

Written evidence submitted by the Wellcome/EPSRC Centre for Interventional and Surgical Sciences (WEISS) (DHS0021)

House of Commons Select Committee on Health and Social Care Expert Panel

Inquiry: Evaluation of the progress that the Government has made against its commitments in the area of the digitisation of the NHS

Chosen policy area to provide evidence: **The health of the population**

Commitment 1

“Through the Data for Research and Development programme we will invest up to £200 million to transform access to and linkage of NHS health and genomic data sets for data-driven innovation and inclusive clinical trials, whose results will be critical to ensuring public confidence in data access for research and innovation purposes.”

Commitment 2

NHS Digital will develop and implement a mechanism to de-identify data on collection from GP practices by September 2019”

Executive Summary

- Although some progress has been made for the linkage of NHS health and genomic data sets for data driven innovation, it is unclear whether the government is on track to meet this commitment and its implications.
- Possible issues that prevent this transformation include: lack of dedicated support for managing digital data for research; a lack of interoperability in the current digital landscape within the NHS; financial constraints on dealing with legacy IT systems; and a fragmented approach to the deployment of electronic patient record platforms.
- The government’s General Practice Data for Planning and Research (GP DPR) programme sought to improve the security and efficiency with which patient data from GPs was collected after de-identification. This programme has been delayed and halted due to public concerns about transparency, data security and future use.
- Transparency and clear messaging on how health data is going to be used is very important as it directly affects trust in institutions and how much patients and the public are willing to engage.
- Patients have particular concerns that very sensitive data may be exploited for monetary gain, where private firms are involved in handling patient data.
- Government, NHS Trusts and academic/research institutions should work together towards establishing a common framework for secure data sharing. Core infrastructure for secure long-term clinical data storage and sharing would also help to make more data available for clinical research.
- Patients and the public should be more involved in research and governance around data stewardship. This may facilitate collecting important information such as demographics, while maintaining high standards in privacy and security.

Introduction

[WEISS](#) is an interdisciplinary research centre based at UCL that specializes in the fields of surgical and interventional sciences. At WEISS, engineers, clinicians and computer scientists work together to develop new technologies for more precise and less invasive procedures, enabling more patients to benefit from safer, more localized treatments and shorter recovery times. WEISS is funded by the Wellcome Trust (Grant number 203145/Z/16/Z) and the EPSRC (Grant number NS/A000050/1).

The contributions in this document follow from a previous response to the inquiry “Digital Transformation in the NHS” reporting from the experience of our team members and from a series of policy workshops organised on the topic of “Artificial Intelligence, Surgery and Inequalities. Further insights and comments were extracted from the response by the then Secretary of State for Health and Social Care, the Rt Hon Steve Barclay MP.

[Commitment 1 - “Through the Data for Research and Development programme we will invest up to £200 million to transform access to and linkage of NHS health and genomic data sets for data-driven innovation and inclusive clinical trials, whose results will be critical to ensuring public confidence in data access for research and innovation purposes.”](#)

There are some indications that this commitment is progressing though it is unclear where it is on track to be met. The concept of trusted research environments (TREs) or more broadly secure development environments has been one of the policy areas that the government has committed to invest on, particularly by pledging to “deliver the policy and requirements needed to implement secure data environments (SDEs)”

Guidance about SDE has been recently published and there are good signs from multiple institutions coming together to align strategies on the implementation of TREs. However, there are still risks that some more medium-term commitments are not on track to be met, particularly when “required standards and interoperability patterns – both local to local and local to national” have not yet been clarified.

The pressure to develop complex infrastructures and inter-linkages (which need dedicated skills as well as shared standards) has sometimes been addressed by turning to the tools big tech firms have available, which may not be sustainable both from a reputational and practical point of view.

There is a need to build more support for managing and sharing digital data. This can be done by promoting greater involvement of healthcare professionals to identify practical solutions to overcoming administrative barriers and also to build capacity for researchers to engage with increasingly complex governance.

Finally, it is essential that discussions around what best constitutes these environments and how to deploy them are developed with input from researchers and the communities that will ultimately benefit. As a result, it may be possible to achieve further commitments that the government has set

such as developing “a data pact setting out mutual expectations for the public and health and care system”.

Below we cite some of our previous responses highlighted in the Inquiry “digital transformation of the NHS”, which we believe to be particularly relevant for the Expert Panel:

[What progress has been made in digitising health and care records for interoperability, such that they can be accessed by professionals across primary, secondary, and social care?](#)

a. The lack of interoperability is a major weakness in the current digital landscape within the NHS. Although some advances have been made over the last decade, the flow of information between different parts of the healthcare system (primary, secondary, and social care) is poor. As healthcare professionals, members of our team report daily struggles in obtaining patient records and/or results that are critical for patient care. The lack of interoperability within the NHS is multifactorial.

b. There are many NHS trusts that still utilise patient records on paper, and in trusts that have transitioned to electronic patient records significant proportions of older paper records remain to be digitised (such records are by default not interoperable). Moreover, digitisation of paper health and care records invariably involves document scanning and deposition to libraries that are cumbersome to search (for specific information) and difficult to share. Test results performed in one NHS trust are not easily accessible by healthcare professionals, which is often impacting clinical management (for example: cancellation of operative procedures when essential test results cannot be accessed, or repeating tests when results cannot be accessed with obvious patient related and financial implications).

c. Sharing of radiological images (x-rays, ultrasound/CT/MRI scans) within the NHS is much more advanced (and has been taking place for a long period of time through the introduction of picture archiving and communication systems; PACS), but images must be actively sent from one trust to another – often requiring manual and time-consuming input - and access is limited. The gradual introduction of electronic patient record systems in multiple NHS trusts (as well as some GP practices, but much less so in social care) has not resulted in the interoperability “revolution” that most health and social care professionals have been craving. This is because (due to the lack of an NHS-wide IT strategy) various electronic patient record systems are currently in use, which lack inter-connectivity (in other words, they are unable to “talk” to each other).

[What progress has been made in dealing with the proliferation of legacy IT systems across the NHS?](#)

Financial constraints

a. Legacy software is based on outdated operating systems and in many instances is an amalgamation of distinct platforms (e.g. separate programs for electronic records, test results, and x-rays) that are slow, not user friendly, and might contribute to the NHS’ “weak” data security defences. Financial constraints have led to many NHS trusts adopting a policy of updating legacy IT systems, but despite this such systems are simply not good enough for the

NHS in the 21st century. Moreover, the need for frequent updates over a long period of time is likely to be associated with significant cumulative financial cost. The proliferation of legacy IT systems within the NHS is out of necessity and not choice for many hospitals, and as a result progress dealing with it has been rather slow. It highlights financial inequalities among NHS trusts, as well as the lack of an NHS-wide IT strategy.

Lack of an integrated strategy

a. Although several NHS trusts are now proceeding with deployment of modern electronic patient record platforms such as EPIC, the choice of platform as well as timing of deployment remains trust specific (determined by local financial and IT resources). This fragmented approach limits scalability as well as cost-effectiveness. The development of a global IT strategy would allow the adoption of an electronic patient record system that suits the needs of the whole of the NHS (and not individual trusts) and could be scaled-up rapidly (as part of an UK-wide effort). Moreover, the size of the NHS is a weakness but is also one of its greatest strengths; **a uniform, NHS-wide approach to the deployment of electronic patient record platforms would be much more cost-effective and ameliorate digital heterogeneity and inequality within the NHS.**

We propose further ideas for the government to explore in this area:

- **Empower patients to be part of governance around data stewardship. Trusted research environments (TREs) have been suggested as a route for increasing trust around security and privacy of data. Participants suggested that involving patients and the public in the design and governance of TREs might help to increase trust further.**
- **Develop more flexible and agile research infrastructure and proportionality in regulations – further investing in diversifying the actors in charge of developing TREs;**

[Commitment 2 - NHS Digital will develop and implement a mechanism to de-identify data on collection from GP practices by September 2019](#)

“In 2021, the General Practice Data for Planning and Research (GPDPR) programme, which sought to improve the way in which patient data from GPs was accessed and used to run and improve NHS health and care services and for research purposes, quickly ground to a halt when the public raised concerns about transparency, data security and future use.”

This first-hand report of NHS digital highlights one of the main problems to safely implement a mechanism to de-identify data on collection from GP practices, and why it has not been achieved yet.

The population in the UK is very diverse and contains multiple cultures, nationalities, religions and ethnicities. This means that there may not be a universal way to improve people’s trust and willingness to share their data. We highlight the importance of policy makers and researchers talking

with the public about sharing and governance of health data. This will make the argument for data sharing easier.

Finally, we flag the importance of this commitment and how failure to reach it can lead to incomplete and unrepresentative datasets which are a major source of health inequalities.

Below we once again cite some of our responses to the questions asked in the “digital transformation of the NHS” inquiry.

[What progress has been made on making data captured for care available for clinical research through digital transformation?](#)

Insufficient standardisation

- a. The UK has world-leading expertise on the core components of digital healthcare, which can be utilised to develop impactful clinical research. In the current environment, the governance and legal aspects surrounding sharing of data for clinical research are handled individually by each NHS Trust generating significant obstacles and logistical difficulties in making data captured for clinical care available for research. **The government together with NHS trusts and academic/research institutions should work towards establishing a common framework for secure data sharing.**

Core infrastructure

- a. This can be also extended to a framework covering data sharing agreements with industry. Moreover, the **government (in collaboration with academic institutions) should put in place core infrastructure for secure long-term clinical data storage, in conjunction with specialised personnel (e.g. data analysts, IT specialists) and computational/in silico analysis capabilities (e.g. for development of artificial intelligence/machine learning platforms).**

Data collection

- a. Finally it is also important to highlight the fact that digital transformation in the NHS could also aid standardisation of data collection (this would allow NHS-wide data pooling for research purposes), streamline prospective data extraction from electronic patient records (currently such data is extracted manually by researchers, but the process could be automated), and ultimately improve the quality of the data collected (leading to high quality research that can impact patient care and outcomes).

[How can the Government communicate the benefits of digital approaches in healthcare to the public and provide assurances as to the security of their data?](#)

Understanding patients concerns

- a. The COVID19 pandemic has resulted in a paradigm shift on multiple aspects of healthcare provision and accelerated the introduction of digital platforms (and pathways) within the NHS. Although virtual medicine will never replace direct patient contact, the widespread use of these platforms during the pandemic have made parts of the NHS more “user-friendly” (albeit

paradoxically) and have made the public much more aware of the benefits of digital approaches within the NHS.

b. However, there is still a lot to be done to identify what are the main concerns that patients and the public have towards digital approaches in healthcare (such as the use of Artificial Intelligence), in understanding how patient data is actually used and how to ensure those approaches are made available for all.

Data security

a. Recent examples of digitalisation like virtual GP and outpatient consultations, virtual multidisciplinary team meetings (making attendance to such meetings more practical for healthcare professionals), and patient access to health records/results have transformed (and mostly improved) healthcare provision within the NHS and were fast-tracked out of necessity during the COVID19 pandemic. As a result, communication “channels” between patients and healthcare provision teams were also improved through mobile phone-based applications (such as the NHS application, as well as the “My EPIC” application).

b. Uptake of and public confidence of these initiatives very much depends on data security standards and how they are upheld. Despite the highly sensitive nature of patient data, the NHS has not always maintained the highest standards in data security (highlighted by recent, widely publicised healthcare data breaches). As a result, widespread public scepticism remains regarding the presence of effective data security frameworks within the NHS. The latter is compounded by concerns regarding sharing of data with third parties (including private healthcare and insurance providers).

Transparency and showcasing benefits of sharing data

a. Digital healthcare success stories should be examined closely (so that lessons can be learnt) and should be highlighted to the public to enhance confidence. An example of the latter is the Moorfields Eye Hospital/Google Health partnership, in which data security was extensively considered. **The aim should be to develop and implement a transparent data governance framework that is able to adapt to constantly evolving data security threats and is linked to high-quality data security training for healthcare professionals. The latter should become integral to continuing professional development (CPD; current NHS data governance/security training programs are mostly a “tick-box” exercise for staff).**

More specific ideas for exploration in this area are:

- **Devise systems to disseminate and implement health dataset standards, including an active voice of patients, clinicians, researchers and policy makers.**
- **Expanding on current initiatives to track public attitudes towards data and new technologies such as Artificial Intelligence by further examining the influence of socio-demographic and health-related variables in their acceptance.**

Nov 2022