Parliamentary brief
bma.org.uk

BMA

Data Protection and Digital Information Bill

Second Reading, House of Lords
19 December 2023

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.

Key points

The BMA's focus on the Government's wide-ranging Data Protection & Digital Information 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, and we have serious concerns that the Bill could dilute these standards and protections.

We urge Peers to challenge the problematic provisions and to seek reassurances and revisions from the Government. We are concerned that:

- Some of the Bill's proposed reforms represent a **departure from the existing high standards of data protection for health data**, and not enough emphasis has been placed on the public's expectations as to how confidential health data is handled – concerns that were highlighted in the House of Commons[1]. Specifically:
    - Clause 11 risks eroding transparency of information to data subjects
    - Clauses 32, 35 & 143–144 risk eroding regulatory independence and freedom
    - Clause 1 risks eroding protections for data by narrowing the definition of 'personal data'
    - Clause 14 risks eroding trust in AI
    - Clause 17 risks eroding the expertise and independence of organisational oversight
    - Clause 20 & 21 risk eroding organisational data governance

- **A failure to consider the negative impact of losing public trust** in how the healthcare system manages data would be to the detriment of data quality – both for the safety and effectiveness of individual care, and for system-wide research and scientific development.

- This departure could mean the Bill diverges from EU standards, and **potentially risk the free flow of personal data between the EU and UK**. This free flow is critical to medical research and innovation and must be maintained.

[1] House of Commons, Report stage debate on the DPDI Bill, available at: https://hansard.parliament.uk/Commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill#contribution-6B2D8160-933B-4112-BEFF-007D2CEF02C4

Data protection standards – the wider context

Divergence from EU standards

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. This data flow is critical to medical research and innovation, including important clinical trials.

If the EU were to conclude that data protection legislation in the UK were inadequate – for example, MPs have raised the possibility of this in the context of the Bill's reform to the Information Commissioner's Office (ICO)[2] – 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.

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

Eroding transparency – Clause 11

The BMA urges the Government to remove Clause 11 from the Bill.

Currently[3], 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.

The Bill (clause 11) 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[4].

We are deeply concerned that this provision will water down the transparency of information to data subjects. 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. 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'[5] for patients about how and why their data is used.

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'[6]. 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.

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

[2] Stephanie Peacocke MP, Committee Stage on the DPDI Bill, see p.106 https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf
[3] Article 13 of the UK GDPR
[4] See clause 11
[5] See NHS Digital, Protecting Patient Data
[6] See clause 11

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.

Eroding regulatory independence and freedom – Clauses 32, 35 & 143–144

The BMA urges the Government to remove Clauses 32, 35 & 143-144 from the Bill.

Currently, the Information Commissioner's Office (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.

The Bill (clause 144(1)) abolishes the current ICO role and replaces it with a corporate body called the Information Commission[7], subject to greater oversight from the Government. Whilst we welcome the Government's removal[8] of the proposed power to veto ICO Codes of Practice, in recognition of concerns raised about the independence of the ICO, we are concerned that the proposed new structure still risks diluting the regulatory freedom of the ICO by exposing it to political direction or government interference.

In particular, the ICO will be compelled to consider the Government's strategic priorities when exercising its regulatory functions,[9] which could lead to the Government exerting undue influence over the ICO's independence in determining its own strategic priorities and approach to regulation. It would be entirely inappropriate for the regulation of health data to be subject to government interference. To maintain public confidence there must be clear separation between the regulation of data and those who might wish to access it.

Eroding protections by narrowing the definition of 'personal data' – Clause 1

The BMA urges the Government to address the ICO's analysis that the Bill's new definition of 'personal data' 'creates a theoretical privacy risk and is potentially confusing.'[10]

Currently, 'personal data' means any information relating to an 'identified or identifiable living individual', taking into account 'all the means reasonably likely to be used' to identify someone, either by the controller or a third party.[11] Thus, the current definition is broad in scope and applies in all circumstances. When data is 'personal data' it must be protected in accordance with the data protection legislative framework.[12]

The Bill (clause 1) amends and narrows the existing definition of 'personal data' from an objective test to a more subjective one – i.e. the new definition appears to rely on the judgments of data controllers or on what the controller knows. The result is that the range of information which constitutes personal data – and is therefore within the scope of the protections in the legislation – is reduced.

Specifically, under clause 1 information would be treated as personal data in two situations – creating two definitions, rather than the singular one that currently exists:

i) where the individual would be identifiable by the data controller or processor by 'reasonable means' at the time of processing (noting that 'reasonable means' excludes future technological developments)

[7] See clause 143(2), new section 114A

[8] Minister of state, House of Commons' final stages on the DPDI Bill, available at: https://hansard.parliament.uk/Commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill#contribution-6913B475-03F6-48F0-99C4-BDC78E4D1F7F

[9] See clause 32(2), new sections 120E and F

[10] See Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill), May 2023, available at https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf

[11] Section 3(2) Data Protection Act 2018

[12] The protections include the well-established 'data protection principles' which require data to be processed lawfully, fairly and in a transparent manner, with certain restrictions applying to special category data such as health data.

ii) where the controller or processor 'knows, or ought to reasonably know' that another person 'will obtain the information as a result of the processing' and the individual 'will be, or is likely to be, identifiable' by the person who obtains the information.

We are concerned that clause 1 risks reducing protections for data because it opens the door for controllers and processors who have been accused of breaching the law to put forward arguments in their defence based on their own circumstances of what they knew, or did not know, and what judgments they made. The ICO has also flagged[13] this issue, describing it as a 'theoretical privacy risk': should a controller judge that a third party is unlikely to obtain the data, then the data is not personal data and the protections under the legislation do not apply. Therefore, an individual who is identified by a third party that has obtained the data would 'not have recourse under data protection law for the failure to protect their data'.

Any amended definition of 'personal data' should meet the existing standards in ICO guidance and should not risk eroding protections for personal data. Furthermore, rather than provide greater clarity as the Government believes,[14] the new clause is likely to cause confusion and increase complexity because two definitions of personal data would replace the current single definition.

Separately, we would welcome reassurance that the ICO is content that the new definition of personal data does not alter the current position in relation to pseudonymisation (pseudonymisation is a technique which removes information that can identify an individual, such as name or date or birth, and replaces it with a unique code or pseudonym which does not reveal the individual's real world identity).[15] Currently, personal data which has undergone pseudonymisation remains personal data and is in scope of data protection law. The status of pseudonymised data as personal data must remain unchanged.

Eroding trust in AI – Clause 14

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

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)[16]. As such, a controller carrying out solely automated decision-making must implement certain measures to safeguard the data subject.

The Bill (clause 14) 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,[17] to amend or set aside these Article 22 safeguards.[18]

New Article 22D says:

[13] See Information Commissioner's Response to the Data Protection and Digital Information (No 2) Bill (DPDI No 2 Bill), May 2023, available at https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf
[14] Para 108, Bill Explanatory Notes, available at: https://publications.parliament.uk/pa/bills/cbill/58-04/0001/en/230001en.pdf
[15] Pseudonymisation is a technique which removes information which can identify an individual (such as name or date or birth) and replaces it with a unique code or pseudonym which does not reveal the individual's real world identity.
[16] 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."*
[17] Subject to the affirmative resolution procedure
[18] See clause 14(1), new section 22D

"*The Secretary of State may by regulations provide that, for the purposes of Article 22A(1)(a)[19], 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 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.

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.

We understand that the Secretary of State requires a degree of flexibility to amend legislation in an area of fast-paced technological change. However, 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.

Eroding the expertise and independence of organisational oversight – Clause 17

The BMA calls on the Government to amend clause 17 so that the Senior Responsible Individual role can operate independently of an organisation's senior management team.

Currently, organisations are required to appoint a Data Protection Officer (DPO) if they are a public authority, or if certain types of processing activities are carried out. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.[20]

The Bill (clause 17) removes the requirement for organisations to appoint a DPO and replaces it with a new requirement to appoint a Senior Responsible Individual (SRI) who is 'part of the organisation's senior management'[21]. If the SRI will no longer be allowed to be an external consultant, this may deprive healthcare organisations of specialist expertise that may not be available within the senior management.

It is essential that SRIs can operate independently from senior management otherwise they will be 'marking their own homework'. The creation of a requirement for SRIs to be part of the collective responsibility of a senior management team will increase the potential for conflicts of interest and create specific difficulties for doctors. For example, many doctors who currently perform the role of DPO will also perform the role of Caldicott Guardian, given the overlap of expertise which is required for both roles within healthcare organisations. Caldicott Guardians provide independent advice on complex considerations about the disclosure of confidential health data and must be free to raise concerns at senior management level and express an independent view that might not be the same as the corporate view. It is difficult to see how it will

[19] 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…"*

[20] HoC library note, page 33

[21] See clause 17(2), new Article 27A (2) and (3)(a)

be possible for an individual to hold both roles in the future should it become a requirement for the SRI to be part of the decision-making body within an organisation.

Eroding organisational data governance – Clauses 20 & 21

The BMA urges the Government to retain the current obligations in relation to conducting Data Protection Impact Assessments (DPIAs); we are concerned that clauses 20 and 21 will water down high standards of data governance, which are necessary when organisations are handling health data.

Currently, a data controller must carry out a DPIA for processing that is likely to result in a high risk to individuals. The DPIA is a systematic and comprehensive process, which helps controllers identify and mitigate the data protection risks of a project. Where a high risk which cannot be mitigated against is identified the controller must notify the ICO.

The Bill (clause 20) dilutes existing obligations in relation to conducting DPIAs – the proposed data protection assessments will require only 'a summary' of the purposes of the processing, rather than the current requirement to carry out 'a systematic description' of the envisaged processing.[22] The result is a reduction in emphasis on obligations to identify and minimise data protection risks. Removing the requirement to conduct a thorough assessment of risks posed to health data is likely to lead to a less diligent approach to data protection for individuals and increases the risk of reputational loss for organisations processing health data.

Furthermore, clause 21 removes the requirement for organisations to consult the ICO on high-risk processing[23]. Instead, it appears that informing the Information Commissioner will be optional prior to processing considered to be high risk. We view this approach as a backward step from good governance and a less rigorous approach to data protection, which is not appropriate when organisations are processing large quantities of sensitive health data.

Points for clarification

Lawfulness of processing – Clause 5 & Schedule 1

The BMA is seeking confirmation that health data held by the NHS is beyond the scope of clause 5.

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 test for applying an LIA:

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

The Bill (Annex 1, Schedule 1) 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.

Public bodies

We are unclear on the extent of the impact of clause 5 on the processing of health data. We note that the 'recognised legitimate interests' avenue appears to be available only to data controllers that are not public authorities; therefore, NHS organisations appear to be excluded. We would welcome confirmation that health data held by the NHS is beyond the scope of clause 5, now and in the future.

Non-public bodies

[22] See clause 20(3)(d)
[23] See clause 21(3)(5)(a))

We would also welcome clarity and reassurance that there is no scope for the new 'recognised legitimate interests' avenue to apply to the processing of identifiable health data held by non-public bodies, for example research organisations. It would be of significant concern should it be deemed that the principles of necessity and proportionality (components of an LIA) are automatically met when health data is being processed.

Online anonymity – Clause 109

The BMA is seeking clarification from the Government on the implications this clause will have on health data.

Currently, Regulation 6(1) of the Privacy and Electronic Communications (PEC) Regulations prohibits an organisation from storing information or gaining access to information stored in the terminal equipment of an individual (e.g. a computer), unless the individual has given consent. These rules apply to the placement of cookies and similar technologies on people's devices.

The Bill (clause 109) amends the PEC Regulations. We understand that the effect of the clause is that consent will not be required for the use of online trackers (or 'cookies') to be placed on users' devices for certain purposes, including collecting statistical information with a view to bringing about improvements to that service.[24]

The implications for special category health data require clarification. For example, if an individual has been seeking online advice about a particular health condition, we are not clear whether this clause will enable the non-consented collection and storage of personal data, such as IP address, which reveals that the individual has visited certain health-related websites. The fact that an individual has sought online advice from an NHS or other healthcare website must not be shared in identifiable form for statistical or other purposes without the individual's explicit consent. Any indication that information about online searches for health advice will automatically be collected and shared would understandably deter individuals from seeking online advice due to fears about the confidentiality.

December 2023

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

[24] See clause 83(2)(a), new paragraph 2A