Data Protection and Digital Information Bill Briefing
KONP Working Group
(August 2022)

KONP is a non-party political organisation campaigning against the underfunding and privatisation of the NHS, including the privatisation of NHS data. We do not contest the value of data in improving treatments, planning and service provision. However, we have deep concerns that the Data Protection and Digital Information Bill will have serious implications for how health data is used and how data protections will be undermined.

The briefing outlines clauses and schedules in the Bill that have particular significance for healthcare data (including sensitive health data), and their consequences. (# denotes those clauses granting Henry VIII powers that are particularly relevant to health data.)

To support our analysis, further information about these clauses and other more general clauses of concern are provided here.

Clauses relevant to healthcare data
(numbers and wording that identify the Clauses in red)

1 Information relating to an identifiable living individual (Redefining 'anonymous' data)

Data controllers or processors will be able to decide that personal data currently classified as 'pseudonymous' and therefore safeguarded by legislation can be reclassified as 'anonymous' (and therefore unprotected by legislation), simply because at the time of processing they decide that it will take more than a 'reasonable' amount of time for anyone to reidentify it in future.

2 Meaning of research and statistical purposes (Redefining 'scientific' and 'historical 'research)

Scientific research becomes anything that can 'reasonably' be described as such, enabling (for example) the use of personal data for commercial research, so risking the undermining of trust and certainty about legitimate medical research.
Historical research includes genealogical research, which nowadays can include DNA research. This kind of genetic information is currently classed as a special category requiring extra safeguards because its use is open to abuse (including of human rights). The Bill allows the Secretary of State powers to amend safeguards for processing this and other forms of sensitive personal data.[1]

3 Consent to processing for the purposes of scientific research

Consent to use data for 'new' uses will be assumed if it is for anything 'reasonably' described as scientific research, including avenues of research that had not been realised when consent was originally given.

5 Lawfulness of processing

Private companies will be able to process data if they have any 'legitimate interest' which the Secretary of State recognises. The Bill proposes an initial six examples of 'recognised' legitimate interests in Annex 1 (with more to follow)- these do not require data users to conduct a 'legitimate

[1] http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DPBill_GWbrief_Feb18.pdf

interest test' to clarify purpose, necessity and the balance of processing against the individual's interests, rights and freedoms.

6 The purpose limitation (Transparency about reasons for obtaining personal data) #

Personal data can be processed, including reprocessing, without consent if it is for 'anything like' scientific, historical (genealogical) or statistical research or anything else the Secretary of State thinks appropriate by amending Annex 2, even when the data can be re-identified. Purpose limitation is one of the seven Core Principles of the UK GDPR.

7 Vexatious or excessive requests by data subjects

Currently individuals have the right to request a copy of the data an organisation holds on them. The Bill allows a data controller to refuse to deal with a request, or charge a fee, if they consider the request to be 'vexatious' or 'excessive' which includes the fact that they do not have enough resources to deal with requests. It also appears that when assessing 'intent to cause distress', 'making in bad faith' and 'abusing process' the wider context in which a subject request is made – such as litigation proceedings – may be taken into account.

9 Information to be provided to data subjects

Data controllers do not have to inform data subjects about further processing of their data if it is for anything 'reasonably like' scientific or historical (genealogical), archiving or statistical research and if it involves too much effort on their part.

10 Data subjects' rights to information: legal professional privilege exemption

The data controller does not have to tell the data subject how their data is being used if that use is in the context of a duty of confidentiality by a legal adviser to a client such as is seen in commercial contracts used in the development of products.

14 Senior responsible individuals

Organisations can now monitor their own compliance with data protection legislation with an employee taking on the role of a 'senior responsible individual'. This replaces Data Protection Officers (independent, data protection 'informed' individuals). If organisations have fewer than 250 employees, then they do not have to keep records- which are usually helpful in showing compliance.

17 Assessment of high-risk processing and 18 Consulting the (Information) Commissioner prior to processing

'Data Protection Impact Assessments' will be replaced with 'Assessments of High-Risk Processing' and organisations will be allowed to conduct risk assessments on their own terms-see Clause 14. Data subjects will not be consulted and the data watchdog the (Information) Commissioner does not have to be consulted about 'high-risk processing without mitigation'.

21 Transfers of personal data to third countries and international organisations

The Secretary of State may by regulations approve the transfer of personal data to a third country or an international organisation; and by making regulations on this, the Secretary of State may consider

any thing they think to be relevant, including 'the desirability of encouraging transfers of personal data to and from the United Kingdom' (Article 45A (3)).

The Secretary of State may also, by regulations, write 'standard data protection clauses' which they consider will pass the 'data protection test' necessary for the transfer of personal data, and they may also decide the levels of safeguards that may be relied on to enable transfers.

22 Safeguards for processing for research etc purposes #

Processing of personal data may not be carried out if it is likely to cause 'substantial damage' or 'substantial distress'. However, the Secretary of State can use regulations to decide the meaning of any 'substantial distress'.

27 Duties of the (Information) Commissioner in carrying out functions

As well as trying to protect personal data and promote public trust, the (Information) Commissioner must have regard to promoting innovation, the need to promote (business) competition, the need to act against criminal offences and the need to safeguard public and national security. The Commissioner must develop a strategy with all these things in mind and must consult other regulators about how the strategy may affect economic growth, innovation and competition, and review the strategy and revise it as appropriate.

28 Strategic priorities

The Secretary of State may set out the strategic priorities of Her Majesty's Government in relation to data protection (which will include economic, commercial and political wishes); the Commissioner must consider supporting these and explain how they will do so.

29 Codes of practice as to the processing of personal data; 30 Codes of practice: panels and impact assessments #; 31 Codes of practice: approval by the Secretary of State

The (Information) Commissioner must prepare Codes of Practice giving guidance as to good practice in the processing of personal data if required to by the Secretary of State having consulted them and 'appropriate others' beforehand.

The Commissioner must establish panels of experts and those likely to be affected by the code to consider it and write a report. The Commissioner must alter the code in the light of the report. The Secretary of State may by regulations make a final decision to approve the code.

32. Vexatious or excessive requests made to the Information Commissioner; 40 Power of the Commissioner to refuse to act on certain complaints

The (Information) Commissioner may refuse to act on a complaint if, where appropriate, the data subject has not already approached the relevant data controller, or if the controller has not finished handling the complaint, or if the complaint is deemed to be vexatious or excessive as demonstrated by the Commissioner.

SCHEDULE 13 The Information Commission Section 100 #

In the new 'body corporate' Information Commission that will replace the ICO, the non-executive members appointed by the Secretary of State must out-number the executive members appointed

by the non-executives; the Commission's powers may be delegated to Committees; and if any member has 'a declared interest' this may be disregarded by a unanimous vote of members present.

More information about the KONP Data Working Group can be found at
https://keepournhspublic.com/health-data-working-group/