Implications of the revised Data Protection and Digital Information Bill (No 2) (DPDIB) for the NHS

1. Summary:

The changes in law in the DPDIB are intended to help government and business gain increased access to personal data. Such access may have greatest repercussions in the health sector where personal data is increasingly relied on for Government's aims to 're-design' the NHS and provide opportunities for its private 'partners'. It is clear from the Bill that the protections we have had for our health data in terms of privacy, transparency and consent are to be sacrificed to these ambitions. The Bill also gives new powers for the Secretary of State (SoS) to introduce changes to the data protection legal framework without properly consulting Parliament while undermining the role of the new Information Commission.

2. The issues:

2.1 Financial matters

NHS heath data has huge financial potential, and many private corporations such as Oracle Cerner, United Health / Optum, Centene/ Operose Health (see also the Report on US Healthcare Organisations given to Camden Social services, London) , and HCA are already accredited by NHSE (through the HSSF) or otherwise embedded within the NHS infrastructure in pursuit of profit. Many of these corporations, who are set to be 'major players' in our future healthcare services, have had numerous legal cases filed against them resulting in millions of dollars in fines-see 'US Violation Tracker'.

2.2 New technology, new practices, data privacy and our rights

As well as enabling the development of welcome science and technological innovations, our data provide the new 42 integrated care systems with the information and the new technologies needed to pursue their form of financially 'sustainable care'. In doing this, the use of the powerful new technology Artificial Intelligence (AI) brings threats to data privacy and 'opt out' as it requires the joining up of multiple data sets with maximal collection of data to work effectively. The use of AI to decide how services are rationed threatens transparency and our 'ability to debate' decisions as contained in our current system. Meanwhile transnational corporations with access to the NHS database may find it easier to move our identifiable data abroad and reprocess it without consent. Importantly, the loss of privacy for patients will undermine trust in health care professionals.

2.3 The potential impact of other proposed legislation

Although it is assumed that this Bill will co-exist with current legislation, there are serious concerns that the government is presenting this Bill despite knowing that the Retained EU Law (Revocation and Reform) Bill could revoke key elements of UK data protection law which are derived from EU law such as the UK GDPR , while the Bill of Rights Bill, if enacted in its current form, will have a fundamental impact on the DPDIB and devastate the existing data protection landscape.
Below we highlight the Bill's clauses that, if enacted, raise particular concerns.

3. How the Bill allows access and the use of our data:

3.1 *It will be easier to process our personal data*

Clause 1 introduces a **significantly lower protection for personal data** by amending Section 3A in the UK Data Protection Act 2018, and the definition of personal data. Under the UK GDPR, data are considered anonymous based on an objective test, reassessed at reasonable intervals, of whether an individual "can be identified, directly or indirectly". In this new Bill, personal data could be considered anonymous merely based on the circumstances and resources available to an organisation, or a subjective assessment of the possibility of re-identifying anonymised dataset only *at one point in time i.e. the time of processing* (see this especially in the context of para 3.5 below).

Clause 5 introduces a new lawful ground of "recognised legitimate interests" to process our data and gives the SoS power to designate a list of these interests 'where appropriate'. This removes the need for organisations to consider the impact of data use on individuals and the measures needed to mitigate such impact. **Clause 6** allows personal data to be processed, and reprocessed, without consent if it is for 'anything like' scientific, historical (genealogical) or statistical research - or anything else the SoS thinks appropriate.
Clause 9 introduces an exemption to the need for transparency in data processing for Research, Archive and Statistical purposes (RAS) where "providing the information is impossible, or would involve a disproportionate effort", and extends this exemption to "personal data obtained directly from an individual". **Clause 22** introduces new Articles empowering the SoS to amend safeguards for processing carried out for RAS purposes, including those forbidding the processing of personal data that is "likely to cause substantial damage or substantial distress".

3.2 *Accountability is reduced*

Clause 7 lowers the threshold for charging fees for individuals requesting information that an organisation holds on them and allows refusal of requests where it deems these to be "vexatious or excessive". What is "vexatious" includes, highly questionably "the [level of] resources available to the controller." New Article 12A(5) allows organisations to refuse requests that "are intended to cause distress" or "are not made in good faith", but how controllers will determine such beliefs is totally unclear. **Clause 14** removes the need to nominate an independent Data Protection Officer (DPO) and introduces new Articles 27A,B and C requiring public bodies or organisations processing large scale sets of sensitive data to appoint a "Senior Responsible Individual" from their own staff to be responsible for the data. This will, for example: reduce the independence of the data protection function, and remove the duty of secrecy and confidentiality DPOs must provide when giving advice on data protection.

3.3 *Easier use of automated decision making (ADM)* (i.e. without 'meaningful human involvement'). ADM is becoming integral to decision making in the planning and delivery of our care in our future 'health systems'.

Clause 11 introduces new Articles that initially protect special category data from ADM except in special circumstances, only then to empower the SoS to decide: what constitutes 'meaningful human involvement' in the definition of ADM, whether any decision is likely to have any significant effect on the subject concerned, and which safeguards to add, vary or omit.

3.4 *Less care will be taken with our data*

Clause 17 will amend "Data Protection Impact Assessments" to "Assessments of High Risk Processing" and exclude both the need to include any systemic description of the proposed processing operation and the need to consult with those who are affected by high risk data processing. This will legitimise data uses with unmitigated risk. Furthermore, **Clause 18** removes the requirement to consult the Information Commissioner before any data processing that represents a high risk.

3.5 *Identifiable data will be transferred abroad more easily and with less protection*

Clause 13 omits Article 27 of the UK GDPR, meaning that overseas organisations would no longer need to appoint a data protection representative within the UK, so making it harder to enforce UK data protection law against overseas organisations.
Schedule 5 of the Bill replaces Chapter 5 of the UK GDPR, and will change the legal bases under which personal data can be lawfully transferred, with New Article 45A empowering the SoS to make regulations approving transfers of personal data to third countries or international corporations, replacing 'adequacy' regulations under the UK GDPR. The amended Article 46 will allow transfer of personal data to countries **without such regulation** if they act "reasonably and proportionately".

There is no specified requirement to consider “public security, defence, national security and criminal law and the access of public authorities to personal data", or “the existence of an independent supervisory authority or effective judicial redress”.

3.6 *The Information Commissioner’s role in enforcement is diminished*

Schedule 13 and **Clause 100** abolish the office of the Commissioner and create a new ‘body corporate’ Information Commission under SoS control. The non-executive members appointed by the SoS must out-number the executive members (themselves appointed by the non-executives); and must consult the SoS before appointing a CEO; the pay of non-executive members is to be determined by the SoS; the executive members will be employees of the Commission; the Commission’s powers may be delegated to Committees; and the regime for dealing with vested interests will be weakened.

Clause 27 inserts new sections into Part 5 of the 2018 Act, that will change the Information Commissioner’s role. While the principal objective is to secure “an **appropriate** level of protection for personal data”, Section 120B introduces additional duties, such as regard for the desirability of "promoting innovation"; and "promoting competition". Such changes will compromise the ability of the Commissioner to fully enforce the GDPR, requiring instead the need to balance the enforcement of the laws against external interests.

Clause 28 gives new powers to the SoS to set out “the strategic priorities of His Majesty’s government relating to data protection, allowing the SoS to issue instructions to the ICO, and to interfere with their “objective and impartial application of the law”.

4. CONCLUSION: Data protection is a fundamental right that can impact on other rights; the monitoring and enforcement of effective data protection must be free from partisan or extra-legal considerations. The proposals of this Bill are unfit for purpose, dangerous, and damaging to the reputation of the UK. Some commentators say we have a duty to donate our data just as we donate our blood for the public good. This is a false analogy. These data protection reforms aim to make our data available for commercial benefit, while putting our personal privacy and right to consent at risk. The Government must not pursue these ‘reforms’.

What you can do:

MPs should ask questions about the repercussions of changes being made to our Data Protection laws and, specifically, the consequences to care, transparency of decisions to deny care, and the privacy of our personal data- including with new technologies such as AI- and the suggested easing of access to personal data and the ability to move data abroad. MPs should consult the ‘US Violation Tracker’ for entries of corporations who are to be part of our future healthcare services. They should also ask their legal experts to consider the potential that the two Bills mentioned above, under point 2, may have to affect our protections and rights.

Contact the KONP Health Data Working Group at **konpdataworkinggroup@gmail.com**

Briefing posted on https://keepournhspublic.com/data-bill-actions-to-take/