

The British Medical Association's response to the Department of Culture Media and Sport's consultation 'Data: a new direction'

About the BMA

The BMA (British Medical Association) 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.

Introduction

The changes proposed in this lengthy consultation are numerous and wide ranging. Our approach has been to highlight the main issues impacting on organisations processing special category health data (which is also subject to legal and professional duties of confidentiality). Given the scale of the consultation, we recognise that additional issues not covered in this response may come to light as discussions about the proposed reforms continue. We would be pleased to engage with the DCMS on any matters which impact on confidential health data, particularly when it becomes clearer which proposals will form draft legislation.

The main themes of our response can be summarised as follows:

- the UK's adequacy agreement with the EU must not be placed in jeopardy
- the UK's current high standards for protection of health data must be maintained
- legislative change may have unintended consequences for medical researchers.

EU-UK adequacy

The government's proposed reforms must be seen in the context of the importance of the recent EU decision to recognise the UK's adequacy in data protection standards. While the government appears to be confident that the UK will maintain adequacy, we are concerned that should the UK reduce current high standards of data protection as proposed there is a risk of jeopardising the EU's adequacy decision meaning that personal data could no longer flow seamlessly from the EU to the UK. The damage and disruption to medical research and innovation which would occur in this event would be severe and would far outweigh any perceived benefits which might be achieved via the reforms.

There are important clinical trials which depend on the exchange of data between the EU and the UK which would be placed in jeopardy should adequacy status be lost. If the adequacy decision was to be withdrawn researchers would have to resort to burdensome and expensive alternative data transfer mechanics and further collaboration is likely to be discouraged. The UK would be unlikely to be able to participate in future multi-centre clinical trials, which are likely to be crucial to its pharmaceutical sector, given the pre-eminent role of the European Medicines Agency. The UK would also risk being marginalised in pan-European research into rare diseases, which can only be done from among the greater population of the EU.

Maintaining high standards of protection for health data

Patients and the public rightly expect that appropriate safeguards are in place to protect their confidential health data. In our view, in proposing a series of reductions in existing high standards of data protection, not enough emphasis has been placed on the public's expectations as to how confidential health data are handled. The consultation fails to properly consider the potential impact of the loss of public trust in how the health system safeguards data.



We are deeply concerned that the consistent theme throughout the consultation is an erosion of fundamental privacy rights and current high standards of protection for health data which risks a loss of public trust in data use. If such a loss of trust occurs it would be to the detriment of data quality both for safety and effectiveness of individual care and for research and scientific development. Building and maintaining public trust is an essential element in maximising participation in research and innovation.

Unintended consequences of legislative change

Many of the issues covered in the consultation which relate to the processing of health data do not require legislative change. In fact, legislative change may have negative consequences which we urge the government to avoid. Where doubt exists about the lawfulness of processing data under UK GDPR much of the uncertainty could be resolved through additional guidance or clarification from the ICO (or appropriate sector-specific body).

Chapter 1: Reducing barriers to responsible innovation

Research purposes

Q1.2.2 To what extent do you agree that creating a statutory definition of 'scientific research' would result in greater certainty for researchers?

Strongly disagree

We suggest that there would be challenges with creating a simple statutory definition of scientific research because it would have to be either:

- so tightly drawn as to exclude legitimate areas of research; or
- so widely drawn, in order to avoid this, that it encompasses activities by commercial organisations that would risk undermining the trust of patients in the process and weaken their vital engagement in medical research whilst not providing the certainty the government says is its objective.

Q1.2.4 To what extent do you agree that identifying a lawful ground for personal data processing for research purposes creates barriers for researchers?

Strongly disagree

We are not aware that medical researchers are currently experiencing difficulties in establishing a lawful basis to process special category health data under UK GDPR. There appears to be little evidence of appetite for legislative change amongst the medical research community. The creation of unnecessary uncertainty about the lawful grounds for processing health data must be avoided. Such a step is likely to inhibit medical researchers in data use rather than encourage them, for fear of breaching the law (and professional obligations). It would also undermine the confidence of patients and the public in medical research, which is so vital to its continued success.

The Health Research Authority (HRA), the Medical Research Council (MRC) and others provide clear guidance which sets out the relevant lawful bases as follows:

- public authorities, such as NHS organisations and universities, can use 'task in the public interest' (Article 6(1)(e));
- charitable research organisations and commercial companies can use 'legitimate interests' (Article 6(1)(f));

- organisations participating in clinical trials can use ‘compliance with a legal obligation’ (Article 6(1)(c) (because of the legal requirement to prepare patient safety reports)).

In addition, the Article 9 basis, required for processing special category health data, is:

- ‘scientific or historical research purposes’ (Article 9(j) (in accordance with the safeguards for data subjects in Article 89)).

UK GDPR therefore does not present barriers to researchers using health data for medical research purposes. Prior to the introduction of GDPR, medical researchers in the UK already operated within a set of rigorous standards for good research governance practice overseen by the Health Research Authority (HRA). Medical researchers must also comply with the common law duty of confidentiality alongside the professional and ethical standards set out by the General Medical Council.¹ Adherence to these standards means that it is generally not difficult for medical researchers to establish lawful grounds under UK GDPR.

Q1.2.8 To what extent do you agree that it would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purpose of personal data processing at the time of data collection?

o Strongly disagree

The consultation suggests changes relating to the processing of data for research with the intention of providing greater certainty for researchers. One of the proposals is to put broad consent, as defined in Recital 33, on a legislative footing as lawful basis for processing. This proposal is unlikely to achieve the intended clarity for researchers. The likely (unintended) consequences would be to create legal uncertainty for researchers and reduce protections for health data as described below.

GDPR requirements for consent

It is questionable whether broad consent will meet the UK GDPR requirements for consent to be valid i.e. consent must be informed, specific and unambiguous. It is difficult to envisage how consent can both be broad and specific. Given the existing clear and certain lawful bases within GDPR for processing data for research – and which do not cause problems for health researchers - we suggest the introduction of broad consent will lead to unnecessary legal uncertainty.

It is helpful to refer to guidance from the Medical Research Council (MRC) and Health Research Authority (HRA) about the use of consent in medical research. Both the HRA and MRC (supported by advice from the ICO) are clear that consent should not be the legal basis for processing. The [HRA states](#): For the purposes of the UK GDPR, the legal basis for processing data for health and social care research should NOT be consent.

The reason for the expectation that consent is not the appropriate legal basis for research under UK GDPR is because there are certain rights afforded to data subjects that follow from consent and which cannot be applied in the context of health research without presenting researchers with significant challenges (some of which are explored below).

Withdrawal of consent

Article 7(3) of UK GDPR sets out that consent must be capable of being withdrawn without detriment to the data subject. The [ICO’s advice about the right to withdraw consent](#) states:

¹ General Medical Council (2010), *Good practice in research*; General Medical Council (2017), *Confidentiality: good practice in handling patient information*

“If you would not be able to fully action a withdrawal of consent – for example because deleting data would undermine the research and full anonymisation is not possible – then you should not use consent as your lawful basis (or condition for processing special category data). Consent is only valid if the individual is able to withdraw it at any time.”

It will clearly be problematic if a data subject withdraws their consent for data processing during a research project. Consequences include unreliable results which could limit the validity of the research project or lead to biased outcomes.

Risk of reduced safeguards for health data

The Article 9 basis for processing special category health data - (Article 9(2)(j) ‘scientific or historical research purposes’) - requires compliance with the ‘appropriate safeguards’ set out in Article 89 (as supplemented by section 19 and Schedule 1 of the Data Protection Act 2018).

The HRA and MRC provide guidance to researchers about compliance with the safeguards which include: respect for data minimisation via the use of pseudonymisation techniques; that the processing must not cause distress to individuals; and that the processing must be ‘in the public interest,’ for example by being conducted in accordance with the [UK Policy Framework for Health and Social Care Research](#).

The Article 89 safeguards are specifically attached to the Article 9(2)(j) grounds for lawful processing. Data subjects whose data are not processed under Article 9(2)(j) - but instead rely on broad consent - would not benefit from the Article 89 safeguards. The addition of broad consent as a lawful basis for processing will therefore create a framework of inconsistent standards of protection when data are processed for research i.e. data subjects whose data are processed under Article 9(2)(j) will have additional safeguards applied to their data and those who provide broad consent will not.

Power imbalance

There is an expectation in UK GDPR that where a power imbalance between the data controller and the data subject exists, for example where the controller is a public authority (such as an NHS body) and the data subject is dependent on their services, then consent is inappropriate. While new legislation could potentially address this problem from a legal perspective, legislative change would not be necessary should researchers continue to use the existing, and more appropriate, lawful bases as described above.

Interpretation of Recital 33

As it is expressed in Recital 33, our understanding is that ‘broad’ consent is broad only insofar as it might capture different research projects within a particular area of scientific research. This is re-affirmed by the ICO’s advice which states that: [“If you are seeking consent to process personal data for scientific research, this means you don’t need to be as specific as for other purposes. However, you should identify the general areas of research...”](#)

The government’s interpretation of Recital 33 is not clearly described. A wider interpretation to that of the ICO’s (as above) would be highly problematic and damaging should it allow the data controllers to share personal health data with a variety of third parties for wide ranging purposes which will not be made known to the data subject. Under this interpretation of broad consent, the consent cannot be described as ‘informed’ and ‘unambiguous’ and would more likely be invalid under the current definition of consent in UK GDPR.

Such an approach creates critical problems with maintaining public trust in research through a lack of transparency and clarity about what individuals are being asked to consent to. The detrimental

effects loss of trust would cause to the continuation and advancement of important medical research, which relies on public confidence and participation, must be avoided.

Q1.2.10. To what extent do you agree with the proposals to disapply the current requirement for controllers who collected personal data directly from the data subject to provide further information to the data subject prior to any further processing, but only where that further processing is for a research purpose and where it would require a disproportionate effort to do so?

o Strongly disagree

We support an approach of co-production between researchers, academics, patients and the public. Co-production goes beyond the provision of information, it means that patients and the public are not simply participants in medical research but co-producers of it i.e. participation in the identification of research questions, formulation of the questions, data collection and promulgation of results. We believe this mitigates data misuse or spurious use.

This is particularly important because we are in an era where the public has greater awareness about data use (and misuse); in particular with recent prominence in the media of, for example, the arrival of GDPR, the Cambridge/Analytica/facebook scandal – and crucially, in terms of health data, the paused introduction of the GP Data for Planning and Research (GPDfPR) programme.

In our view, this question presents a false choice between disproportionate efforts to provide privacy information to data subjects and the disapplication of the requirement to provide information in its entirety. The transparency obligations enshrined in Articles 12 – 14 do not require contact to be made with each individual data subject – an approach that, in many cases, would indeed be considered disproportionate for medical researchers. Transparency obligations can, however, be satisfied by providing privacy information in more general terms and using different techniques such as use of relevant websites, social media, local newspapers, or notices displayed in relevant settings etc. The [ICO's guidance](#) recognises the distinction between contacting individuals and a more general approach to the provision of information:

“If you determine that providing privacy information to individuals is impossible, you must publish the privacy information (eg on your website), and you should carry out a DPIA.”

Medical researchers can – and do - make reasonable efforts to bring any new uses of personal data to the attention of the relevant population by providing updates on the study website and/or the website of relevant charities (which are often partners in health research projects). While these efforts will not reach every data subject, they will reach some (or most) and the fact that efforts are being made to inform is an acknowledgement of the importance of maintaining public confidence in medical research which is critical to its success.

The overall effect is that more – not less – transparency and information provision about data use is expected and required to build and maintain public trust. It is significant that one of the criteria for the progression of the GP Data for Planning and Research (GPDfPR) data collection is a national communications campaign to increase public awareness of the programme. It therefore seems contradictory (and contrary to societal expectations) for the government to recognise the necessity of communication with patients to ensure a ‘social licence’ for GPDfPR while at the same time providing an exemption to transparency for other projects.

Any reduction in transparency requirements is a backward step in terms of promoting confidence in the use of health data. We would go further and strongly advocate for increased direct patient

involvement and engagement in decisions about use of/access to health data. Support from relevant patient groups can significantly strengthen the public interest argument in permitting unconsented data access.

Further processing

Q1.3.3 To what extent do you agree that the government should seek to clarify when further processing can be undertaken by a controller different from the original controller?

o Somewhat agree

Article 5(1)(b) and Recital 50 indicate that further processing for scientific and historical research purposes should be considered as compatible processing.

The issue which can cause uncertainty when processing data for research is when the data is transferred to a new data controller. Our understanding is that when there is a new data controller the Recital 50 presumption that research is a compatible purpose does not apply. In these circumstances the new data controller must identify a new Article 6(1) basis for processing. In other words, the presumption of compatibility applies only when there is no change in data controller.

It is our view, that clarification on this point could be achieved via guidance from the ICO without the need for legislative change.

Q1.3.4 To what extent do you agree that the government should seek to clarify when further processing may occur when the original lawful ground was consent?

o Neither agree nor disagree

Our understanding is that when consent is the original lawful basis for processing no further processing can occur unless new consent is sought – to do otherwise would undermine fairness and transparency. This point is made in the [ICO's guidance](#) but could benefit from greater prominence where it is causing uncertainty. We are not aware it is causing a problem for medical researchers who rely on alternatives to consent as their GDPR lawful basis for the reasons set out earlier in our response.

Legitimate interests

Q1.4.1. To what extent do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test?

o Strongly disagree

An essential part of the concept of legitimate interests is the balance between the interests of the data controller and the rights of the individual. A legitimate interests assessment (LIA) therefore helps to ensure that the need to collect and use data is balanced against any risks to individuals. As [stated by the ICO](#), the more sensitive or 'private' the data, for example health data, the more likely the processing is to be considered intrusive or to create significant risks to the individual's rights.

There is a lack of detail about the exact circumstances when the legitimate interests balancing test might automatically be treated as falling in favour of processing, particularly where health data is concerned. In any event, a disapplication from conducting an LIA when an organisation wishes to process special category health data reduces organisational accountability and transparency. We do

not support removal of a safeguard which helps to protect the interests of those involved in research and represents good practice in data protection.

An exemption from an LIA may also create practical difficulties for data controllers when demonstrating transparency and accountability. Any controller wishing to rely on legitimate interests must inform individuals that it is processing personal data on this basis and what the legitimate interests are. In providing this information to individuals via privacy notices, data controllers should explain that the decision to rely on legitimate interests was taken ensuring the privacy rights of individuals were considered and not severely impacted. If an LIA has not been conducted it may be more challenging for data controllers to explain and justify to individuals how proper consideration has been given to their rights and interests.

AI and Machine Learning

The consultation sets up a tension between the interests of innovation in AI, and the privacy rights and interests of data subjects – both those subjects whose data are processed for ‘background’ purposes (such as identifying bias) and those on whose behalf AI will be making decisions – people, that is, who have significant personal interests in the outcome of the decision-making process. Having set up this tension, the consultation relentlessly puts innovation above the rights and interests of data subjects, including the proposal to delete Article 22 which encompasses data subjects’ ‘right to human review’ of automated decision making.

The overriding narrative is that privacy rights are direct impediments to innovation and must therefore be sacrificed. We recognise that AI and machine learning will play an ever-increasing part in our lives, and will be an important driver of economic growth. Nonetheless we remain concerned that the consultation document seeks aggressively to override fundamental rights and interests in pursuit of innovation and growth. It is entirely plausible to suggest that the tension between innovation and privacy is misconstrued – that without appropriate respect for the privacy rights of data subjects, there will be a widespread lack of trust in AI and significant consumer and citizen pushback. Agile regulation should be able to both permit innovation and reassure individuals that their strong interests in privacy will not be sacrificed on the altar of economic growth. The removal of an entire Article (22) is also a clear risk to EU – UK adequacy.

Tackling bias and discrimination

We agree about the need to tackle bias in the design stage of AI systems (paragraphs 92 & 93) – it is often too late to fix once the software/systems have been designed. We would also suggest a form of mandatory diverse user testing at design-stage to ensure that systems are accessible and non-biased.

Right to Access Gender Recognition Certificates

In our [submission to the Gender Recognition Act reform](#) consultation we stated that obtaining a Gender Recognition Certificate should not be a medicalised process. At the moment it is. Therefore, doctors are often holding sensitive gender data information about people. How this would be managed in any future changes to the Gender Recognition Act and GDPR must be considered - along with guidance about how/where gender and gender fluid identities should be held securely in different medical settings.

Data Minimisation and Anonymisation

Q1.6.1. To what extent do you agree with the proposal to clarify the test for when data is anonymous by giving effect to the test in legislation?

- Strongly disagree

We do not agree that it would be helpful for legislation to clarify the test for anonymisation for two reasons. Firstly, in view of the extent and pace of technological change in the way data is processed, anonymisation is an evolving area which means the risks of reidentification and ability to link datasets are likely to increase over time. It would therefore seem unwise to create a statutory test which may become obsolete in the face of a continually changing technology.

Secondly, in our view, it would be more helpful to clarify the standards for rendering health data anonymous. It has long been the case that healthcare organisations are in an uncertain position about how to meet standards for anonymisation to ensure that, as far as reasonably practicable, information which has been rendered anonymous cannot re-identify individuals.

There is a need for detailed guidance which goes beyond the matter of the test for anonymisation and provides a set of standard tools which organisations can use to ensure good practice when rendering data anonymous. Legislation can only go so far in the detail it can provide – particularly cross-sector legislation such as UK GDPR. The ICO is best placed to provide this guidance. (The ICO’s anonymisation guidance is currently being updated which we welcome).

Once the ICO’s guidance on anonymisation is in place, there is a need for specific guidance to help healthcare organisations determine how the ICO’s standards on anonymisation and pseudonymisation of personal data relate to confidential patient information. It would therefore be appropriate for the health service to develop its own guidance using the ICO’s framework as the starting basis.

It would be helpful if guidance could include:

- clarity for organisations to help determine when the data they are processing is pseudonymous and when it is anonymous;
- how far the regulator would accept risks of re-identification;
- how the ‘reasonable likelihood’ of identification should be interpreted at a particular moment in time in a backdrop of technological change.

It is certainly a helpful step that the ICO intends to include a chapter titled ‘*How do we ensure anonymisation is effective?*’ within its updated anonymisation guidance.

Chapter 2: Reducing burdens on business and delivering better outcomes for people

Reform of the accountability framework

Q2.2.1 To what extent do you agree with the following statement: The accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, iii) be more risk-based?

o Strongly disagree

We support strong accountability safeguards to ensure individuals are not exposed to increased risks or adverse impacts of data processing. The consultation sets out proposals to remove and amend various requirements relating to accountability. As the consultation acknowledges, the accountability principle is recognised ‘as a key building block of effective data protection regulation...’ The proposed removal and dilution of accountability requirements therefore appears highly likely to result in lower standards of accountability required by organisations and protections for patients’ health data in the UK. We do not support this approach and refer to previous comments about risks of undermining public trust in organisations which process health data and the loss of EU – UK adequacy.

Q.2.2.8. To what extent do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments?

○ Strongly disagree

The government is proposing to remove the need for specific data protection impact assessments (DPIAs) which will be replaced by privacy management programmes. DPIAs are a core element of data controllers' demonstration of accountability. While the full implications of the loss of DPIAs in favour of privacy management programmes are unclear, we note the increased discretion for organisations on how to achieve compliance within the new accountability framework. We urge the government to ensure that this does not result in a reduction in emphasis on obligations to identify and minimise the data protection risks before organisations change data sharing systems or undertake a new data sharing project.

If properly conducted, DPIAs enable an organisation to:

- consider and mitigate privacy risks at the planning stage of a project rather than enacting changes further down the line which is likely to be more time consuming and resource-intensive
- more easily audit (or make available for audit) their data processing activities therefore increasing accountability
- develop a defined process for considering privacy risks rather than ad hoc assessments which can be inconsistent and more time consuming
- reduce the overall risk of a data breach with the associated financial and reputational losses
- provide evidence that risks to data were considered should there be a complaint and ICO investigation.

We suggest consideration of the added value a DPIA brings to an organisation and to ensure these benefits are not cast aside under the proposed new framework.

Q.2.2.11. To what extent do you agree with the proposal to reduce the burden on organisations by removing the record keeping requirements under Article 30?

○ Strongly disagree

Undertaking the data-mapping exercise required under Article 30 is an important part of data protection. Holding comprehensive records can also help organisations to adapt to changing legal and technological requirements, as well as societal expectations. The consultation acknowledges that: 'There are risks that removing the requirements under Article 30 could hinder effective enforcement and offer less regulatory protection to data subjects.' These are serious risks and we do not agree that they can be dismissed as 'minimal'. More information and assurance are needed to explain how these risks will be mitigated through use of the proposed personal data inventories.

Subject Access Requests

Medical records are necessarily complex and often contain hundreds of pages. Our 2018 survey of GP practices revealed that the average SAR takes 74 minutes to respond to. This resource cost is well below the £450 and £600 limits under the Freedom of Information Act but given the numbers involved can cause an unacceptable strain for GP practices which are almost universally small to medium turnover businesses. Our survey revealed that all surgeries felt significant patient care resource was being diverted to servicing SARs.

Increasingly patient records are held in electronic form only and there is a programme in England to digitise all NHS GP records including the historic paper records that had been scheduled to be completed by 2020 but has been delayed by the pandemic. Additionally, since 2019 patients have had online access to their records through NHS approved systems and from December 2021 it is planned that this access will expand. These systems are configured and specified by NHS Digital with input from the profession's representative body the Joint General Practitioners IT Committee.

The BMA believes that a digital approach to SARs would remove the burden currently carried by practices. In our view, this can be achieved via providing access to electronic medical records through an NHS approved app or online access. Where patients authorise a third party to make the SAR on their behalf, temporary access rights could be provided, though more system development work will need to be done to determine what form this takes. These access mechanisms would be free to patients.

A digital approach would not preclude SARs being made directly to the practice for those patients (or their authorised representatives) who:

- do not have internet access or a digital device; and/or
- wish to receive a paper or electronic copy from the practice.

In these cases, we believe a proportionate charge should be levied to enable the practice to recover its reasonable costs whilst a proportion of records remain in paper form only.

Q2.3.1. Please share your views on the extent to which organisations find subject access requests time-consuming or costly to process. Please provide supporting evidence where possible, including:

o *What characteristics of the subject access requests might generate or elevate costs*

The issues for general practices are the copying of the historic paper records and the volume of paper produced when the electronic records are printed out. These issues present staff and resource costs. This is also a considerable burden in ecological terms.

o *Whether vexatious subject access requests and/or repeat subject access requests from the same requester play a role*

Vexatious and repeat SARs from different agencies on behalf the same subject is an issue where a dispute results from a practice advising multiple agencies that a fee will be charged for multiple SARs as per paragraph 3 of article 15 of GDPR. We know that this is an issue for some practices.

o *Whether it is clear what kind of information does and does not fall within scope when responding to a subject access request*

This is relatively clear to NHS practices.

Q2.3.3. To what extent do you agree that introducing a cost limit and amending the threshold for response, akin to the Freedom of Information regime (detailed in the section on subject access requests), would help to alleviate potential costs (time and resource) in responding to these requests?

- o Strongly agree

Please see the above introductory section. The BMA believes patients should have digital access to their medical record via NHS approved apps (or other online access method). This should be at no cost and will be minimal burden to the practice when complying with SAR responsibilities.

SARs made directly to the practice outside of the digital process should attract a fee according to the volume of data being provided and the staff time and resource being utilised. The sliding scale should aim to represent a “costs recovery”.

Please explain your answer, and provide supporting evidence where possible, including on

o What a reasonable cost limit would look like, and whether a different (ie. sliding scale) threshold depending on the size (based on number of employees and/or turnover, for example) would be advantageous

We would suggest for SARs produced by the practice the minimum fee should be £50.

Q2.3.4. To what extent do you agree with the following statement: ‘There is a case for re-introducing a small nominal fee for processing subject access requests (akin to the approach in the Data Protection Act 1998)’?

- Strongly agree

Please explain your answer, and provide supporting evidence where possible, including what a reasonable level of the fee would be, and which safeguards should apply.

See above

Q2.3.5. Are there any alternative options you would consider to reduce the costs and time taken to respond to subject access requests?

- Yes

Please explain your answer, and provide supporting evidence where possible.

As described above, establish a digital first process for SARs when access to medical records is sought. We would be happy to participate in discussions as to how this could be achieved.

Chapter 4: Delivering better public services

Use of personal data in the Covid-19 pandemic

Q4.3.1 To what extent do you agree with the following statement: Private companies, organisations and individuals who have been asked to process personal data on behalf of a public body should be permitted to rely on that body’s lawful ground for processing the data under Article 6(1)(e) of the UK GDPR?

- Strongly disagree

We do not agree with the premise that private companies do not have to reflect on whether processing data instructed by a public body is lawful for them to undertake, and do not have to reflect on whether it is lawful for them to disclose personal data to a public body when asked. The approach in the consultation appears to be that all private companies can ‘piggy-back’ on the public

bodies' assessment of the lawfulness of the processing. In our view, this is likely to lead to a less diligent private sector and an overall reduction in safeguards for health data.

Q4.3.3. To what extent do you agree with the proposal to clarify that public and private bodies may lawfully process health data when necessary for reasons of substantial public interest in relation to public health or other emergencies?

o Strongly disagree

Our understanding from the consultation document is that the proposal appears to be the removal of a safeguard under the Data Protection Act 2018 (DPA) by allow the processing of health data for public health purposes to occur without the oversight of a healthcare professional subject to a duty of confidentiality. Rather than removing safeguards for patient data we suggest addressing practical questions about how health data sharing and processing in a pandemic can be done efficiently within the current safeguards.

It is difficult to comment further as the consultation does not provide detail about the circumstances which have posed problems. Given that the purpose of the processing is public health there must be extremely limited circumstances which would not ordinarily engage a public health clinician at some stage of the processing. This raises the important question of why it would ever be appropriate to process personal health data for public health reasons without the oversight of a public health clinician or another appropriate medical professional.

Q4.4.7 To what extent do you agree that there may be a need to add to, or amend, the list of specific situations in Schedule 1 to the Data Protection Act 2018 that are deemed always to be in the substantial public interest?

o Strongly disagree

One of the proposals appears to be adding a pandemic to Schedule 1 of the DPA 18 so that health data can be processed in the substantial public interest without the need to rely on the public health condition for processing within Schedule 1. (Schedule 1 Part 1 (3)(a) permits special category data to be processed if it 'is necessary for reasons of public interest in the area of public health').

This approach is problematic for two reasons. Firstly, if there is no oversight from a public health clinician then it will be difficult, if not impossible, to justify the processing as being 'necessary'. Secondly, it is hard to envisage the circumstances when processing health data in a pandemic would not be captured by the existing 'public health' provision in Schedule 1. Rather than a legislative change which may diminish protections for health data, we suggest a better approach is for guidance to set out which of existing lawful bases can be used and for what purposes, including for a pandemic.