APPG ON CYBER SECURITY MEETING MINUTES HELD ON THE 19TH OCTOBER AT 4.00 p.m. VIA ZOOM: The NHS, patient data and how it is secured.

Chairman's welcome – The Chair thanked the attendees and speakers. Summarised the issue as Parliamentarians are worried about data who handles it and to whom it is passed. The aim of the meeting is therefore to discuss this.

Apologies: The Rt Hon the Lord Arbuthnot of Edrom, Lord Mackenzie of Framwellgate.

Present: Simon Fell MP (Chair), Sara Britcliffe MP, Andrew Henderson & Prof Keith Mayes (Secretariat)

Speakers:

a) Simon Madden

Simon Madden is Director of the Data policy directorate at NHSX, as well as for the NHS Covid Pass policy. He is a career civil servant with experience in front line operations, policy development, project delivery, strategy, planning and performance. His previous posts have included Programme Director for Places for Growth in the Cabinet Office, leading a cross-government programme delivering a government commitment to move public bodies and civil service roles out of London into the regions and nations of the United Kingdom and Deputy Director in the Prime Minister's Implementation Unit where he led on government planning and performance strategy. NHSX' role is joint with DHSC. Portfolio covers:

- Data policy in Health and Care system
- Information Governance
- SRO for the NHS AI Lab.

Covid has taught us much in terms of health data. We have been able to use the Control of Patient information Regs[1] and issue COPI notices to allow the greater flow of data and aid planning / research. Where we are now is that we want to try and lock in some of the beneficial change which we have experienced whilst ensuring we can do that safely and securely.

Able to harness data safely, securely and ethically for the benefit of patients, building on the opportunities for change deriving from the Pandemic.

Data Saves Lives[2] has been published in June in draft form for feedback. Have set out ambitions to ensure that all systems implement a shared record and work towards a more comprehensive system of data sharing and integration. Have set out legislative options for the sharing and access of data for the health and care sector. Trying to tighten up where NHS Digital cannot do certain things or there is a degree of ambiguity. Makes clear exactly what can be done.

It also introduces methods to enable healthcare leaders to handle data through simplified guidance. There is a multiplicity of guidance about what can be shared. Put in mechanisms to rationalise this and ensure guidance from professional bodies is consistent with this approach. Citizens now have rights to amend their own records. Want to push data driven technology to improve outcomes.

Need to lock in beneficial changes and the momentum gained through Covid. Need to build confidence in the public and the staff that the system can be trusted. The final version of the

[1] The Health Service (Control of Patient Information) Regulations 2002 (legislation.gov.uk)

[2] Data saves lives - NHSX

strategy has a section on improved trust and transparency. Sees this as a reset of the way the public sees how data is used. The patient owns the data and the NHS holds it in trust. Want to develop new ways of sustaining dialogue with patients about how we implement this. Also need a broader campaign around the benefits of not opting out of data sharing. Need to explain the benefits of planning and research within the NHS and data sharing. The development of the vaccine for Covid has shown us the power of research. Without a significant mass of people staying opted-in for data we cannot make proper use of data.

Wants to set standards for how individual healthcare organisations use data to help the public. Approach will be around secure environments which data never leaves. This will end the copying and shipping around of health data. Looking to set up an infrastructure that allows data to be held in one place and accessed securely. This should give the public confidence and benefit the wider society as a result.

A recent spurt of controversy over the summer around the NHS Digital Programme needs to be addressed. We need to understand that data has been flowing from GPs to the centre for a long time. The new system, GPDRR replaces a ten year old system with improved security and privacy protections. Also more efficient. This will provide near real time data to the system and achieve much better data for research purposes.

The NAO has criticised the current system for cost and lack of security. GPDRR introduces new protections etc. and makes the system of data storage and flow more efficient.

Delay to the implementation following concerns from the public and the profession. Have made a commitment to work with patients and clinicians, step up communications for GPs, introduce safeguards etc. Have not given a specific start date but set out a series of tests. Patients able to opt out or in and there is increased flexibility with greater control for the public. Previously uploaded data can be deleted. It also provides a trusted research environment for approved researcher. They will work on de-identified patient data.

Campaign of engagement and communication in 4 phases: starts with listening to the public. If individual members of the public still choose to opt out, they will be provided with the means.

b) Phil Huggins

Phil is the Interim National Chief Information Security Officer for Health and Social Care at NHSX. Phil has over 24 years' experience within security, technology and data roles, with extensive experience of leadership, governance, management, system engineering and enterprise architecture. He has designed and operated security for critical national infrastructure and has also advised and managed global financial services organisations as well as national regulators on cyber resilience and cyber security. Phil recently took up post as National CISO

Runs a split team between NHSX and civil servants. Remit has NHS, Health and Social Care and implements cyber security services and works with CQC to advise on standards. Phil is also the Cyber Programme for Healthcare Senior Responsible Officer

Funds:

1. services provided by NHS Digital incl. Cyber Security Ops Centre
2. System improvements such as legacy platforms or unsupported systems.

Setting a new strategy for healthcare and cyber security over the next 3 to 6 months. Specific strategy being developed for the SOC.

Prior to this worked as CSO for the NHS Test and Trace.

In new role pleasantly surprised by what has been done in the NHS. Post WannaCry there has been a lot of work to improve cyber security.

c) Professor Stephen Wolthusen

Stephen Wolthusen is Professor of Information Security at the Department of Information Security, Royal Holloway, University of London and holds a concurrent appointment as Professor Information Security at the Norwegian University of Science and Technology. His research interests include the investigation of formal models for the resilience and robustness to attacks of networks including of critical infrastructures and cyber-physical systems. He has led and is participating in a number of research projects on the security of medical devices including defibrillators and pacemakers as well as diagnostic Internet of Things devices and currently investigates deontic models for automated reasoning about privacy of medical data.

Whether we like or not the NHS is not the largest holder of patient information anymore. Some of that may be with commissioned entities, IOT devices or in the hands of US based genetic testing companies over whom we have very little control.

Privacy and integrity are the key areas here.

Firstly, anonymised data does not stay as such, this is a fundamental aspect of data-based security. You can reconcile anonymised data against other databases without proper controls. What makes this problematic is that many of the data sets that are being collected are not part of what the NHS is holding. Private sector data holders may not bother with privacy and integrity guidelines.

Unpleasant side effects such as non-co-operative biometrics based on facial recognition which may be linked with patient records. A slow leak can be as problematic as a sudden breach. Can be hard to control. You can monitor heart rates and irregularities by tuning your Amazon Alexa. People sign this off in the terms of use!

Secondly when considering privacy, what constitutes data? The documentation concentrates on records. Maybe by focussing on records, it might be that there is a risk that we lose sight of the data we collect before it becomes a record. For an electronic GP consultation people photograph themselves and do they know that they end up on Google photos before being sent to the GP?

The move to integrate the care sector described by PH exacerbates the problem as sensors are now linked into a personal broadband before being passed onto a Trust. This intermingling throws up challenges that were not part of the problem a few years ago.

There is better guidance on sanitising medical equipment than re-using medical IT equipment.

Integrity – not just about the record but also the entire lifecycle from the first reading on some device and into a database. Even though a lot of homework has been done, the required level of maintenance of embedded systems in sensors etc. will lead to a massive amount of homework in maintaining and / or updating them or de-commissioning them. Even small embedded components will be vulnerable, not glamourous but a challenge. Getting this right, end to end integrity form point of collection to safe erasure is a substantial challenge. Imagine if you have not encrypted the data but had a slow burn attack, the clean-up would be hugely painful

In sum it is not only about the data but also the code used to interpret the data, the metadata etc. Becomes poignant as we try to analyse data sets by machine learning, it becomes vulnerable to mis-use. Surprised that there is not much of a stick to wave in the face of medical device manufacturers. Will have to tighten the screws a little bit. Device manufacturers are unresponsive to approaches pointing out problems.

Q&A:

The Chair invited responses from the other two speakers:

SM – agree that the reality of anonymisation is that technology will continue to challenge us. You can with a broad set of data points identity individuals. That is why we need to stay ahead and we are moving to trusted research environments. Have been doing a lot of work with Ben Goldacre and ONS. Challenge for the NHS is to avoid being complacent. Need to keep pace constantly.

PH – in security have talked about the risk of harm, here in healthcare we can see opportunity. I am a professional worrier. I am aware of the opportunities which connected devices create such as virtual wards. Need to balance connectivity with risks and the benefits to healthcare. Fantastic guidance has been provided for IOT devices. MHRA is a good provider of guidance on security. We are on a wave of innovation, somethings fail sometimes.

Kevin Borley- one of the original workers on the infrastructure supporting the NHS at a time when concepts of security could be spelt but not understood. Been treated for a brain tumour using connectivity. Spent a lot of time in Silicon Valley and seen concepts that the NHS needs and should be aligned with. The bad guys will provide threats but urges people to see what is being developed e.g. remote operations. Need to be ahead of them not behind.

SM – very fair challenge. We do talk to the tech sector and innovators. Part of our role to make sure that innovators can flourish in the UK. I see the challenge of getting ahead of the thinking. Always playing catch up.

Mike Hurst – interested in the talk about connected devices. Retired police officer and prior to that worked in IT. In last few years worked on economic crime prevention (Operation Stirling) helping vulnerable adults. Have also looked after old people personally managing their healthcare and finances etc. Did an MSc. 10 years looking at this. Accept need to share data. Looked at using remote monitoring to help old people. Spoke about personal experience caring for his wife and the difficulties trying to get the result of a blood test. System is failing old people. Acting with the expectation that those who are getting older will have the cognitive skills to use technology.

KB- recently went through treatment and agrees with MH. Had problems using technology and had to find trusted people to help. Those who develop the software should put themselves in the shoes of the elderly and the sick when developing systems.

MH – need to think about the use of technology and those who are ill or old.

SW – been involved in projects with people with early onset dementia. Wants to raise the issue that you are accumulating a lot of legacy equipment (older than 2 years) and has been working with companies in this area. The core competence of the business is not usually cyber security. Market pressures have a big role to play. Lack of regulations for instance which are just not there so companies do not pay attention as they should to security.

KB – my comments on Silicon Valley are balanced by my work with Smart Cities. A lot of what is being referred to as personal data needs a lot of regulation.

PH – there has been a bunch of work on the clinical safety work being done and cyber security is a key pillar. Risk assessment is a clinical safety issue. Clinical safety officers act as important gatekeepers. New areas of cyber security come with their own problems, we are not walking blindly into this.

Sanjana Mehta – SM you mentioned the role of professional bodies in clarifying data sharing. Can you clarify this?

SM – they are not helping to clarify our guidance. We are consolidating and rationalising the message. The NHS is not a single body, it is a multiplicity. With some of the professional bodies we are making sure that their guidance is consistent with ours. It would be counterproductive if BMA guidance was at odds with ours. Trying to tackle institutional and individual paralysis about data sharing. Professional bodies need to reflect this in their guidance.

SF – SM you talked about using data to drive improvement in health outcomes. Are the mechanisms there in the wider NHS to look at that data?

SM – the centre has an important role (NHS Digital, England etc) in making sure that the insights which the centre gets are shared across the systems. We are seeing how an Integrated Care System is supported by technical infrastructure. Building analytical capability is a challenge in the health system. You are classified as an administrative worker as an analyst not a professional. Have set up a network of analysts with about 5,000 taking part. Need to make sure leaders in the NHS are data and analytical-literate. Thanks to Covid, leaders have realised how important this is.

KB – volunteered to provide some additional options for analysts.

Prof Keith Mayes – just wanted to make an observation on the security of medical data and access to it. I appreciate the intent that patient data belongs to the patient, likes this and likes proper processes etc. The amount of data is so huge, so many staff in different categories etc. all of whom need access in an emergency. Thinks that the NHS is on a hiding to nothing from a cyber security viewpoint. Would click the opt-out button.

Not necessarily that the NHS has the most attractive pot of information. During Covid a runner could not just turn up at an event, they had to register which means sharing information. Most runners have fancy watches that take your heart rate, have a GPS and syncs with your phone. Many of these types of people give away information to organisations such as Strava. There is still the principle of choice. Most concerned by the kind of data which SW touched on such as real time data. Where is that data, who ensures that it is being looked after correctly? Gut feel is that it ends up in the US. Is this being addressed?

SM – do need to tackle the perception that health data is all in one place with access for anyone in the NHS. Our data protection laws are permissive but robust. Common Law proposes an additional level of protection for individuals. It is my duty, even if I clash with other areas of Govt, to preserve the Common Law duty of confidentiality. Important to understand that the Law is robust in this area. You do not get access to health data easily. Patient consent is the passport to getting access to data. Data is not kept in one place with everyone having access.

PH – we do have data in lots of places with many organisations with sets of data here and there. We do have a robust legal system. When talking about pre-records data, it is covered by the same laws. Used to call it data dust as it collected.

Apurva Saral – RHUL alumna, VP at Barclays Bank. When we use new tech like Cloud, how important is access control in your views? What assurance can you provide us that the data will not go out as it should not?

PH – have some extensive standards which we use, both own and Government. Pretty aggressive in making sure that they are applied. There is always an opportunity for an insider to break the rules, we address this as a concern. We are talking about human beings in a complex system.

SM – agree with that. Job of the technologist is to operationalise the legal framework which we have to protect data. The legal framework for health is pretty robust. You need a clear legal basis to access data. You do not get all of the data, most people just need a small part of the data. The need for someone to have access on a large scale is very rare other than providing direct care. Technologically we do not have the join-up across the whole system. We are trying to get there. The legal basis is there.

SW – it is reasonable to assume that something will go wrong. To support resilience, it is important to consider “forensic readiness” so that you collect the information that you need if something goes wrong. A large customer could push for this from their supply base.

SF thanked the speakers for sharing their time and knowledge.