Labour's Data Use and Access Bill and the use of NHS data

Keep Our NHS Public (KONP) Briefing

December 2024

OVERVIEW

The Data (Use and Access) Bill (DUA), introduced in the House of Lords in October 2024 and aiming to "harness the power of data", is central to the Government's strategy for economic growth. It retains many of the provisions of the previous Data Protection and Digital Information Bill (DPDI) that fell before the general election, which means that much of the new Bill's content has already been discussed. Because of this (and due to the consequences of starting its journey in the Lords) the Bill is expected to progress rapidly through Parliament with little scrutiny, even though it contains new provisions that will lower important data protections.

The DUA includes proposals about data sharing, digital ID, Smart Data, digitising key public registers and assets, as well as amending data protection laws. Although the Bill raises many concerns, this briefing focuses on its implications for the NHS, its patients and their personal health data.

If unamended, the Bill is likely to undermine the public's trust in the way their personal health data is used. The Bill also weakens the role of Parliament: a large number of its proposals contain little detail but instead give considerable power to the Secretary of State (SoS) to create new provisions via Statutory Instrument.

KEY ISSUES

i) SPECIAL CATEGORIES OF DATA

Special category data is sensitive information (for example about an individual's health, genetic make up, or political views) that needs protection. The existing UK General Protection Data Regulation (GDPR) sets out a comprehensive list of special categories of personal data, and processing of data covered by this list is prohibited unless certain conditions are met.

The DUA will enable the SoS to add new special categories and change the conditions governing their use, as well as to remove certain categories and add new definitions, arguing that this power will allow the Government to respond quickly to future technological developments or societal change. On a positive note this could, for example, allow the protection of neurodata (i.e. data increasingly gathered directly from a person's neural system, including the brain and nervous system) by its inclusion in the list of protected categories. However, the DUA would equally enable the removal of such new categories in future without proper debate. The overall impact of this SoS power is hard to predict.

ii) FURTHER DATA PROCESSING FOR RESEARCH

The DUA will amend the definition of 'scientific research' to facilitate the processing of data for any research, whether this is publicly or privately funded or a commercial or non-commercial activity – as long as the research can broadly be described as 'scientific'. The criteria for determining what is 'scientific' are not clear. The proposal fails to acknowledge evidence showing that people are generally in favour of sharing their data in the public interest but not for private profit.

Consent to the use of one's data for a particular research project will automatically be taken as consent for its use in future research projects, even if the nature of these projects is unknown at the time. This runs counter to guidance from the Information Commissioner's Office calling for transparency on how personal data is used.

It is notable that, in its consideration of the Bill, the Lords' Constitution Committee stated that "[d]ata protection is a matter of great importance in maintaining a relationship of trust between the state and the individual", and that the power to use personal data should not become so broad as to unduly limit the rights of the individual.

iii) ARTIFICIAL INTELLIGENCE (AI)

During the second reading in the Lords, concerns were expressed about failure to ensure greater transparency over the use of AI systems for processing personal data. There were also fears that broadening the definition of 'scientific research' could encourage AI companies to go beyond the intention of the Bill and create data-driven AI products under the guise of scientific research. Others might think that this is precisely the intention of the Bill.

iv) AUTOMATED DECISION MAKING (ADM)

ADM refers to the use of data, machines and algorithms to make decisions in a range of contexts, including health care, with little to no human oversight. ADM can involve profiling – i.e. where ADM uses personal data to analyse or predict someone's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. In the context of the NHS, ADM may be used, for example, in individual patient assessments and triage.

The Bill includes provisions to expand the lawful base for the use of solely automated decision making. Companies will no longer be required to demonstrate why ADM is allowed. Instead, ADM can be used to subject an individual to an automated decision without their consent: if the Bill is passed, it will be up to individuals to enforce their rights, even though they may be unaware that an automated decision has been made.

Until now, governments and corporations have been prevented from using ADM to make decisions that will have legal or other significant effects on an individual. The Bill clarifies that a decision will qualify as being based solely on automated processing if there is no meaningful human involvement in the decision, and it will qualify as being 'a significant decision' if it produces a legal or similar significant effect for the data subject.[1] However, the Bill will give the SoS new regulatory powers to determine when decisions have meaningful human involvement and to decide what is, or is not, a significant decision in the face of new technologies and changing societal expectations.

It appears that existing restrictions on the use of ADM where special category data is involved remain largely unchanged.

According to the BMA, where ADM might be used in a healthcare context, such as the allocation of resources, "use of the SOS's regulation-making powers could have a significant negative impact on some patient groups – for example, if the funding of services favours certain patient groups or geographical areas at the expense of others".

v) *DATA SHARING*

The Bill aims to increase access to the data held by public bodies and make it easier for organisations to share data. This means that data collected for one reason, such as healthcare, may be shared with public authorities and private companies who may use it for something else**,** such as immigration control or predictive policing. This risks undermining the public's trust concerning the use of their data, prompting individuals to 'opt out' of data sharing. This would mean their data could not be used for research and development intended for the common good.

[1] According to the GDPR, a 'data subject' is an "identified or identifiable natural person" from whom (or about whom) information is collected.

Currently, when a data controller[2] intends to reuse personal data for a separate purpose beyond that for which it was originally collected they must provide additional information to the data subject. The Bill creates an exemption in the case of processing for research, archiving and statistical purposes where this involves a 'disproportionate' effort to provide the required information to data subjects. A list of factors is provided to help the data **c**ontroller determine what constitutes a disproportionate effort but ultimately this is a subjective process.

Like its predecessor, the Bill aims to make it easier to transfer personal data across borders. It introduces a 'data protection test' that allows transfer if the standard of data protection in the recipient country is 'not materially lower' than in the UK.

TO CONCLUDE

The Bill contains proposals that will undermine the public's trust in the use of their personal data, at the risk of limiting the data available for the public good. Proposals concerning ADM risk significant negative impacts on some patient groups or geographic areas, while the Bill will make it easier to use patient data for non-health applications and to extract patient data for private sector exploitation. KONP urges the government and the House of Lords to provide meaningful scrutiny of this Bill and ensure amendments that will address the concerns above or, if such amendments are not agreed, to vote against the Bill.

Keep Our NHS Public is a non-party-political organisation campaigning against the privatisation and underfunding of the NHS.

[2] A 'data controller' is a legal or natural person, an agency, a public authority, or any other body who, either alone or with others, decides on the use of any personal data and how its processed.