bsi.

...making excellence a habit.™

Cybersecurity in the age of Telemedicine

A BSI white paper

The risks of cyberattack in numbers

30,000

malicious emails were sent to the NHS in March and April 2020

6,000%

increase in 'Phishing' attached related to Covid in March and April 2020

51,910

signs of malicious activity were notified to the NHS by the end of August 2020

595

general practices were infected by the 2017 Wannacry cyber attack

1%

of total NHS activity was directly affected by Wannacry

10%

of all UK healthcare organisations have been breached more than 10 times in the last year

Contents

1 Introduction

2 Why is cybersecurity so important in primary healthcare right now?

3 What could a cybersecurity breach mean for healthcare providers?

4 How does remote working and telemedicine affect cybersecurity risk?

5 Who is responsible for cybersecurity in primary care?

6 Mitigation of cybersecurity risks

7 Education and standards

8 Conclusion

9 Resources

10 References

1. Introduction

The NHS experienced the havoc a cyber-attack can cause in 2017, when hackers brought parts of the health service to a halt with a ransomware attack that froze online records. The SARS-Cov-2 pandemic has heightened the potential risk, with heavy reliance on digital healthcare, many more staff working from home, and rapid adoption of remote consultations.

And the threat affects not just the NHS, but healthcare systems worldwide. Cyber attacks in Germany and Finland in 2020 have already shown some of the damage that can be caused by cybercriminals during a pandemic. The US in particular has seen a significant increase in attacks, and within private facilities there is a lack some of the organisational protection the NHS provides.

> SARS-Cov-2 both raises the possible impact of a cyber attack, and increases the likelihood of it happening.

The very real threat of a cyber-attack leading to a 2017-style melt-down in the middle of a pandemic exists. But inability to access services would only be the beginning. Hackers have already published stolen sensitive mental health records online. There's the possibility of deliberate data corruption, for example by mixing up test results. Even the temperature controls for freezers storing SARS-Cov-2 vaccines could be hacked.

Whilst the risks are high, some of the mitigation can be reassuringly simple. Ensuring staff know about and comply with the basics of cyber-hygiene is one of the most important ways to reduce risk. And there is a wealth of advice and support to help organisations improve their cybersecurity posture.

2. Why is cybersecurity so important in primary healthcare right now?

Cybersecurity, according to the UK's National Cyber Security Centre (NCSC), is 'how individuals and organisations reduce the risk of cyber attack.' Cybersecurity should 'protect the devices we all use and the services we access from theft and damage' and 'prevent unauthorised access to the vast amounts of personal information we store on these devices and online'.

For healthcare organisations, this means that all data stored digitally – everything from medical records to staff bank account details – is kept secure, so it can only be accessed, used or changed by those authorised to do so.

SARS-Cov-2 both raises the possible impact of a cyber attack, and increases the likelihood of it happening.

With unprecedented demand on healthcare, the impact of service disruption on the scale seen in 2017 could be devastating. Acute services in particular are under strain, and there is no slack in the system to divert patients away from affected hospitals. In addition, while some face-to-face care was possible without access to digital technology in 2017, the majority of healthcare is now reliant on digital technology.

Cybercriminals have tried to take full advantage of the pandemic. NCSC reported a significant uptick in phishing attacks during the SARS-Cov-2 pandemic.

Phishing attacks are opportunistic mass emails asking for sensitive information, encouraging people to open attachments or visit a fake website which runs malicious software on the victim's machine. The aim is to harvest all information, such as login details to systems holding valuable data, or bank details. This information is very often resold on the dark web for a fee. An average stolen data set is worth about £20 per record; clinical data can be worth up to £100 per record.

Adoption of remote and online working at speed significantly increases the risks by staff using their own devices (phones, tablets or laptops); working in new ways in potentially less secure environments; and using unfamiliar technologies such as teleconferencing for remote care provision.

In addition, moves beyond the clinical commissioning group structure of primary care towards new partnerships at local level will introduce new ways of working. Integrated care partnerships will bring together commissioner and provider NHS bodies with local authorities and others to focus on population-level health – such as Infection Control during infectious disease outbreaks. This will inevitably mean more data sharing across organisations. While data sharing is vital to allow these partnerships to flourish, the sharing of unsecured data and reliance on potentially vulnerable information systems does expose gaps in cybersecurity which can be exploited by hostile actors or 'hackers', as they are more commonly referred to.

Hackers can launch attacks by sending phishing emails or releasing code that exploits loopholes in software. The purpose is the same – to gain access to or disrupt data and systems.

Cybercriminals have tried to take full advantage of the pandemic. NCSC reported a significant uptick in phishing attacks during the SARS-Cov-2 pandemic.

3. What could a cybersecurity breach mean for healthcare providers?

A breach of cybersecurity means criminals can access, freeze, manipulate and publish data. For a primary healthcare facility, this could include:

- **blocking access to email, online appointment booking and triage systems, patient records, staff rotas and contact details**
- **manipulating or corrupting data, for example removing 'red flag' alerts from clinical records, changing test results**
- **publishing confidential clinical records**

In 2017, the NHS was infected by ransomware, malicious software which froze clinicians' access to the data, in the Wannacry attack. Affected users in Primary and Secondary care were unable to access patient records, online diagnostics, appointment booking systems and emails. The hackers issued a ransom demand, in an attempt to extort money to unlock the files. Wannacry type ransomware attacks have continued to evolve with Ryuk emerging as the most damaging in 2020.

The NHS was not targeted specifically, this was a wholly opportunistic incident, but it did expose Primary and Secondary care as 'soft-targets' for such attacks. It was one of many organisations to fall victim of the attack, which exploited weaknesses in software operating systems. Although a patch (effectively an update) for the weakness had been rolled out, it had not been installed on some devices, while others were running old, unsupported systems that could not be patched.

Even so, the attack caused widespread disruption. Some hospitals and practices had to temporarily close to admissions and cancel outpatient clinics while hundreds of machines were checked, disinfected and clean back-ups restored.

Dr Saira Ghafur, digital health lead at the Institute of Global Health Innovation, Imperial College London, says: 'We've got a lot better [since 2017] in terms of phishing emails and educating staff and having systems in place to recognise them and filter them. But any cyber-attack in the middle of a pandemic would be absolutely catastrophic, if you had Wannacry hit a London trust or GP surgeries, when you are already struggling to provide good care [because of the impact of SARS-Cov-2].'

Jonathan Lee, UK director of Public Sector Relationships at digital security software provider Sophos, says at least one death has already happened as a result of a ransomware attack. 'A German hospital recently had a ransomware attack and there was a patient on the way to the Emergency Department in an ambulance. This person was diverted to another hospital and they sadly died in the ambulance. It's the first known incidence of someone dying because of a malware incident at a hospital.'

Today, the potential impact is even greater than 2017. As Dr Ghafur points out: 'If you think about what happened in Wannacry, it would be very difficult now because everything, every bit of healthcare we are delivering has some digital element to it.'

Three years ago, some departments reverted to pen and paper to manage the inability to access patient records or diagnostics. Now, with almost all records and imaging digitised, many staff working remotely and appointments and triage managed online, it is hard to see how that could happen.

On the other hand, the NHS has made big changes to improve cybersecurity since the attack. Daniel Taylor, who was at the time Director of Data Science at NHS Digital and is now Associate Partner in Health and Life Sciences at IBM, says: 'Unfortunately it often takes a major incident to make an improvement. Ultimately Wannacry 2017 was a shock to the system... we saw the impacts to patient care; we saw organisations go on divert. You just have to look at the investment there's been since.' He pointed to NHS Digital's data security centre, which he says is now much better at 'identifying issues and risks and helping organisations improve and manage those risks.'

3. What could a cybersecurity breach mean for healthcare providers?

Targeted attacks

The NCSC reports an increasing trend for cybercriminals to target healthcare organisations specifically because they hold personally-identifiable, sensitive information about patients.

'The NCSC has identified a new disturbing trend in ransomware attacks which sees attackers not only withholding access to the data but also threatening to publish it unless the ransom is paid,' said a spokesman for the centre.

In Finland in October 2020 an attack on a private company which runs psychotherapy services resulted in confidential treatment records of tens of thousands of patient being hacked. Patients were sent emails demanding money to prevent records of their confidential discussions with therapists being published online. Some records have been published, causing severe distress and a loss of trust.

The incident has been blamed on lack of reliable encryption of data files stored by the company. 'That's why data needs to be encrypted at rest,' says Mr Lee. 'It's imperative that personally identifiable clinical data is kept secure.'

Increasing reliance on digital information increases the risk of data being corrupted for malicious purposes.

'It's all ways of hacking and attacking data,' says Dr Ghafur. 'If you rang up a hospital and said, 'every other blood result has been tampered with', what proof does the hospital have that it's not? And what is your back up, how would you test again, what does that mean for the samples you stored?' she asks. The possibility of tampering with test results underlines the potential harm that could be caused.

'Integrity of data has become more and more important,' says Mr Taylor, and even more so for healthcare than – for example – the often-targeted financial services industry. 'If my adverse drug reaction for Penicillin is taken off the system, then the outcome for me is much worse than not being able to access my bank account.'

Dr Ghafur raises the possibility of other nightmare scenarios. Researchers in Israel last year demonstrated the ability to intercept digital images from medical scans and make changes which would change the diagnosis – for example adding or deleting signs of cancer by changing pixels on the scan. The researchers speculated that attackers could use this technology 'to sabotage research, commit insurance fraud, perform an act of terrorism, or even commit murder.'

Mr Taylor says that 74% of the 2.6 million people who attend Emergency Departments each year require diagnostics – and that usually means digital imaging. 'When you consider that all imaging is digital in the NHS, if an organisation loses its imaging department, it loses the ability to treat patients in the Emergency Department,' he says. He believes making clear the quantifiable impact of cybersecurity threats is important to ensure they are taken seriously.

The Internet of Things, which allows remote, digital control of systems such as fridges and freezers, could be another target. 'We've got these new vaccines coming on board, so how easy would it be if you had that dark mindset – which these people unfortunately do – to potentially hack into the thermometers for freezer or fridges that the vaccines are stored in?' asks Dr Ghafur.

> The NCSC reports an increasing trend for cybercriminals to target healthcare organisations specifically because they hold personally-identifiable, sensitive information about patients.

4. How does remote working and Telemedicine affect these risks?

2020 saw huge shifts in working practices. Working from home has been possible thanks to widespread adaptation of technology. However, this also opens up the potential for significant security incidents.

Dr Ghafur points out that everyone is more vulnerable to making mistakes when adopting new working practices: 'people are not used to delivering care in this way'. Part of the problem, she says, is that working from home means you are responsible for security precautions that your workplace usually provides.

These include ensuring your work laptop, tablet or smartphone is only used online with a secure connection to your wi-fi; remembering that you are not behind the institutional firewall so more phishing emails may get through, and taking responsibility for the physical security of your devices.

Phishing attacks have become far more targeted and sophisticated, says Mr Taylor. 'It isn't the 'I've got £10,000 in a Nigerian bank account' approach that was prevalent five years ago. It's very much more that they know who you are, the area you come from, your interests,' he says. He is concerned that people working under increased pressure, in new working environments, working in new ways, may be more vulnerable to such attacks.

Home working can raise particular security problems for people working from shared households, who may not have secure, private workspaces. Even if people do have a home office, the different mindset engendered by working from home can mean people take risks they would not take in a public workspace.

'Everyone who works in the NHS, whether it's paper records or e-health records, we're all custodians of patient data,' Dr Ghafur points out. 'You would never leave a patient list lying around your home, especially if you've got people sharing households. In the same way, you shouldn't leave your laptop.'

Laptops, tablets and other devices are vulnerable to physical burglary from home as well. And if the device hold unencrypted patient information, that could lead to a serious breach of data security as well as a loss of property.

> ... people working under increased pressure, in new working environments, working in new ways, may be more vulnerable to such attacks.

Personal devices

Early in the pandemic, GPs reported that they and their staff often had to use their own devices, such as smart phones, tablets or laptops, because of a shortage of practice devices suitable for remote working. While personal devices can be made secure, this is not best practice or recommended. Devices need to have up to date, high quality virus and malware protection, to have security patches applied as they are released, and to be using up-to-date operating systems. They also need an industry standard level of encryption, so that if the device was compromised, the data contained within it cannot be read.

'Can you rely on people to do it individually?' asks Dr Gafur. 'If you've got a device issued by a provider then you would expect all of those protections to be installed and to have the most up-to-date operating system as well.'

Mr Lee adds: 'Ideally you would want to be using an NHS device to access the data because then you've got all the safeguards, for example VPNs [virtual private networks] in place so you've got encrypted traffic between your machine and wherever you're viewing that identifiable patient data. Obviously, you don't want to store patient data on your machine in case it's lost.'

4. How does remote working and Telemedicine affect these risks?

Video consultations

Before the pandemic, the vast majority of care was provided in person, with patients travelling to GP surgeries or outpatient clinics. Within weeks, that flipped completely, with most care now being delivered remotely, a significant proportion of it by teleconsultation. But how secure are teleconsultations? With phenomena such as 'Zoom-bombing' where unauthorised people have gained access to private meetings, how confident can patients be that their consultation is truly private?

In the early days of the pandemic, clinicians were encouraged to use whatever worked to get services up and running. While consumer software like the video-conferencing platforms Zoom and Skype can be made secure, they are not necessarily secure by default.

An NCSC spokesperson said: 'For NHS GP teleconsultations, platforms provided by practices' IT system suppliers should be used.'

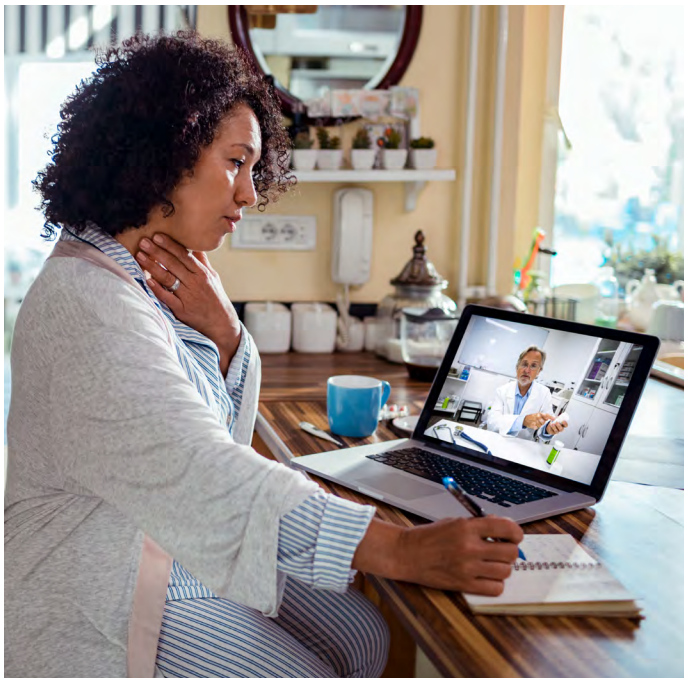
In Scotland, the NHS Near Me video consultation system was already up and running for hospital outpatient appointments and has been scaled up to offer GP appointments.

In England, NHS Digital's website provides information and advice on video consultations, including approved suppliers. However, the website also states: 'It's fine to use video conferencing tools such as Skype, WhatsApp and Facetime as well as commercial products designed specifically for this purpose, particularly as a short-term measure.' Now that we are in 2021, the short-term solutions no longer apply.

> ... how confident can patients be that their consultation is truly private?

Mr Lee says people using these tools need to ensure they are correctly configured. 'All of the platforms have their own security systems that clinicians should be aware of and should be advised on by their IT departments. They are not inherently insecure, they just need to be configured properly,' says Mr Lee. Safeguards include using different URLs and IDs for each consultation, using passwords and access controls.

In addition, says Dr Ghafur, managers need to ensure that staff have somewhere secure and private to work, where calls will not be overheard – not always the case for people working from shared accommodation. Allowing staff to access the clinic or practice to carry out their consultations may be necessary.



5. Who is responsible for cybersecurity in Primary Care?

Everyone working in the NHS has responsibility for the security of the data they are working with – as Dr Ghafur says, 'we are all custodians of patient data'. At a regional level, the arms-length bodies NHS Digital and NHS X are responsible for providing technical support and guidance to NHS providers in England. In Scotland, the responsibility falls to Digital Health and Care Scotland, which published a strategy setting out data protection requirements in 2018. The NHS Wales Informatics Service manages cybersecurity for Wales and the Department of Health in Northern Ireland covers similar ground through its records management processes.

However, it is less obvious who takes responsibility for what at local level. NHS X says these responsibilities are outlined in the document Securing Excellence in Primary Care Digital Services.

The document states that:

- **clinical commissioning groups are responsible for 'enabling services' such as cyber security and information governance, providing support on data breaches and management of incidents**
- **clinical commissioning groups are responsible for assuring the 'cyber security responsibilities of all providers' including GP IT partners**
- **clinical commissioning groups are responsible for data processing, either directly or through NHS-commissioned suppliers**
- **locally commissioned providers are responsible for completing a data protection and security toolkit (DPST), and achieving set standards, and for data processing responsibilities**
- **GP contractors are responsible for data controlling, GDPR, and to register for urgent alerts.**

NHSX also says that CCGs and general practices, like other NHS organisations in England, are required to complete an online self-assessment tool, the Data Security and Protection Toolkit, to 'provide assurance that they are practicing good data security and that personal information is handled correctly.'

Mr Lee believes more clarity is needed about who is responsible for what at Primary Care level.

'I don't think it's clear,' he said. He said that the 'individual GP' was unlikely to have the expertise to complete the DSPT and that most would rely on commissioning services to buy in IT. 'Quite where the risk sits on that is open to debate,' he says. 'It is a concern.'

It is also less clear where responsibility sits, for example, in integrated care networks or services, where people work across organisations. 'Technology can be a real enabler in terms of passing your data about you as a patient around, but that data needs to be secure in transit... It's more of a collaboration rather than an organisation that owns it. It is ultimately a question of who is accountable?' says Mr Lee.

As primary healthcare evolves, this may become more of an issue. Integrated care services – partnerships that bring together providers and commissioners across the purchaser-provider split – will involve not just NHS bodies, but local authorities and potentially other local agencies. As healthcare moves beyond clinical commissioning groups, integrated partnerships are likely to become the new normal. Establishing where responsibility for cybersecurity standards sits, especially where non-NHS bodies are involved, will become ever more important. At present, these voluntary partnerships have no formal accountabilities.

NCSC says: 'IT equipment in NHS general practice is provided through a national framework for clinical systems and at a regional level for the underlying IT infrastructure. This is organised by NHSX and NHS Digital.' Their spokesperson adds: 'While individual practices have responsibility for following best practice in their use of IT systems, NHS-provided systems will already be configured to be 'secure by default'.'

> Establishing where responsibility for cybersecurity standards sits, especially where non-NHS bodies are involved, will become ever more important.

6. Mitigation of cybersecurity risks

Many of the risks outlined can be managed by basic cyber-hygiene. While nothing can guarantee that an attack won't happen, following the basics of cyber hygiene can substantially reduce the risk. Good cybersecurity means applying layers of security measures in case one fails.

'By adopting a layered approach, organisations can make themselves a less attractive target to attackers and reduce the chances of an attack being successful,' says an NCSC spokesperson.

Physical security

Healthcare providers need to ensure the physical security of devices used to process or store sensitive information, such as laptops, tablets and smart phones. An NCSC spokesperson warns of 'an increased likelihood of devices being stolen or lost while working from home.'

Users need to be educated to lock devices away securely when not in use. Removable devices such as USB memory drives should never be used to store clinical information.

Staff should be discouraged from lending their device to others – for example to their children to play computer games – due to the risk of loss or infection of the device with malware.

.

Safe information storage

Healthcare providers should ensure the information stored on devices is protected, so if devices are lost or stolen, the information cannot be compromised. 'It's vital for organisations to check their devices encrypt data while at rest, so that people who shouldn't have access to data don't have access,' said the NCSC spokesperson.

Measures may need to include the ability to remotely 'wipe' data from devices, should they be lost or stolen. This is easier if all staff are using devices purchased and provided by the healthcare organisation, rather than using their own personal devices.

Mr Lee says organisations' IT professionals need 'real-time visibility' of the devices people are using, so they can spot anomalous activity early and respond to it remotely if need be.

In addition, providers need to ensure that devices themselves are not compromised, by installing and updating industry-standard antivirus and anti-malware protection and ensuring patches and updates to software are installed promptly.

.

6. Mitigation of cybersecurity risks

Safe use of information systems

Healthcare providers need to ensure the systems used to access information are kept secure. Effective access controls, such as requiring strong and regularly changed passwords and two-step authentication, are recommended.

The spokesperson from NCSC says: "The NCSC strongly recommends organisations use virtual private networks (VPNs) to allow remote users to securely access your organisation's IT resources. If VPNs are already in use, then organisations should ensure they are fully patched.'

However, systems only work as well as the staff using them. It's important that users only log onto systems when they are needed, log out afterwards, and do not leave unlocked devices unattended. Staff need to be educated not to share login details or passwords or make them easy to find.

Education is also important to help staff recognise phishing emails seeking access to information systems.

'Phishing is still a big way for cybercriminals to try to breach your organisation,' says Mr Lee. 'Educate your users in what an attack that tries to get hold of their credentials looks like, by providing some training or some sort of simulation tools that can catch people out – then people can learn from their experiences and that is really valuable.'

Mr Lee makes the point that patients, too, are at risk of phishing attacks, which may pretend to come from their GP. 'It's important for patients as well – is this email from your GP, how will the GP communicate with you? What is that communication going to look like?'

Even basic things like ensuring you are connected to a secure Wi-Fi network are important for staff working from home. Mr Lee encourages people to set a new Wi-Fi password, rather than relying on the default password. This can make it harder for hostile actors to access the systems you are logging into.

7. Education, support and standards

The NCSC provides a range of educational tools and advice via their website, which can help small organisations such as general practices test their cyber-resilience and educate staff in cyber-hygiene. The Cyber Essentials framework can be used by organisations with limited experience of cyber security to improve their defences and demonstrate publicly their commitment to cyber security. For larger organisations, the centre's Exercise in a Box toolkit allows them to test their resilience and security in a simulation exercise.

The NHS Data Security and Protection Toolkit is designed to allow organisations to check their performance against the 10 Data Security Standards set out by the National Data Guardian.

NHS Digital published guidance on remote working for general practice staff in England in March 2020 and NHSX has advice on how to safely manage staff use of personal devices.

Adherence to standards also allows organisations to demonstrate to customers and patients that they take cybersecurity seriously. For organisations wishing to show this at a higher level, the International Standards Organisation's Information Security Management ISO 27001 is still viewed as the gold standard for cybersecurity.

8. Conclusion

Healthcare providers are not technology companies – however increasingly everything they do is underpinned by technology, and never more so than in today's digital world. Cybersecurity underpins safe patient care, the reputation of the healthcare organisation, and the trust patients place in it. If the technology fails, the healthcare organisation will fail too.

The huge strides in Telemedicine made in 2020 have allowed the NHS to continue to function. Protecting all aspects of healthcare information from theft, breaches or corruption will ensure that healthcare services can not only continue to function, but to thrive.

Ensuring cybersecurity systems are in place, and staff are educated and supported to use them, is an essential part of healthcare management today.

9. Resources

NCSC information for users about spotting and reporting suspicious 'phishing' emails: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

NCSC Cyber-essentials information for organisations: https://www.ncsc.gov.uk/cyberessentials/advice

NHSX Remote working in primary care: guidance for GP practices during COVID-19 emergency response: https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/03/C0165-remote-working-in-primary-care-gp-practices-during-covid-19-v1.2.pdf

NHS Digital. Data Security and Protection Toolkit: https://www.dsptoolkit.nhs.uk/

BSI Cybersecurity and information resilience service: https://www.bsigroup.com/en-GB/our-services/cybersecurity-information-resilience/

10. References

National Cyber Security Centre Annual Review 2020. Available at: https://www.ncsc.gov.uk/files/Annual-Review-2020.pdf

NHS Improvement, Lessons learned review of the WannaCry Ransomware Cyber Attack, published February 2018. Available at: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf

National Cyber Security Centre What is Cyber Security? Available at: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

The Guardian, 'Shocking' hack of psychotherapy records in Finland affects thousands. Available at: https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

Y Mirsky et al, CT-GAN: Malicious tampering of 3D Medical Imagery using Deep Learning. Published in the 28th USENIX Security Symposium (USENIX Security 2019). Available at: https://arxiv.org/pdf/1901.03597.pdf

Is primary care ready to switch to Telemedicine? Medscape UK, March 2020. Available at: https://www.medscape.com/viewarticle/927631

NHS Digital, Advice on using video consultation systems. Available at: https://digital.nhs.uk/services/gp-it-futures-systems/approved-econsultation-systems

NHS England, Securing Excellence in Primary Care Digital Services. https://www.england.nhs.uk/wp-content/uploads/2019/10/gp-it-operating-model-v4-sept-2019.pdf

NCSC, About Cyber Essentials. Available at: https://www.ncsc.gov.uk/cyberessentials/overview

NCSC, Exercise in a Box toolkit. Available at: https://www.ncsc.gov.uk/information/exercise-in-a-box

NHS Digital, Data security and protection toolkit. Available at: https://www.dsptoolkit.nhs.uk/

Department for Health and Social Care, 10 Data Security Standards. Available at: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/national-policy/

NHS X, Remote Working in Primary Care Guidance for GP Practices during COVID-19 Emergency Response. Available at: https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/03/C0165-remote-working-in-primary-care-gp-practices-during-covid-19-v1.2.pdf

NHS X, Bring your own device policy. Available at: https://www.nhsx.nhs.uk/key-tools-and-info/procurement-frameworks/clinical-communications-procurement-framework/bring-your-own-device-policy/

International Standards Organisation, Information security management ISO/IEC 27001. Available at: https://www.iso.org/isoiec-27001-information-security.html

Why BSI?

Expertise lies at the heart of what we do. As trusted advisors of best practice, we empower you to keep your business safe through a diverse portfolio of information security solutions. Whether it's certification, product testing, and consultancy services or training and qualifying your people, we can help you achieve your cybersecurity goals.

Our products and services

Knowledge

The core of our business centres on the knowledge that we create and impart to our clients. In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top 10 management system standards.

Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of standards.

Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools which help facilitate this process.

For more information on improving your organisation's cybersecurity practices
Visit: **bsigroup.com**
Call: **+44 345 080 9000**

bsi.