ukcloud health

Pure Commitment.

Privacy first: Healthcare digital transformation

Putting the 'Trust' into NHS Trust technology systems by putting privacy first

Summary

The Five Year Forward View, a strategy document issued by NHS England in 2014, clearly describes the challenges facing the UK healthcare community - the demand for better patient experience needs to be achieved at the same time that budgets and resources are increasingly scarce. There is a broad consensus that harnessing innovative technology solutions to facilitate collaboration and improve patient outcomes will be essential if the necessary efficiencies and savings are to be delivered, but this cannot be at the expense of privacy.

UKCloud Health, the specialist healthcare division of UKCloud, recent recipients of the Queen's Award for Enterprise for Innovation, commissioned a survey to gauge the opinions of over 2,000 UK adults. Our research found that the majority of British adults are concerned about the protection of their health data and are most likely to trust secure networks (such as N3, HSCN, PSN) and UK firms (58%) that are exclusively bound by UK data protection law to securely store and process personal data. They are sceptical of the security of non-governmental networks (such as the Internet) and non-UK firms, believing that the Government should seek their permission (82%) before storing and processing their personal data with non-UK businesses.

The research also found that the majority of British adults (55%) say they think the UK Government should prioritise working with UK businesses if the price and service is comparable with non-UK businesses, with one in five (20%) saying they should always work with UK businesses regardless of their price and service. This sentiment is reflected by the Government's view of Social Value and how focusing public expenditure on local firms can benefit the UK economy.

The use of innovative technologies such as cloud computing is a key aspect of the Government's strategy to transform healthcare. In our view, these survey results reveal that public opinion favours a cautious approach to the selection of technology providers, with security and data protection of specific concern to those surveyed. Cloud services, as provided by UKCloud Health, will have a critical role to play in transforming healthcare by accelerating innovation, collaboration and the secure access to sensitive heathcare data. When choosing their cloud providers, healthcare organisations would be prudent to look for ones that not only have a track record of service excellence, but also specialise in working with the unique demands of public services to deliver efficiency gains. The general public would prefer that such cloud providers should be UK-based with UK-sovereign data centres with connectivity to N3 and HSCN.

2,000 UK adults surveyed

Introduction

ukcloud health

Objectives

As part of the launch of UKCloud Health, a division of UKCloud dedicated to the healthcare sector, a research report on data privacy was commissioned, specifically to look at:

- General concerns with data privacy
- Levels of trust for securely storing and processing personal data
- Attitudes to privacy consent
- Attitudes to putting UK firms first when it comes to government business

Methodology

- ComRes interviewed 2044 adults in the UK aged 18+ online between 26th and 27th April 2017.
- Data are weighted by age, gender, socio-economic grade and region to be representative of all GB adults aged 18+.
- ComRes is a member of the British Polling Council and abides by its rules (www.britishpollingcouncil.org). This commits it to the highest standards of transparency.

Table of Contents

Context

- **Data Protection:** If you handle and store information about identifiable, living people – for example, about patients – you are legally obliged to protect that information in compliance with the Data Protection Act 1998. With the NHS the 1997 Caldicott Report highlighted six key principles, and made 16 specific recommendations. In 2012 Dame Caldicott produced a follow up report which made 26 further recommendations including the addition of a seventh principle. In 2016 a further follow-up report was produced following controversy over the 'care data' initiative from HSCIC. In May 2018 new data protection laws will come into force in the UK through the General Data Protection Regulation (GDPR). This will widen the legal definition of what personal data is, for example to include genetic data, and give data subjects new and far reaching rights.

- **Sovereignty:** In the past it might have been sufficient to use a cloud service provider that guaranteed not to store or process data offshore, thereby providing a level of data residency. However recent new laws and regulations in the USA have introduced extraterritorial powers that can compel US-based firms to hand over personal information, even if it is stored in the UK. This means that to ensure full UK data sovereignty you now need to use a cloud provider that not only has UK data centres, but is also a wholly UK owned and registered firm.

Full UK data sovereignty is essential

- **Societal Value:** The Public Services (Social Value) Act 2013 requires people who commission public services to think about how they can also secure wider social, economic and environmental benefits. Before they start the procurement process, commissioners should think about whether the services they are going to buy, or the way they are going to buy them, could secure these benefits for their area or stakeholders. The Act is a tool to help commissioners get more value for money out of procurement. It also encourages commissioners to talk to their local provider, market or community to design better services, often finding new and innovative solutions to difficult problems. A subsequent green paper issued in January 2017, 'Building Our Industrial Strategy', sets out how the government proposes to build a modern industrial strategy post Brexit. Procurement is a key pillar of the government's Industrial Strategy, and social value is embedded in the government's procurement proposals.

- **Secure Government Networks:** There are a number of secure government networks that facilitate the exchange of sensitive data between various public sector organisations such as Local Authorities (PSN – the Public Services Network) and NHS organisations (N3 – the NHS National Network). Although the Internet is increasingly used to connect with non-public sector users such as patients, NHS Digital remains committed to a next generation Health and Social Care Network (HSCN) to replace the N3. According to NHS Digital, HSCN has been designed to "provide a reliable, efficient and flexible way for health and care organisations to access and exchange electronic information, while at the same time reducing costs and complexity, standardising networks, enabling service sharing, and extending the parameters of collaborative working."

Overview:

Public sector organisations are all too familiar with the never-ending challenge of 'doing more for less'. The same is true in the healthcare sector where innovation and collaboration are increasingly required to improve patient outcomes whilst reducing waste, inefficiency and cost. Not only are we seeing collaboration between public and private sector organisations, but also between firms in different sectors like Health & Care, Research & Life Sciences and Pharmaceuticals. In addition we are seeing further collaboration between these healthcare firms and their technology providers.

The NHS is facing significant funding gaps and efficiency challenges relating to the broader austerity agenda, requiring savings of more than £30bn by 2021, so such innovation and collaboration is essential. In many areas it requires truly new ways of working, as simply slashing budgets or cutting corners would reduce service capacity while also putting patient safety and privacy at risk.

Cloud Penetration Statistics (% of workloads)
CLOUD PENETRATION IN UK PRIVATE SECTOR: ~20%
CLOUD PENETRATION IN UK CENTRAL G'OVT: ~10%
CLOUD PENETRATION IN NHS & HEALTHCARE: ~2%

Cloud computing is a technology that has already enabled similar transformation across other industries and the wider public sector. The Digital by Default policy, enabled by cloud technology, has already delivered dramatic results in central government integrated vehicle and driver records at the DVLA enabling it to dispense with tax disks and paper counterpart driving licences, and with HMRC able to collect tax return data online. Indeed, digitisation, the pooling of central government resources and the movement of workloads to the cloud has resulted in £600 million in savings, leading to the UK being recognized by the United Nations as the most digitally advanced government in the world.

One of the main inhibitors to moving systems to the cloud has been fears about security and privacy. In research conducted by ComRes for UKCloud Health, 2,044 UK adults were interviewed aged 18+ online between 26-27 April 2017, to see how the general public felt about data protection.

The research found that the majority of UK adults are concerned about whether their personal data (e.g. financial/ tax records or criminal records) (75%), personally identifiable data (e.g. date of birth or address) (72%), and health records (e.g. medical history or social care records) (65%) are protected by companies and public services.

Patient-identifiable Data (PiD): Guidelines
PERSONAL INFORMATION THAT A TRUST HOLDS INCLUDES ANY CONFIDENTIAL INFORMATION WHICH IDENTIFIES A LIVING PERSON, THIS MAY THEREBY BREACH THEIR RIGHT TO PRIVACY OR PRESENT A RISK OF IDENTITY THEFT IF LOST OR INAPPROPRIATELY SHARED. THIS APPLIES TO DATA RELATING TO PATIENTS, STAFF AND ANY OTHER PARTIES. IT DOES NOT APPLY TO IDENTIFIABLE DATA ALREADY IN THE PUBLIC DOMAIN.

Overall the level of concern about privacy and protection of these kinds of personal information was far greater than for Social Media content (e.g. Facebook posts). Obviously when it comes to Patient-identifiable Data (PiD) guidelines already exist to address many of these concerns and further regulation in the form of the General Data Protection Regulation (GDPR) will also be adopted in the UK from May 2018.

In seeking efficiencies and cost savings from moving to the cloud, firms obviously need to take public privacy concerns and regulatory requirements into account. This also applies in terms of which networks and service providers they use to store and process personal data.

The research found that the majority (63%) of British adults would be likely to trust secure government networks (not on the internet) to securely store and process personal data.

It also found that the majority (58%) of British adults would trust UK-based businesses (bound by UK data protection law) to securely store and process personal data, while just 15% would trust non-UK businesses

There are a number of cloud service providers vying for business in the healthcare sector. Many of them are large US-based multinationals that have limited accreditation or connectivity to the secure government networks in the UK (such as N3 and HSCN). The research indicates that the British adults would have significant reservations about the use of such providers, preferring for healthcare organisation to use UK-based businesses and that have connectivity to the key secure government networks.

GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR is designed to improve the balance between private citizens, business and public authorities, and is intended to be cloud friendly.

The EU's paper "Unleashing the Potential of Cloud Computing" in 2012 made clear from the very start of the process of GDPR's development that data protection was a central part of the Commission's strategy to enable cloud computing.

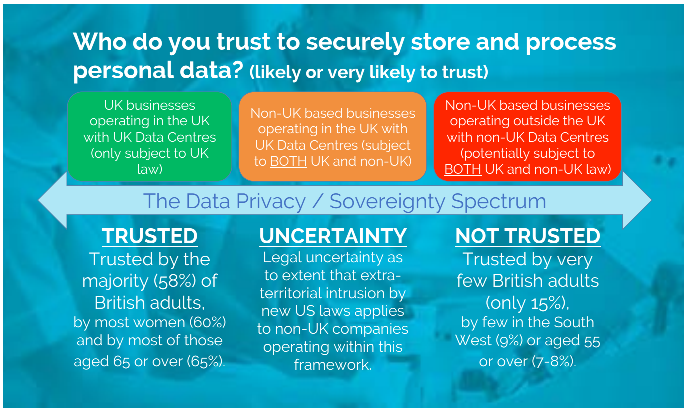
Once implemented, GDPR requires cloud providers who are processing the data of EU citizens to comply with the Regulation, whether the data centre or servers are located in the EU or outside. If located outside the EEA, an appropriate data transfer solution must be implemented by the cloud provider in order to ensure compliance.

GDPR will apply to the UK from 25 May 2018 and when Brexit occurs, the law will remain in force unless amended by virtue of the Great Repeal Bill.

GDPR is generating significant attention because of increased protection for data subjects and the stronger focus on enforcement. The uncertainty over data transfer persists as a result of privacy activism, recent calls to review EU data transfer mechanisims, and multiple overlapping decisions about the impact of law enforcement authorities' rights to access data.

The real problem is exactly how to classify non-UK based businesses (including the major global cloud giants) that are operating in the UK with UK Data Centres. Their UK subsidiaries are bound by UK data protection law, but their parent companies are subject to US law. The problem is that there is legal uncertainty as to the extent that extra-territorial intrusion by new US laws applies to non-UK companies operating within this framework. A number of legal cases are currently being contested with the US Department of Justice and the FBI seeking to force the global cloud giants to hand over data that is based outside the USA. The actions of the current Trump administration have also put the future of the transatlantic data sharing accord, Privacy Shield, into doubt.

Until these legal conflicts are resolved, and until the future of Privacy Shield is clarified, there can be no certainty with regard to how the major global cloud giants should be classified. Arguably if any of the current rulings go against them, they risk experiencing a dramatic loss of trust.



Who do you trust to securely store and process personal data? (likely or very likely to trust)

UK businesses operating in the UK with UK Data Centres (only subject to UK law)

Non-UK based businesses operating in the UK with UK Data Centres (subject to BOTH UK and non-UK)

Non-UK based businesses operating outside the UK with non-UK Data Centres (potentially subject to BOTH UK and non-UK law)

The Data Privacy / Sovereignty Spectrum

TRUSTED
Trusted by the majority (58%) of British adults, by most women (60%) and by most of those aged 65 or over (65%).

UNCERTAINTY
Legal uncertainty as to extent that extra-territorial intrusion by new US laws applies to non-UK companies operating within this framework.

NOT TRUSTED
Trusted by very few British adults (only 15%), by few in the South West (9%) or aged 55 or over (7-8%).

Figure 1: The Data Privacy / Sovereignty Spectrum

The research found that eight in ten (82%) British adults say they think the Government should seek their permission before storing and processing your personal data with non-UK businesses.

82%

say that they think the Government should seek their permission before storing and processing your personal data with a non-UK business.

Not only do British adults have significant reservations about the use of non-UK businesses, they also feel very strongly that the Government should seek their permission before storing and processing their personal data with these foreign-owned and regulated firms.

The research found that most British adults (55%) say they think the UK Government should prioritise working with UK businesses if the price and service is comparable with non-UK businesses, with one in five (20%) saying they should always work with UK businesses regardless of their price and service.

At a time when the US is adopting an America First policy and the EU appears to be preparing to play hardball on the Brexit negotiations, it is hardly surprising that British adults favour giving UK businesses favourable treatment.

The Public Services (Social Value) Act 2013 and the green paper issued in January 2017, 'Building Our Industrial Strategy', both include guidance on taking social value and support for UK businesses into account in public sector procurement.

There is real opportunity for the required innovation and transformation in healthcare to drive social value in supporting skills and capabilities inherent in businesses in the UK.

Conclusion 1: Most British adults are concerned about privacy

The majority of British adults say they are concerned about whether their personal data (e.g. financial/ tax records or criminal records) (75%) and personally identifiable data (e.g. date of birth or address) (72%) are protected by companies and public services.

58%

would trust UK-based businesses to securely store and process personal data.

Table 1: Q. For each of the following types of personal data, how concerned are you about whether it is protected by companies and public services?

OPTIONS	NET Concerned %	Very concerned %	Fairly concerned %	Not very concerned %	Not at all concerned %	NET concerned %	Don't know %
Your personal data (e.g. financial/ tax records or criminal records)	75%	40%	35%	18%	4%	21%	3%
Personally identifiable data (e.g. date of birth or address)	72%	33%	39%	20%	4%	25%	3%
Your health records (e.g. medical history or social care records)	65%	31%	33%	26%	5%	32%	3%
Social media content (e.g. Facebook posts)	55%	21%	34%	26%	39%	39%	6%

Base: All GB adults (n=2,044)

- Two in three (65%) British adults say they are concerned about whether their health records (e.g. medical history or social care records) are protected by companies and public services.
- Two in five (39%) British adults say they are not concerned about whether social media content (e.g. Facebook posts) is protected by companies and public services. A slim majority say they are concerned (55%).
- Women are more likely to say they are concerned about whether social media content is protected by companies and public services than men (60% v 50%).
- Adults aged 65+ are more likely to say they are concerned about whether their personal data (e.g. financial/ tax records or criminal records) is protected by companies and public services. Four in five (81%) say they are concerned about this, while seven in ten (70%) 18-24 year-olds say the same. This youngest age group are more likely to be concerned about social media content than their older counterparts; three in five (62%) 18-24 year-olds say they are concerned about whether social media content is protected by companies and public services while half (51%) of adults aged 65+ state this. This lower figure is likely to be due to this age group using social media less than their younger counterparts.

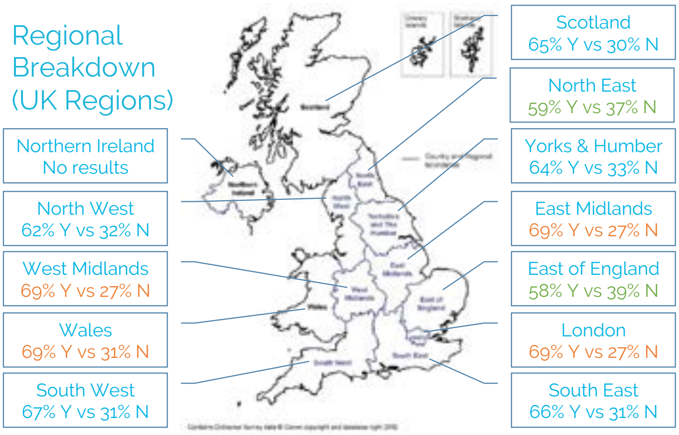

Regional Breakdown (UK Regions)
Northern Ireland No results
North West 62% Y vs 32% N
West Midlands 69% Y vs 27% N
Wales 69% Y vs 31% N
South West 67% Y vs 31% N
Scotland 65% Y vs 30% N
North East 59% Y vs 37% N
Yorks & Humber 64% Y vs 33% N
East Midlands 69% Y vs 27% N
East of England 58% Y vs 39% N
London 69% Y vs 27% N
South East 66% Y vs 31% N

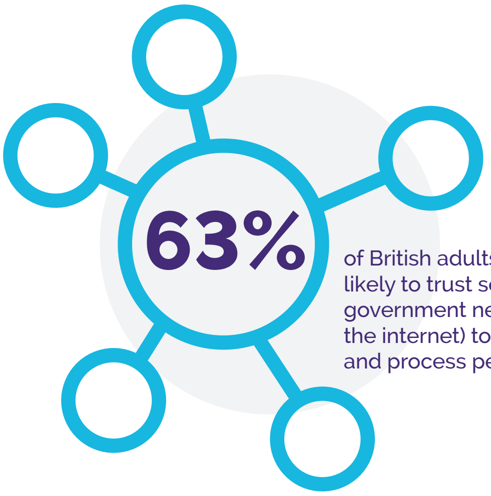
Figure 2: Privacy concerns about your health records including medical history or social care records (Y = very or fairly concerned, N = not very concerned or not at all concerned)

Looking at privacy concerns about health records by region (including medical history or social care records) people in the East Midlands, West Midlands, Wales and London were most concerned, while people In the North East and East of England were least concerned.

Conclusion 2: Most British adults trust secure government networks

The majority (63%) of British adults say they would be likely to trust secure government networks (not on the internet) to securely store and process personal data.

- The majority (58%) of British adults say they would trust UK-based businesses (bound by UK data protection law) to securely store and process personal data, while just 15% say the same for non-UK businesses.
- Four in five (82%) British adults aged 65+ say they would be unlikely to trust non-UK businesses to securely store and process personal data, compared to three in five of those aged 18-44 (59% 18-24 year-olds, 58% 25-34 year-olds, 62% 35-44 year-olds).
- These high levels of trust in secure government networks should be highly encouraging for NHS Digital and the investment in the Health and Social Care Network (HSCN)



of British adults would be likely to trust secure government networks (not on the internet) to securely store and process personal data.

Table 2: Q. There have been recent reports of cyber attacks and foreign surveillance activities that could mean your personal data is less secure. To what extent do you trust each of the following to securely store and process personal data?

OPTIONS	NET Likely %	Very likely to trust %	Fairly likely to trust %	Fairly unlikely to trust %	Very unlikely to trust %	NET Unlikely %	Don't know %
Secure government networks (not on the internet)	63%	14%	49%	16%	8%	24%	13%
UK-based businesses (bound by UK data protection law)	58%	6%	52%	20%	9%	29%	12%
Non-UK based businesses	15%	1%	14%	34%	36%	70%	16%

Base: All GB adults (n=2,044)

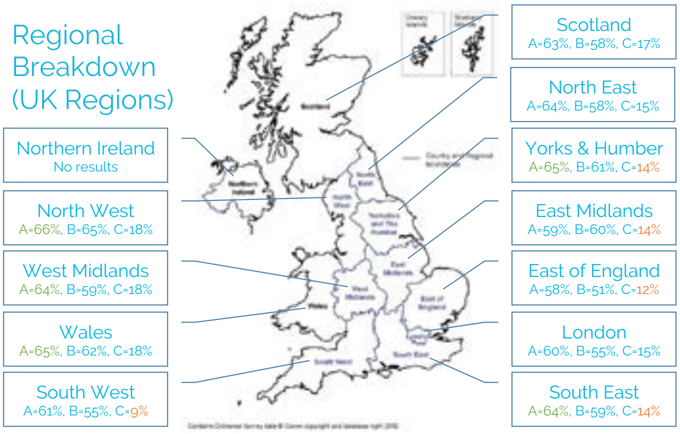


Figure 3: Who do you trust to securely store and process personal data? (likely or very likely to trust) - A = Secure government networks (not on the internet), B = UK-based businesses (bound by UK data protection law), C = Non-UK based businesses

Looking at who British adults trust to securely store and process personal data by region, people in the East Midlands, West Midlands, Wales and London were most in favour of using secure government networks, while people In the South West were least in favour of using a non-UK based business to securely store and process personal data (only 9% being in favour).

Conclusion 3: British adults want the UK Government to seek their permission before using foreign firms to store and process their personal data

Eight in ten (82%) British adults say they think the Government should seek your permission before storing and processing your personal data with non-UK businesses.

Table 3: Q. The UK Government holds various personal data about you (e.g. medical records, tax records etc). Should the UK Government seek your permission before storing and processing your personal data with non-UK businesses?

OPTIONS	%
Yes - they should seek my permission	82%
No - I trust them to decide what is best	12%
Don't know	6%

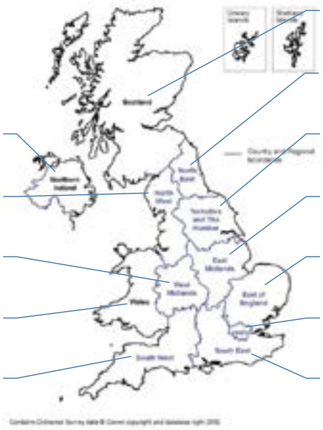
Base: All GB adults (n=2,044)

- Just one in eight (12%) British adults say they trust the UK Government to decide what is best rather than agree they should seek permission before storing and processing their personal data with non-UK businesses.

2/3

British adults are concerned about their health records being protected

Regional Breakdown (UK Regions)



Northern Ireland
No results

North West
79% Y vs 16% N

West Midlands
84% Y vs 10% N

Wales
82% Y vs 13% N

South West
82% Y vs 12% N

Scotland
84% Y vs 10% N

North East
85% Y vs 12% N

Yorks & Humber
84% Y vs 11% N

East Midlands
81% Y vs 10% N

East of England
80% Y vs 15% N

London
84% Y vs 10% N

South East
83% Y vs 10% N

Figure 4: Should the UK Gov't seek your permission before using foreign firms to store and process your personal data?

Feelings about this were strongest in Scotland, the North East, Yorkshire and Humberside, West Midlands and London and weakest in the North West and East of England

Conclusion 4: Most British adults think that the UK Government should prioritise working with UK businesses

The majority of British adults (55%) say they think the UK Government should prioritise working with UK businesses if the price and service is comparable with non-UK businesses, with one in five (20%) saying they should always work with UK businesses regardless of their price and service.

Table 4: Q. Which of the following best reflects your view when it comes to the UK Government working with businesses?

OPTIONS	%
The UK Government should always work with UK businesses regardless of their price and service	20%
The UK Government should prioritise working with UK businesses if the price and service is comparable with non-UK businesses	55%
The UK Government should not take where a company is based into account when deciding who to work with	10%
Don't know	14%

Base: All GB adults (n=2,044)

- Only one in ten British adults (10%) say they think the UK Government should not take where a company is based into account, when deciding who to work with.
- Three in five (62%) British adults in the ABC1 socio-economic grades say they think the UK Government should prioritise working with UK businesses if the price and service is comparable, while less than half (46%) of adults in the DE grades state this. One in five (22%) British adults in the less affluent DE socio-economic grades say they don't know their view when it comes to the UK Government working with businesses; three times the proportion of those in the AB grades that state this (7%).

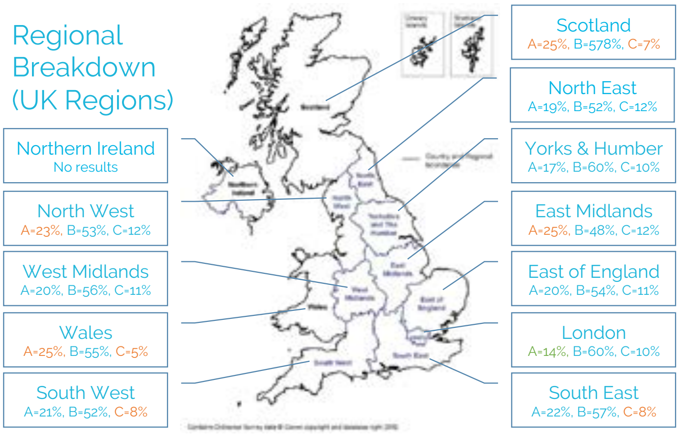


Figure 5: When it comes to the UK government working with businesses, should it favour/prioritise UK firms? Prioritise: A = UK firms always, B = UK firms when comparable, C = Doesn't matter

Reflections in Light of Recent Cyber Attacks:

The research was carried out in late April 2017. Shortly afterwards organisations across the world, including the NHS in the UK, were hit by the largest ever cyber attack. Before publishing the results of the survey, we wanted to reflect on this incident and ask if the respondents in the survey were right to have been concerned. A vulnerability occurs at the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. All three of these elements converged in a very short period of time, in the case of this incident:

- **March 2017:** Microsoft acknowledged the existence of a vulnerability affecting Windows computers and issues a set of patches for supported platforms. No patches were issued for older platforms such as Windows XP that are no longer supported by Microsoft (some corporate users pay to retain support for XP, but the vast majority of users are unsupported).
- **April 2017:** An entity known only as the "Shadow Brokers" released an arsenal of powerful software tools apparently designed by the NSA to infect and control Windows computers which included weaponised tools that were designed to exploit this vulnerability. These tools appear to have been in use by the NSA long before Microsoft acknowledged the existence of the vulnerability.
- **May 2017:** Hackers spread a variant of 'WannaCry' ransomware by repurposing the NSA tools to exploit the vulnerability in Microsoft's Windows operating system. This enabled them to automatically spread the package across large networks. In a matter of days, the attack spread to over 200 countries and impacted over 200,000 computers. Microsoft belatedly issued an updated patch for all platforms – including XP.

A blame game rapidly ensued with Law enforcement agencies sought to track down the hackers, Microsoft faced criticism for not patching the vulnerability sooner and not issuing patches for all platforms earlier, the NSA faced criticism for developing weaponised tools to exploit the vulnerability rather than report the vulnerability immediately to Microsoft and also for then allowing its weaponised tools to be leaked, and users faced criticism for continuing to use Windows XP (a version of Microsoft's operating system that has not received publicly available security updates for half a decade), for not installing the available patches earlier and for opening attachments from untrustworthy sources (the way the malware entered each network).

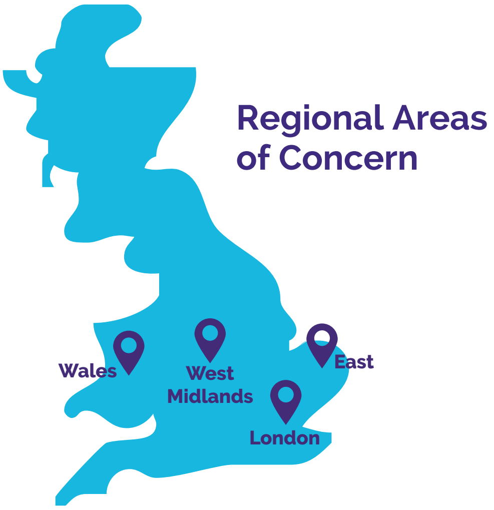
As the research was conducted in late April 2017, ahead of the ransomware outbreak, we revisited the research findings. Tellingly a number of the findings resonate with the issues highlighted by this major incident:

- **Britons were right to be concerned about whether their personal data (including their health data) was protected by companies and public services.** While no health data was leaked, its protection was found to have been inadequate.
- **Britons were right to have trusted UK-based businesses (bound by UK data protection law) to securely store and process personal data – at least in relation to cloud-based businesses.** UK-based cloud providers that adhered to local data protection law would have ensured that all security patches had been implemented. Typically such cloud providers have higher levels of security skills and tools than on-premise datacentres, and they don't tend to use outdated platforms such as XP. In addition, patches and software updates can be quickly and easily rolled out across cloud-based platforms, while fragmented on premise estates are notoriously difficult to update.
- **Britons were right to be reluctant to trust non-UK businesses to securely store and process personal data.** The NSA (and FBI) use a number of approaches in their surveillance activities. Not only do they use the kind of weaponised tools to exploit vulnerabilities, as was shown to have been the case in this instance, but they also use an ever growing set of legal powers over US-based companies to access data (even when it is held outside the US – such as in the UK-based datacenters of US cloud firms). UK-based businesses are beyond the reach of such intrusive extraterritorial legal powers.
- **Britons were right not to trust the UK Government to decide what is best rather than agree they should seek permission before storing and processing their personal data with non-UK businesses.** There is a very real threat from the NSA and the tools and intrusive extraterritorial legal powers that it employs. This threat is massively amplified when its tools are allowed to fall into the hands of criminals.

A final note from someone that understand the NSA better than most:

Edward Snowden has been outspoken in his criticism of the NSA, its surveillance activities and its practices. In relation to these recent incidents he squarely blamed the NSA for not preventing the whole incident and for not issuing patches to protect people from the tools that it had created once these tools had been leaked. In addition, a week earlier he also spoke passionately in favour of open source software and OpenStack (an open source cloud platform) arguing that the communities that support open source are more effective in identifying vulnerabilities, less likely to allow them to be exploited and more likely act responsibly in the interests of all – something that a number of parties failed to do in this case. He warned against the use of proprietary public cloud firms - the very cloud firms that are not-based in the UK, that are subject to the intrusive extraterritorial legal powers mentioned above and that use their own proprietary software instead of OpenStack.

Microsoft later issued a statement also pointing the finger of blame at the NSA.



Opinion

Efficiencies and Service Improvements:

- There is a definite need for innovation and transformation across healthcare, in order to drive efficiencies, reduce costs and improve service level and outcomes.
- Cloud providers supporting the UK government's cloud first strategy, the most significant of which is UKCloud, have enabled central government to save £600 million by moving workloads to the cloud, earning the UK recognition from the UN as the most digitally advanced government in the world. UKCloud's solid track record in central government, supporting hundreds of UK public sector projects, and enabling them to achieve new efficiencies and better outcomes, is immediately applicable in other sectors as well, including health and local government.
- UKCloud has hundreds of partners that bring specialist skills and capabilities to help Healthcare organisations with their transformation.

Privacy and Consent:

- The recent cyber attacks exposed the vulnerability of the NHS to external threats. It is no coincidence that the NHS, with a fragmented on premise estate that is relatively out of date and notoriously difficult to patch, and keep secure, was hit particularly badly by the cyber attack, while central government which has been quicker to adopt cloud computing was not.
- The public is more concerned about the protection of personal health data than other digital data such as social media – an opinion that will only have been heightened by the recent cyber attack. This shows that one-size-doesn't-fit-all – standard technology specifications and systems will not suffice for the sector, with enhanced privacy provisions being required.
- NHS Digital's new HSCN is supported by public opinion, UK adults much prefer personal health data to be protected within secure government networks where possible.
- And GDPR will be increasingly relevant, with the UK public clearly expressing a desire for their consent to be sought before their data is given to foreign businesses for storing and processing.

Sovereignty and Social Value:

- Public opinion shows that it is important for public sector organisations in general and healthcare ones in particular to support British services, skills and innovation.
- At the same time, there is a clear lack of trust in non-UK businesses. The recent attack and the actions of the NSA will have only added to such concerns. The public will not only be alarmed at the illegal use of exploits by the NSA (and their subsequent use by hackers), but also by the extent of the intrusive extraterritorial legal powers that the NSA and Trump administration have over US companies. Given that UK businesses not only keep data in the UK, but also operate beyond the legal reach of the NSA and Trump administration, there is a clear advantage in using such UK-based businesses.

> "British adults want the UK Government to seek their permission before using foreign firms to store and process their personal data"

About UKCloud Health

UKCloud Health powers healthcare communities. Providing a secure, but easy to use cloud platform that supports digital transformation and enables the optimisation of patient-oriented healthcare, UKCloud Health supports health and care organisations, as well as research and life sciences and pharmaceuticals.

We're focused on cloud. Our easy to use platform offers an open, collaborative environment to help enhance the way you and your Healthcare colleagues work.

We're open. You are never locked in. Giving you the choice and flexibility of a range of technology platforms as well as payment models in GBP to avoid currency fluctuations.

Dedicated to the UK Healthcare sector. We support cloud and digital transformation of services across the healthcare sector, including health and care, research and life sciences and the pharmaceutical industry.

We develop communities. UKCloud Health is bringing Healthcare communities together – enabling collaboration, innovation and digital transformation.

Customer engagement. With UKCloud Health you're never alone. Enjoy peace of mind, knowing we understand the challenges you face. Your success is our success.

Additional information about UKCloud Health can be found at www.ukcloud.com and www.ukcloudhealth.com

UKCloud Health is a division of UKCloud – a 2017 Queen's Award for Enterprise for Innovation winner – dedicated to the UK Public Sector. We provide assured, agile and value-based true public cloud that enable our customers to deliver enhanced performance through technology.

ukcloud
health

E info@ukcloudhealth.com
T 01252 303 300
ukcloudhealth.com