**Data: A New Direction:**

**KONP’s response to the consultation from the Department of Digital, Culture, Media and Sport**

**Introduction**

We are writing on behalf of Keep Our NHS Public (KONP), a civil society group concerned about the future of the NHS as a comprehensive, publicly provided and publicly accountable health service, funded from public taxation and free at the point of use.

This consultation on a new data regime from the Department of Digital, Culture, Media and Sport (DDCMS) appears at the same time as the Police, Crime, Sentencing and Courts Bill and the Health and Care Bill. If passed, these will provide new powers for government and, potentially, private companies, to allow increased access to individuals’ confidential data. The Cabinet Office is also currently looking at the Digital Economy Act of 2017 and exploring how to reduce ‘barriers’ to information sharing and extend existing public service delivery powers to the business sector. As a civil society group, Keep Our NHS Public is concerned that these initiatives represent a concerted effort to weaken the rights and protections governing the sharing of personal data, very often for commercial purposes.

The DDCMS proposals will make it more difficult for individuals to know what is being done with their data, while making easier for the government and corporations to access, reuse and potentially misuse it. The implications are far reaching, affecting for example, the rights of workers, students and pupils and vulnerable or marginalised groups, making it harder to uncover and challenge discriminatory practices and reducing public safety.[[1]](#footnote-1)

Proposals in Chapter Five would undermine the independence of the Information Commissioner's Office (ICO) by, for example, giving the government powers to dictate the ICO's priorities and amend the ICO's salary without Parliamentary approval. In addition, new duties are proposed for the ICO to consider economic growth, innovation and competition when discharging its functions: these could allow more weight to be given to the interests of commerce than to the interests, fundamental rights and freedoms of data subjects. This cannot be right.

Our particular area of concern however is how the proposals will increase access and wider sharing of sensitive health data, and our response to the consultation will largely focus on questions relating specifically to this.

**Chapter One: Reducing barriers to responsible innovation**

**Q1.2.1a To what extent do you agree that consolidating and bringing together research-specific provisions will allow researchers to navigate the relevant law more easily?**

***KONP’s response: Strongly disagree***

The UK GDPR provides a clear legal framework to govern researchers’ responsible use of personal data. If researchers have any doubts about data protection rules, clear additional guidance from the Information Commissioner’s Office (ICO) will be more useful to researchers than further legal complexity.

The Government suggests that current data protection rules represent a barrier to innovation: this claim is undermined by the Government’s own acknowledgement that the UK is ranked only second in the world for science and research. At the same time, it is baffling how the Government can suggest that ‘responsible innovation’ can trump the rights and freedoms of individuals.

**Q1.2.2.a To what extent do you agree that creating a statutory definition of ‘scientific research’ would result in greater certainty for researchers?**

***Response: Strongly disagree***

Recital 159 provides clarity about the kind of research activities that are covered by the UK GDPR. The same Recital also provides enough flexibility to allow for future social and technological change without the need to amend the legal definition of ‘scientific research’. Our concern is that expanding the existing definition will allow it to include commercial activity and so damage public trust that personal data collected for research purposes will only be used in the public interest.

The government made two recent attempts to extract patients’ GP data without consent (initially through the exercise known as ‘care.data’ and then in what was described as ‘data grab’), with fears that this data could be made available to the private sector. This led to many patients ‘opting out’ - that is, refusing to allow their data to be extracted for any purpose, with potential implications for bona fide academic research. In addition, if it is known that sensitive health data is not collected exclusively in the public interest but potentially for commercial purposes, the risk is that patients’ trust in healthcare professions will be undermined and information from patients necessary for accurate diagnosis and treatment will be withheld.

A first necessary step to build the ‘health data solidarity’ that is essential for any world class data regime must be to distinguish very clearly public interest from private interest in all data use.

**Q1.2.6 To what extent do you agree that creating a new, separate lawful ground for research (subject to suitable safeguards) would support researchers to select the best lawful ground for processing personal data.**

***Response: Strongly disagree***

The UK GDPR already strikes an appropriate balance between the rights of individuals and the interests of researchers. We are concerned that this balance will be put at risk by the introduction of a new legal ground for research purposes.

Any new legal ground would have to maintain the fundamental distinction between publicly funded university research ‘in the public interest’, and the major legal duty of companies whose directors have to ‘act in the way they consider, in good faith, would be most likely to promote the success of the company for the benefit of its members as a whole.’ Any claim by private companies simply to be working ‘in the public interest’ would be seen as a façade and rapidly destroy public trust and public wish to share data, especially when accumulating company profits become evident. This means that the grounds for public and private research and the benefits they seek must be dealt with separately, so that the public can confidently choose where to place their data.

Researchers can be supported by user-friendly guidance from the ICO to decide on the best lawful ground for processing. This would allow researchers to meet legal requirements without affecting the legal protection currently available to individuals.

Great care must be taken not to develop a digital regime that runs counter to the potential for ‘global good’ that digital health possesses. This will occur if we support the development of powerful businesses and unfettered access to, and control of, data in order to achieve our government’s wish for ‘super-power’ status in AI technologies. Such actions to improve our economic and geopolitical competitiveness[[2]](#footnote-2) will put us in direct opposition to any global vision of universal health care[[3]](#footnote-3), and will help lead to the fragmentation of global governance approaches and erosion of multilateralism.[[4]](#footnote-4)

**Chapter Two: Reducing burdens on businesses and delivering better outcomes for people.**

**Q2.2.1. To what extent do you agree with the following statement: ‘the accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, and iii) be more risk-based’?**

***Response:* Strongly disagree**

We strongly disagree with the statement in Q2.2.1 People need certainty that their agreement for the use of their personal health data will be followed: for example, to be kept fully anonymised and/or used only in ways, and with organisations, that they have specified. Clear accountability rules are absolutely necessary for legal certainty and enforceability. Fewer prescriptive requirements will diminish the rights of individuals.

**Q2.2.1A. Please explain your answer, and provide supporting evidence where possible.**

We are concerned that the Government presentation within this proposal misreads the UK GDPR. Generally, responsibilities under the UK GDPR are influenced by the level of risk involved, with increased risk requiring stronger data policies and stronger data security.

The UK GDPR accountability framework is flexible and provides proportionate accountability depending on the ‘nature, scope, context and purposes’ of data use. This includes differences in the use of records; security measures (e.g. encryption and pseudonymisation); and contractual safeguards in ‘data use’ agreements. There are also a number of tasks that organisations only have to carry out if a certain risk threshold is met. Examples include: Data Protection Impact Assessments only for high-risk activities; notification of data breaches to the ICO only if they present a risk for individuals, and informing individuals only if they are likely to result in a high risk for their rights and freedom; Data Protection Officers being required only for public bodies or authorities, or for activities presenting a high risk for individuals.

Clear legal requirements are the only way to promote legal certainty, and organisations need that certainty in order to be sure that they know what they have to do in order to demonstrate compliance. This clarity is also needed to ensure that redress is enforceable when required for any individuals.

**Chapter 4: Delivering better public services**

**Q4.2.1. To what extent do you agree with the following statement: ‘Public service delivery powers under section 35 of the Digital Economy Act 2017 should be extended to help improve outcomes for businesses as well as for individuals and households’?**

***Response: Strongly disagree***

It is imperative to maintain the clear differences between public and private interests in the sharing and processing of healthcare personal data to enable ‘health data solidarity’. It is therefore extremely worrying that the Cabinet Office – currently driving changes to reduce barriers for sharing healthcare data with private companies - is directly influenced by the private sector. For example, the new Downing Street health advisor, Samantha Jones, comes straight from her role as CEO at Operose, the UK arm of the US health insurance giant Centene, which is gaining a significant presence in the NHS.

There is evidence that increasing the extraction of personal data by public and the private sectors can lead to a wide range of negative consequences for individuals and societies, ranging from human rights infringements and extensive surveillance practices to interference with electoral and other democratic processes.[[5]](#footnote-5) Health and health-related data represent an important aspect of these dynamics, with the health-care sector predicted to be the fastest-growing industry in terms of data produced..[[6]](#footnote-6)

The uptake of digital technologies in health and health care relies heavily on trust from patients, doctors, and other health system professionals.[[7]](#footnote-7) However, recent research suggests that such trust can be eroded by several personal, technological, and institutional factors, including fear of data exploitation, paucity of accessibility and digital skills, and poor reputation of service providers.[[8]](#footnote-8). We believe that any resource that is required to ensure that the processing of personal health data is compliant with full data protection is time, effort and money well spent.

The consultation document claims that the experience of fighting Covid has shown the power of using personal data responsibly in the public interest and the benefit of collaboration between the public and private sectors. However, we suggest that there has not always been transparency about the motivation behind this ‘collaboration’. It is not clear to us exactly what crucial/value for money roles the private sector have provided during the COVID-19 pandemic. In response to the statement ‘The UK’s experience of fighting the COVID-19 pandemic has demonstrated the power of using personal data responsibly in the public interest, and the benefits of collaboration between the public and private sectors’, we argue that this is not true. The notion that ‘There is an opportunity to build on this experience in order to deliver public services in more agile, innovative, effective and efficient ways’ we find a frightening thought.

We would like to offer the following evidence from ‘openDemocracy’[[9]](#footnote-9) research, the Public Accounts Committee and the Centre for Health and the Public Interest:

1. In March 2020, during the COVID-19 outbreak, the controversial technology company Palantir was contracted by the NHS to develop the NHS COVID-19 Data Store for £1. The contract was extended in June 2020 for 4 months for £1 million. The entire contract could have been worth up to £18 million a year over five years-totalling around £100 million. Google, Amazon, Microsoft and the AI firm Faculty all held contracts to work on the platform. A major concern was that the Government failed to publish the original contracts and only did so eventually in June, just before legal proceedings brought by ‘openDemocracy’ were due to start. In addition there were concerns being raised about how the private technology firms were using NHS data.

Palantir has allegedly ‘built software accused of fuelling racist feedback loops in the hands of the LA police’, and has come under fire from its own staff over its role in the US Immigrations and Customs Enforcement (ICE) agency’s ‘brutal policy of family separations’.

We agree with Mary Fitzgerald editor-in-chief of ‘openDemocracy’ that the lack of due process and the choice of Palantir ‘is no way to build trust or convince anyone that our government has the public interest at heart. It begs the question: what have they got to hide? Why are they so afraid of public scrutiny or debate over this?’

Also, we agree with Cori Crider, director of Foxglove, in being deeply troubled by the government’s lack of candour around these data deals. Despite promising a fair process that would let the public see what was at stake, the government pushed through another secret contract for two years. We too believe that the deals were no longer about the pandemic; rather they were about the future of our NHS. Transparency is critical and people do not want the NHS and our health data privatised by stealth.

On 11th September 2021, ‘openDemocracy’ reported that government had terminated a data deal with Palantir and was ‘seeking to move away from reliance on third party data analytics platforms and software’, this by using a system built by the British defence contractor BAE Systems. We also note that BAE, through its subsidiary BAE systems Inc, sells more to the US Department of Defence than to the UK Ministry of Defence!

1. Test and Trace (NHST&T) was set up in May last year with all components – administering tests, processing samples in laboratories, and contact tracing – contracted to private companies. This despite the existence of established testing facilities in established universities and hospitals. Multinational consultants Deloitte - who handle testing logistics including the collection of statistics - appointed outsourcing companies Serco, Mitie, G4S and Sodexo, together with the Boots pharmacy chain, to run drive-through or walk-in test centres. Between April 2020 and November 2021, Test and Trace was allocated a budget of £19. 7 billion.[[10]](#footnote-10) Yet despite ‘the unimaginable resources thrown at this project’ Test and Trace could not point to a measurable difference to the progress of the pandemic, and the promise on which this huge expense was justified - avoiding another lockdown – had been broken, twice. Not only this, there have numerous examples of incompetence on the part of companies awarded Test and Trace contracts. For instance, the government is facing legal action over the contract awarded to Immensa, a company without full UK accreditation, and responsible for around 43,000 false negative Covid results over a two-month period.[[11]](#footnote-11)
2. The Centre for Health and the Public Interest[[12]](#footnote-12) reported on 1st June 2021 that over the past year multi-billion pound contracts had been struck with the private hospital sector to provide services to NHS patients with the expressed intent of helping the NHS with extra capacity to clear the huge post-COVID backlog of patients waiting for treatment. But this language – which has been repeated across the media – concealed a crucial fact: the private hospitals could only do this work by using NHS consultants, as they had none of their own doctors. This falsity of the ‘helping the NHS’ narrative was only too clear from last year’s deal with the private sector with the NHS paying £400m a month for the private sector’s entire capacity, covering not only its running costs, but also all the interest payments on its debt, saving some companies from a serious risk of failure after COVID wiped out demand from private patients. But two-thirds of the private hospital’s capacity remained unused – a key reason being that many consultants, like other NHS staff, were redeployed to cope with COVID patients, and so were not available to work in the private hospitals. It is extremely difficult to see the benefit the public gained in this ‘collaboration’.

**Q 4.3.1 To what extent do you agree with the following statement: “Private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body’s lawful ground for processing the data under Article 6 (1) (e) of the UK GDPR?**

***Strongly disagree***

Chapter One of the consultation document indicates that work is already underway by the Cabinet Office to address barriers to data sharing and explore how to extend the public service delivery powers under Section 35 of the Digital Economy Act 2017 to the business sector. However, neither the barriers, nor the type of powers that might be extended to the business sector, are explained. Notably, Section 35 already allows for information sharing between public authorities (or specified persons providing services to public authorities) for specified public service delivery objectives, and additional objectives can be set by regulations. This could relate to a frontline service outsourced to a body outside the public sector but, in addition to conditions set out in the Digital Economy Act 2017, also involves consideration of whether such sharing of information is necessary to achieve the desired objective. In other words, it seems that the legal basis for sharing government-held data with the private sector already exists and the types of service delivery objectives can be extended when this is *in the service of a public authority*. Does the government wish to allow data to be shared with the business sector when this is *not* in the service of a public authority?

The consultation document suggests that there is a lack of clarity about the legal ground that private companies can rely on for processing personal data when this is at the request of public authorities. It cites, for example, the dilemma of data controllers who have to assess if the controllers’ interests outweigh the data protection rights of individuals, when wider public benefits are being sought. The consultation document therefore proposes that companies and others processing personal data on behalf of a public body can rely on Article 6 (1) (e) as the lawful ground for such processing, and other lawful grounds need not be identified.

Our concerns include

1. the consultation document itself makes it clear that private companies have generally been able to identify an appropriate legal ground for processing personal data when requested to help deliver public tasks, raising questions about the rationale for encouraging reliance on Article 6 (1) (e).
2. Article 6 of the UK GDPR provides a number of grounds on which processing can be deemed lawful. Article 6 (1) (e) says that processing is lawful where it is “necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller”. This implies that companies relying on this legal ground are controllers of data, rather than processors. According to the GDPR, the data controller (whether a natural or legal person, public authority, agency or other body) controls and is responsible for the data it holds. Alternatively, a data processor analyses the data for another organisation that decides and is responsible for what happens to the data. We argue that it is entirely inappropriate to allow a private company to hold NHS data and determine the purposes and means of processing it.
3. if the proposal really is that private companies should hold and control publicly collected personal data (rather than process it), determining the legal ground for processing is part of the important scrutiny of the data controller’s interests in relation to their responsibilities to individuals and their rights. Simply relying on A6 (1) (e) could introduce complacency.

Any blurring of the boundaries between public and private interests must be avoided to maintain public trust and ‘data solidarity’. When any companies work for the NHS they should do so under contract with UK GDPR protections for patient personal data safety, and shared data should not be used for any purpose other than that stipulated, should not be shared with third parties, nor should it be retained by the private company after the end of the contract.

We support the status quo that health data is classed as ‘sensitive personal data’ and should be subject to heightened safeguards. *It should only be processed where the individual has given explicit consent*and used when it is necessary for i) health, social care or public health purposes overseen by healthcare professionals; ii) other specified purposes, such as scientific research; iii) or it is necessary for other reasons of substantial public interest, as defined in Schedule 1 to the Data Protection Act 2018. Pragmatic and helpful guidance issued by the ICO should be used to remove any uncertainties.

**Processing health data in an emergency**

**Q4.3.3 To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?**

***Response: Strongly disagree***

The proposal risks undermining the additional safeguards governing the processing of sensitive personal data. This is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership, data concerning sexual activity or orientation as well as data concerning health, biometric or genetic data. Processing of such data is prohibited, unless appropriate legal grounds are identified under Article 9 of the UK GDPR (this is in addition to identifying a lawful ground under Article 6). Grounds allowing the processing of sensitive personal data include

* where an individual has given explicit consent;
* where it is necessary for reasons of substantial public interest, or
* where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems or services and
* purposes such as research carried out by or under the responsibility of a professional, subject to an obligation of secrecy.

The consultation document claims that during the pandemic, non-health bodies have had difficulty in identifying the relevant legal ground under Article 9. The government therefore “proposes to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health and other emergencies”. The existing legal grounds for processing sensitive personal data are already clear, and do not appear to have hampered access to health data for a range of companies during the pandemic. What the proposal seeks to do is further facilitate the private sector’s access to individuals’ sensitive personal data, without saying ‘how substantial public interest’ is to be defined, and what safeguards should be in place to protect the sensitivity of the data.

What constitutes ‘substantial public interest’? One of our concerns is that all sorts of future wishes could be reframed as ‘substantial public interests’. Perhaps our future economic certainty could be threatened by geopolitical competition, and we require access to large amounts of personal data to bolster our A.I. development in an attempt to achieve - to use the government’s terminology - ‘super power’ status. Widening the concept of ‘substantial public interest’ could be seen as the thin end of a very large wedge, especially when the amount of money to be made is huge according to the future financial figures for A.I. We believe that determining ‘substantial public interest’ should be guided by the ICO and its pragmatic approach. In addition we wish to see Article 6(1)(e) of the UK GDPR should be retained as the lawful basis of processing,

**Transparency mechanisms for algorithms**

**Q4.4.1 To what extent do you agree that compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data will improve public trust in government use of data.**

***Response: Strongly disagree***

Algorithms are not neutral tools: created by humans, they are inevitably value laden and designed with particular outcomes in mindthat will privilege some outcomes over others. In the health service, the growing dependence on algorithms runs the risk of undermining clinicians’ use of clinical judgement while relying on under-skilled staff who may not recognise when an algorithm’s decision is unsafe. Where algorithms are used, of course there needs to be transparency so they can be scrutinised for bias and other shortcomings. However, if the personal health data used to develop algorithms is extracted without individuals’ consent or appropriate safeguards, it is hard to see how transparency – for example about an algorithm’s technical specifications or which data sets it has used - will in itself improve the public trust in government use of data.

**Q4.4.5. To what extent do you agree with the following statement: ‘It may be difficult to distinguish processing that is in the substantial public interest from processing in the public interest’?**

***Response: Strongly disagree***

The ICO already clarifies the difference between ‘public interest’ and ‘substantial public interest’ and provides guidance on determining whether processing is in the ‘substantial public interest’.

The conditions for processing data in the substantial public interest are set out in Schedule 1 of the Data Protection Act 2018. Data controllers have to demonstrate that they meet the relevant condition.

1. The proposals will, for example, remove the requirement of human review of algorithmic decisions about the recruitment, management or dismissal of employees, making it more difficult for employees to address work related abuses and discrimination.

   [↑](#footnote-ref-1)
2. <https://www.cnbc.com/2021/09/22/uk-publishes-plan-to-become-ai-superpower-and-rival-us-and-china.html> [↑](#footnote-ref-2)
3. <https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(21)01824-9/fulltext> [↑](#footnote-ref-3)
4. <https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf#page46> [↑](#footnote-ref-4)
5. UN General Assembly. The right to privacy in the digital age: report of the United Nations High Commissioner for Human Rights. New York, NY: United Nations, 2018 [↑](#footnote-ref-5)
6. Reinsel D, Gantz J, Rydning J. The digitization of the world: from edge to core. Framingham, MA: International Data Corporation, 2018. [↑](#footnote-ref-6)
7. Vayena E, Haeusermann T, Adjekum A, Blasimme A. Digital health: meeting the ethical and policy challenges. Swiss Med Wkly 2018;148: w14571. [↑](#footnote-ref-7)
8. Adjekum A, Blasimme A, Vayena E. Elements of trust in digital health systems: scoping review. J Med Internet Res 2018; 20: e11254. [↑](#footnote-ref-8)
9. Fitzgerald M, Crider C. *Controversial ‘spy tech’ firm Palantir lands £23m NHS data deal Exclusive: UK government sneaks through new COVID data contract, despite legal challenges.* Open Democracy 21 December 2020 [↑](#footnote-ref-9)
10. <https://www.tussell.com/insights/covid?hsLang=en> [↑](#footnote-ref-10)
11. <https://www.theguardian.com/politics/2021/nov/01/law-group-threatens-to-sue-over-immensa-covid-testing-scandal> [↑](#footnote-ref-11)
12. Leys C. *Private hospitals have no doctors*. Centre for Health and the Public Interest June 1, 2021 [↑](#footnote-ref-12)