A. Are robots about to enter the healthcare workforce? *Forbes*. Available from: https://www.forbes.com/sites/adigaskell/2019/01/07/are-robots-about-to-enter-the-healthcare-workforce/#95ab62328aea.
29. Sullivan T. HIMSS Analytics delivers a state of the health IT industry report. *Healthcare IT News*. Available from: https://www.healthcareitnews.com/news/himss-analytics-delivers-state-health-it-industry-report.
30. Haimboeck-Tichy A. Cloud computing; is it the treatment for our over-burdened NHS? *IBM* website. Available from: https://www.ibm.com/blogs/think/uk-en/cloud-computing-is-it-the-treatment-for-our-over-burdened-nhs/.
31. IBM. Arthritis Research UK delivers reliable virtual assistant on IBM Cloud. Available from: https://www.ibm.com/blogs/cloud-computing/2018/07/10/arthritis-research-uk-virtual-assistant/.
32. Comstock J. Why healthcare data may be more secure with cloud computing. *MobiHealthNews*. Available from: https://www.mobihealthnews.com/content/why-healthcare-data-may-be-more-secure-cloud-computing.
33. Perry Y. Cloud computing in healthcare with cloud volumes ONTAP. *NetApp* website. Available from: https://cloud.netapp.com/blog/benefits-of-cloud-computing-in-healthcare.
34. Afia Health. Advantages of cloud computing for healthcare. Available from: https://afiahealth.com/advantages-of-cloud-computing-in-healthcare/.
35. Ismail N. How cloud technology is transforming the healthcare industry. *Information Age*. Available from: https://www.information-age.com/cloud-technology-transforming-healthcare-industry-123472352/.
36. Bateman K. Top cloud security risks for healthcare. *Information Age*. Available from: https://www.information-age.com/cloud-security-risks-healthcare-123471521/.
37. Solutions Review. 8 benefits and risks of cloud computing in healthcare. Available from: https://solutionsreview.com/cloud-platforms/8-benefits-and-risks-of-cloud-computing-in-healthcare/.
38. NHS Digital. NHS Digital publishes guidance on data off-shoring and cloud computing for health and social care. Available from: https://digital.nhs.uk/news-and-events/latest-news/nhs-digital-publishes-guidance-on-data-off-shoring-and-cloud-computing-for-health-and-social-care.
39. Snell E. Utilizing cloud computing for stronger healthcare data security. *Health IT Security*. Available from: https://healthitsecurity.com/features/utilizing-cloud-computing-for-stronger-healthcare-data-security.
40. National Human Genome Research Institute. DNA sequencing costs: data. Available from: https://www.genome.gov/about-genomics/fact-sheets/DNA-Sequencing-Costs-Data.
41. Genomics England. The 100,000 genomes project. Available from: https://www.genomicsengland.co.uk/about-genomics-england/the-100000-genomes-project/.
42. Turnbull C. The 100 000 Genomes Project: bringing whole genome sequencing to the NHS. *BMJ*. 2018;361:k1687.
43. Phillips AT. Is UK genetic information at risk from hackers? *TechFruit*. Available from: https://techfruit.com/2018/08/28/is-uk-genetic-information-at-risk-from-hackers/.
44. UK Biobank ramps up whole genome sequencing. *The Horizons Tracker*. Available from: http://adigaskell.org/2018/05/08/uk-biobank-ramps-up-whole-genome-sequencing/.
45. Hughes O. Genomics England says DNA data not moved due to hacking attempts. *Digital Health*. Available from: https://www.digitalhealth.net/2018/12/genomics-england-dna-data-hacking-attempts/.
46. Jay J. Hackers mounting cyber attacks to access DNA data of thousands of Brits. *TEISS* website. Available from: https://www.teiss.co.uk/threats/hackers-dna-data-brits/.
47. Rizkallah J. Hacking humans: protecting our DNA from cybercriminals. *Forbes*. Available from: https://www.forbes.com/sites/forbestechcouncil/2018/11/29/hacking-humans-protecting-our-dna-from-cybercriminals/#291b7f5b5287.
48. Brown KV. Hack of DNA website exposes data from 92 million accounts. *Bloomberg*. Available from: https://www.bloomberg.com/news/articles/2018-06-05/hack-of-dna-website-exposes-data-from-92-million-user-accounts.
49. Molteni M. Genome hackers show no one's DNA is anonymous anymore. *Wired*. Available from: https://www.wired.com/story/genome-hackers-show-no-ones-dna-is-anonymous-anymore/.
50. Gymrek M. Identifying personal genomes by surname inference. *Science*. 2013;339(6117):321-4.
51. Ossola A. Welcome to the future, a place where everyone knows your genetic code. Available from: https://futurism.com/genetic-privacy-hacking.
52. Royal Academy of Engineering. Cyber safety and resilience strengthening the digital systems that support the modern economy. Available from: https://www.raeng.org.uk/publications/reports/cyber-safety-and-resilience.
53. Sittig DF, Singh H. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Appl Clin Inform. 2016;7(2):624–632. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4941865/

Cite as: Ghafur, S., Fontana, G., Martin, G., Grass, E., Goodman, J., & Darzi, A. (2019). Improving Cyber Security in the NHS. London: Imperial College London.

Imperial College
London

Institute of
Global Health Innovation