Written evidence submitted by the British Medical Association (BMA) (DUAB39)

Public Bill Committee on the Data (Use and Access) Bill

About the BMA

The BMA is a professional association and trade union representing and negotiating on behalf of all doctors and medical students in the UK. It is a leading voice advocating for outstanding health care and a healthy population. It is an association providing members with excellent individual services and support throughout their lives.

1. Summary

1.1 The BMA's focus on the Government's wide-ranging Data (Use & Access) Bill is its impact on the processing of 'special category' health data, i.e. identifiable health data. Patients and the public rightly expect high standards of data processing, to protect their confidential health data.

1.2 We strongly welcome the provisions in the Bill that will drive forward something that the BMA has long called for: a requirement on IT suppliers for the health and care sector to ensure their systems meet common standards to enable data sharing across platforms. We hope this will achieve the Government's stated ambition of freeing up 140,000 hours in NHS staff time every year, providing quicker care for patients and potentially saving lives. **We would like to see this requirement on software suppliers to the NHS and adult social care to be extended to include healthcare providers in the armed forces to achieve parity for them.**

1.3 **We urge MPs to amend outstanding aspects of the Bill that could dilute existing high standards of data processing, risking the protection of confidential health data:**

- **Clause 77** risks eroding transparency about how patient information is used – the National Data Guardian has also raised this concern
- **Clauses 117-120 & Schedule 14** appear to risk eroding regulatory independence and freedom
- **Clause 80** risks eroding trust in AI
- **Clause 70** risks diluting protections for health data held by non-public bodies

1.4 With these issues in mind, it is essential that the direction the UK is taking with this Bill will not lead to the loss of data adequacy status with the EU, which would put at risk the continued free flow of personal data between the EU and the UK. Maintaining this data flow is critical to medical research and innovation, including important clinical trials.

1.5 If the EU were to conclude that data protection legislation in the UK was inadequate, this would present a significant problem for organisations conducting medical research in the UK. Losing our data adequacy status with the EU would far outweigh any perceived benefits that might be achieved via the Government's proposed reforms.

2. NHS digitisation – driving forward interoperability across the NHS

2.1 Regulation, adoption and enforcement of information standards – Schedule 15

2.2 **We welcome the Bill's proposal to ensure that the technical foundation is in place to cultivate greater, and easier, data sharing across the healthcare system for the benefit of doctors and their patients.**

2.3 **Currently,** although successive governments have aspired to implement standards for how data is processed across the NHS, none have followed this with any regulatory mechanism that would mandate such standards. As a result, and due to historic and ingrained practices, third party 'private' software suppliers to NHS provider organisations are neither obliged nor motivated to design the products that they sell in such a way as to make them interoperable – which is to say that by and large, software developed by one supplier is unlikely to function effectively or at all with products developed and sold by rival suppliers.

2.4 **This Bill** proposes to bring into law measures that the BMA has long called for across successive budget and spending review submissions, and in written publications[1,2] – chiefly, that commercial suppliers must bear the burden for improving interoperability within the NHS by conforming to information standards set by the NHS.

2.5 The impact of successfully implementing this measure cannot be overstated. In time, it would mean that different IT systems used within a single trust would be able to routinely share and store patient data – currently it's not possible to share even the most basic information between different departments on the same site.

2.6 In a BMA survey[3] from 2022, just 5.1% of doctors felt 'very confident' that they would be able to seamlessly share data in 10 years' time, with 27.3% not at all confident. This measure speaks directly to those concerns and will go a significant way to ensuring that the technical foundation is in place to cultivate greater, and easier, data sharing for the benefit of patients.

2.7 It is commonplace in other sectors, where the primary buyer is the state, for standards to be enforced on suppliers – defence contractors in NATO-aligned countries, for example, must adhere to thousands of mechanical, technical, and digital standards when designing new platforms. It is only natural that the NHS take advantage of its position as the biggest single buyer of medical information systems to make for-profit companies work for the benefit of clinicians and their patients – rather than the other way round.

2.8 Armed Forces – achieving parity

2.9 **We are calling for an extension of the requirement placed on software suppliers to the NHS and adult social care, to meet centrally set technical standards, to include healthcare providers in the armed forces.**

2.10 The same software suppliers sell to the NHS and to the armed forces health sector; therefore, the same requirements should apply in both cases.

2.11 The armed forces health sector suffers from many of the same problems as colleagues in the NHS, with limited interoperability hampering their ability to share vital patient information. Patients within the armed forces often find themselves moving between civilian and military care with important medical data expected to follow them around in a way that is easily accessible. We would, therefore, expect that centrally set standards would apply in such a way as to ensure that systems in use in both settings can easily exchange information. Fundamentally, this change would ensure parity between civilian and military state provided healthcare.

3. Data protection standards – specific concerns to address on the face of the Bill

3.1 Eroding transparency – clause 77

3.2 **We believe clause 77 should be removed from the Bill, due to our concerns that it will water down the transparency of information to patients. The National Data Guardian has also raised concerns about the 'weakening of transparency obligations' in this clause. We are grateful to Peers for raising the issue at the Lords' Committee Stage, and to MPs for raising it at second reading; we hope that our concerns will be addressed in the Commons.**

3.3 **Currently,**[4] data controllers must provide individuals with information about the collection and use of their personal data. These transparency obligations generally do not require the controller to contact each individual data subject. Such obligations can usually be satisfied by providing privacy information, using different techniques, that can reach large numbers of individuals – such as relevant websites, social media, local newspapers, etc.

---

[1] www.bma.org.uk/media/4565/bma-response-nhsx-draft-data-strategy-sept-2021.pdf
[2] www.bma.org.uk/media/6578/bma-infrastructure-2-report-getting-it-right-dec-2022.pdf (p 20)
[3] www.bma.org.uk/media/6578/bma-infrastructure-2-report-getting-it-right-dec-2022.pdf
[4] Article 13 of the UK GDPR

3.4 **The Bill** (clause 77) disapplies the existing requirement to provide information to data subjects when personal data is processed for a further, separate, purpose if it is for scientific research and would require 'disproportionate effort' to provide this information.[5]

3.5 We are deeply concerned that this provision will water down the transparency of information to patients. Any reduction in transparency requirements is a backward step in terms of promoting confidence in the use of health data, given the very close relationship between transparency and public trust. It contradicts the approach in the recently published ICO guidance about improving transparency in health and social care.[6] Disapplying transparency requirements is contrary to societal expectations – more, not less, transparency is required to build and maintain public trust – and reducing transparency is also in direct contradiction to the National Data Guardian's (NDG) advice that there should be 'no surprises'[7] for patients about how and why their data is used.

3.6 Furthermore, one of the factors listed in the Bill which has a bearing on whether 'disproportionate effort' is required is 'the number of data subjects'.[8] The implication, therefore, is that the more individuals whose personal data is being collected, the easier it will be for controllers to apply the exemption to provide information i.e. more processing means less transparency. This is a deeply concerning direction of travel.

3.7 Given that the existing transparency obligations generally do not require contact to be made with each individual data subject, it is hard to envisage how using methods that can reach large numbers of individuals at once would require disproportionate effort, such that it would impair the progression of research. Conversely, failure to be transparent may impair research if a loss of public trust occurs.

3.8 **We urge MPs to act on the National Data Guardian's shared concerns over this matter:** *"…I am concerned with the weakening of transparency obligations in Clause 77 of the Bill. Transparency is a fundamental aspect of earning and maintaining public trust in health and social care data use. As such, any weakening of transparency obligations has the potential to negatively affect people's trust in how health and social care data is used for research. Any erosion of public trust would negatively affect public perceptions of, and sentiment towards, important ongoing and forthcoming health data initiatives…"*

4. Eroding trust in AI – clause 80

4.1 **The BMA urges MPs to remove the regulation-making powers in the Bill which would allow the Secretary of State to ignore or dilute statutory protections that apply to automated decision-making.**

4.2 **Currently**, Article 22 of the UK GDPR provides data subjects with a right not to be subject to decisions solely based on automated decision-making (subject to certain exemptions).[9] As such, a controller carrying out solely automated decision-making must implement certain measures to safeguard the data subject.

4.3 **The Bill** (clause 80) clarifies and makes more explicit the Article 22 safeguarding requirements which apply to automated decision making – for example, individual patient risk assessments and triage decision-making. However, we are concerned that the Bill also gives the Secretary of State considerable powers, via secondary legislation,[10] to amend or set aside these Article 22 safeguards.[11]

4.4 New Article 22D says: *"The Secretary of State may by regulations provide that, for the purposes of Article 22A(1)(a),[12] there is, or is not, to be taken to be meaningful human involvement in the taking of a decision in cases described in the regulations."* We understand this to mean that the Secretary of State can make regulations which say that it is for the Secretary of State to decide whether a particular decision had

[5] See clause 77

[6] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-publishes-guidance-to-improve-transparency-in-health-and-social-care/

[7] See Caldicott Principal 8

[8] See clause 77

[9] Article 22(1) right which is as follows: *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*

[10] Subject to the affirmative resolution procedure

[11] See clause 80(1), new section 22D

[12] New Article 22A(1)(a) says: *"For the purposes of Articles 22B and 22C— a decision is based solely on automated processing if there is no meaningful human involvement in the taking of the decision…"*

meaningful human involvement or not. The effect of this is that the Secretary of State can use regulations to make certain automated decision-making processes immune from the restrictions in Article 22. We are very concerned that this risks these decisions being made on political, rather than technical, grounds.

4.5 Where automated decision-making might be used in a healthcare context, such as the allocation of resources, use of the 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. Under this Bill, those patients who are disadvantaged by the automated process would not be able to rely on the relevant Article 22 safeguard.

4.6 Whilst the Secretary of State will require a degree of flexibility to amend legislation in an area of fast-paced technological change, fundamental statutory protections must not be placed in jeopardy in the interests of increased flexibility. If the public is expected to have trust in AI technology, and in those companies and institutions holding and processing large quantities of health data, AI must operate with safeguards on which the public can rely, and which cannot be reduced for political expediency. It is, therefore, crucial that any new law in this field must not have the effect of reducing the level of protection provided for by the existing data protection law.

5. Points for clarification

5.1 Risk of eroding regulatory independence and freedom – clauses 117-120 and Schedule 14

5.2 **We would welcome clarification from the Government as to how the independence (and perception of independence) of the new Information Commission (IC), to replace the existing Information Commissioner's Office (ICO), can be maintained with the proposed new governance structure. We have concerns, however, that the proposed new structure could severely hamper and dilute the ICO's regulatory independence by exposing it to political direction or government interference.**

5.3 **Currently,** the ICO is the UK's independent regulator for data protection legislation. The ICO's role is to hold to account all organisations which process personal data, including the Government.[13] The formal powers and duties of the ICO rest with the Commissioner – the Commissioner currently has powers to appoint deputy commissioners and other officers.[14]

5.4 **The Bill** (clauses 117-120) abolishes the current ICO role and replaces it with a corporate body called the Information Commission (IC). The Information Commissioner would transition to the role of chair of the Information Commission. Schedule 14 inserts a new Schedule 12A into the DPA 2018, which makes further provision about the new body, including:

Non-executive members

- The chair of the IC is to be appointed from the non-executive members on the recommendation of the SoS (Schedule 14, new schedule 12A para 3 (2)(a) and (b)).
- The SoS will appoint non-exec members (Schedule 14, new schedule 12A para 3 (2)(b)).

Executive members

- Executive members may be appointed by non-executive members (Schedule 14, new schedule 12A, para (3)(3b)).
- Executive members will include the chief executive who is to be appointed by the non-executive members (Schedule 14, new schedule 12A, para (3)(3a)) – following consultation with the SoS (Schedule 14, new schedule 12A, para (3)(5)).

5.5 The salaries of the non-executive members will be determined by SoS (Schedule 14, new schedule 12A, para (10)).

[13] The ICO notes his independence from government in his briefing on the Bill: https://ico.org.uk/about-the-ico/the-data-use-and-access-dua-bill/information-commissioner-s-response-to-the-data-use-and-access-bill/

[14] Data Protection Act 2018 Schedule 12, para 5

5.6 These provisions appear to mean that the Government has increased powers over appointments to the IC – it would have the power to directly[15] or indirectly[16] make the senior appointments to the new IC, as well as deciding their salaries (without measures for Parliament to approve appointments). In addition, the ICO's powers to appoint deputies and officers also appear to be removed.[17] We would welcome clarification on whether this understanding is correct. If correct, we believe the proposed new structure and appointment procedures could allow the Secretary of State to have considerable ability to affect the ICO's approach to its regulatory and enforcement activities.

5.7 Such an outcome would severely hamper and dilute the regulatory independence of the ICO by exposing it to political direction or government interference. At the very least, the perception will be that increased Government powers over appointments (and remuneration) will result in a weakened regulatory regime, where the Government will be viewed by the public as less accountable or less likely to incur sanctions than others. We would welcome clarification from the Government how the independence (and perception of independence) of the IC can be maintained with the proposed new governance structure.

5.8 It is especially important that the regulation of health data is not subject to government interference. To maintain public confidence there must be clear separation between the regulation of data and those who might wish to use it or access it, including government. In the event of data misuse, the regulator must be independent (and perceived to be independent) with the freedom to stand up for the public even in the face of government pressure.

6. Lawfulness of processing – clause 70 & Schedule 4

6.1 **The BMA is concerned that health data held by non-public bodies is included within the scope of clause 70 – we urge the Government to exclude health data from this new 'recognised legitimate interests' lawful basis for processing, which would be consistent with the Government's confirmation that the NHS is excluded (as a public body). We are grateful to Lord Clement-Jones for raising this issue at the Lords' Committee Stage and we urge MPs to make this amendment.**

6.2 **Currently,** if a data controller is relying on the 'legitimate interests' ground for lawful processing, usually, they must carry out a 'legitimate interests assessment' (LIA). The ICO sets out a three-part balancing test for applying an LIA:

- The purpose test (identify the legitimate interest); and
- The necessity test (consider if the processing is necessary); and
- The balancing test (consider the individual's interest)

6.3 **The Bill** (Annex 1, Schedule 4) introduces a new list of 'recognised legitimate interests', which are processing activities that the Government has judged to automatically satisfy the existing legitimate interests balancing test – it appears that the intention is to remove the need for the data controller to carry out an LIA or consideration of balance.

6.4 *Health data held by non-public bodies:* we welcome confirmation from the Government, at Committee Stage, that public bodies such as the NHS are excluded from this new 'recognised legitimate interests' lawful basis for processing. However, we understand that health data that is held by non-public bodies is not excluded. It is not clear whether GP practices would be covered by this exclusion – we would welcome confirmation from the Government that data held by GP practices is excluded.

6.5 We would be extremely concerned if health data held by NHS GPs, private healthcare organisations, and other non-public bodies would no longer be subject to the ICO's balancing test. We are concerned this would significantly dilute the protection of health data held by these organisations. Without the requirement to consider the question of balance and reasonable necessity we are unclear how data

[15] It appears the Secretary of State will appoint all the non-executive members of the IC.

[16] The executive members of the IC are appointed from the non-executive members (which have been appointed by the Secretary of State).

[17] Clause 116 (7) omits Schedule 12 from the Data Protection Act 2018. It is Schedule 12 (5) which gives the Commissioner powers to make appointments.

controllers of health data in non-public bodies will be able to reassure patients they have a valid justification for processing.

6.6 It is also unclear how this provision might affect the rights of data subject (patients), including the right to object to processing.[18] **We would, therefore, request that the Government excludes health data from clause 70.**

7. Opportunity presented by the Bill

7.1 Data subjects' access requests (SARs) to their medical records – clause 76

7.2 **The BMA urges MPs to use this Bill to address a unique issue for GPs, who are personally bearing the cost of SARs after the pre-GPDR administrative fee was abolished. Adequate resourcing must be provided to help GP practices facilitate this important right for patients i.e. that patients can access their medical records.**

7.3 **Currently**, as a result of changes implemented by GDPR (implemented in the UK through the Data Protection Act 2018), if a patient wishes to access their medical records held by their GP, there is no resource for this work – the administrative fee that was in place prior to GDPR (up to £50) has been abolished. However, it has not been considered how this blanket change in policy would impact on GPs versus other record holders (such as utility companies). We know from our members that SARs in general practice are now at least a weekly occurrence in an average sized practice, if not more frequent. The lack of resourcing for this important right for patients is having a knock-on impact on the available time for patient-facing services and delaying essential clinical administrative work.

7.4 Medical records are not merely a collection of clinical facts, but a personal life diary of the patient concerned. They may include highly sensitive information or 'third party' or 'harmful information', such as sexual, social, relationship, safeguarding, third party, and psychiatric data. The format of medical records is a mixture of handwritten notes, typewritten letters, and electronic notes – often with copious free text stretching back many years and often a lifetime. Legacy notes from pre-2004, and many hospital letters since 2004, have never been digitised and, therefore, the production of copies of medical records is a labour-intensive operation. A GP must then read the entire set of notes, redacting as appropriate, followed by the redacted set being re-photocopied to ensure confidentiality.

7.5 Members have previously told us that the average size of a record requested was 300 sheets of A4, printed twice – once for redaction and then once post-redaction. Printing and postage costs, alone, amounted to almost £20 per application – and the administrative cost increases further to around £40 when taking into account staff time for photocopying 300 sheets twice. This does not even include the doctor's time involved; each request can take an average of 80 minutes of a doctor's time to scan for 'third party' or 'harmful' information. This is a costly and time-consuming activity, undertaken in addition to routine clinical duties.

7.6 Furthermore, the General Medical Council places strict obligations on registered medical practitioners concerning patient confidentiality – any breach of confidentiality lays doctors open to the most severe professional sanctions, in addition to any civil legal proceedings by third parties and criminal proceedings by the Information Commissioner. In dealing with SARs, current redaction software is insufficiently discriminating to be of general use, meaning manual redaction is the only recourse.

March 2025

For further information, please contact:
Holly Weldin, Senior Public Affairs Officer
E: publicaffairs@bma.org.uk

[18] UK GDPR Art 21(1) states that a data subject shall have the right, on grounds relating to his or her personal situation, at any time to object to the processing of personal data concerning him or her which is based on point (e) or (f) of Art 6(1). Although the right to object is not absolute, where an objection is raised, data controllers can only continue to process personal data subject where they can demonstrate 'compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject' (UK GDPR Art 1 (1)).