NDG National Data Guardian
for health and social care

The National Data Guardian's response to the government data reforms consultation 'Data: A New Direction'

Submitted 19th November 2021

Introduction

This is the National Data Guardian's (NDG's) formal response to the Department for Digital, Culture, Media and Sport's consultation "Data: a new direction" on the proposed reforms to data protection law in the UK.

This is not an exhaustive review of all the government proposals, but rather the NDG's considerations and recommendations on those areas of the reforms that may impact the health and care sector.

The appropriate use of data is essential to ensure continuous improvements in health and social care. The NDG is supportive of the government's aim of building an improved data protection regime. As such, this response is intended to provide advice and feedback on areas of the consultation where the NDG believes further consideration might be necessary if the government is to achieve its stated aim.

1. Research

What the consultation says

Chapter 1.2 of the consultation outlines several proposals for amendments to research provisions within the existing data protection framework. The government cites a need for legal certainty and a reduction in complexity as two of the reasons why change is necessary. The consultation states that "the structure of the current legislation makes it difficult to realise the full benefits of this system" (**paragraph 37**) and creates "both real and perceived barriers" (**paragraph 39**) for organisations that process personal data for research.

The NDG's considerations

Ensuring compatibility with international data protection regimes

The government acknowledges the importance of international collaboration for scientific research. This includes research for public health and is the focus of this response. To realise the full benefits of health research for patients and the public, it is vital that international collaboration can continue under a reformed data protection regime. As such, compatibility with other data protection regimes is vital in ensuring continuity in this area.

Consolidating research provisions from UK GDPR and DPA 2018

The government proposes to consolidate the research provisions that are currently set out across the UK GDPR and the Data Protection Act (DPA) 2018 (**paragraph 40**) to make them easier to navigate. This may provide some clarity

for researchers. However, in preparing this response, the NDG took part in a research-focussed roundtable hosted by the Wellcome Trust to consider the reforms. The NDG supports the consensus from that roundtable that the health research sector understands and uses the existing legislative provisions effectively. Comprehensive guidance regarding the implementation of data protection legislation has been developed by the Health Research Authority (HRA) and the Medical Research Council (MRC) and is well used by the sector. Given this, the government should consider whether amending legislation that is well understood by those who engage with it, and are able to produce effective guidance from it, will have the effect of increasing rather than reducing complexity.

Providing a statutory definition for 'scientific research'

The consultation proposes to incorporate a definition of 'scientific research' into the main body of the legislation (**paragraph 42**). Scientific research is currently described in Recital 159 of the UK GDPR, where it specifically states that the term requires broad interpretation. The government suggests that using this wording as the basis for a statutory definition would reduce "uncertainty around what constitutes research…reduce the perceived level of risk to organisations, and…improve transparency for individuals". Defining scientific research may be helpful for many. However, it is important that such a definition does not exclude important research by enforcing too narrow a definition, and is also not so broad as to make it impossible to manage people's expectations regarding how their data is used. Research necessarily takes place within a broader governance structure comprising of methodological and ethical sector-related standards. These standards seek to ensure that people understand and trust how their data may be used within a research setting. If a statutory definition is proposed, it must not weaken these governance structures.

Creating a separate lawful ground for research

The consultation proposes (**paragraph 44**) a new separate lawful ground for research. The NDG supports the Wellcome Trust research roundtable consensus that there is no obvious need to introduce or amend legislation to clarify a lawful basis for research, as this is something that is generally well understood. The HRA and MRC guidance cited above also provides further support to the research community regarding compliance with legal bases for research. Researchers felt that if further measures to increase clarity were needed in the research context, this would be better served through ICO and sector specific guidance than legislative changes.

The consultation does not provide evidence to support its claim that the existing lawful bases within the current data protection framework create barriers to research. Further, it states that barriers may be "real" or "perceived". To remedy

this, engaging with, and providing guidance to, sectors that incorrectly perceive barriers may be a more sensible option than enacting legislative change.

Existing bases for processing personal data for research purposes provide important safeguards for individuals. These safeguards are crucial to earn and maintain public trust in health research; therefore, they should not be seen as producing a disproportionate burden to the research community. It is important that any changes to the existing research data protection framework preserve these safeguards.

Consent for research

The government proposes to place onto a legislative footing provisions that will enable data subjects to give consent for their data to be used in broader areas of scientific research (currently in recital 33 GDPR) when it is not possible to fully identify the purpose of personal data processing at the time of data collection (**paragraph 48**). Placing recital 33 onto a legislative footing may have the effect of decreasing rather than increasing certainty in the context of scientific research, because consent is not usually relied on as the legal basis for processing personal data for health research purposes. This may cause some confusion about the relationship with existing lawful bases that are relied upon for research, and the additional safeguards they afford. The Wellcome Trust research roundtable considered that this proposal is unlikely to present clear benefits, and that the consultation fails to recognise that scientific research takes place within a broader established framework of governance and ethics.

Further uses of data for research

The government proposes stating explicitly that further use of data for research purposes is always compatible with the original purpose for processing (**paragraph 48**). The scope of this proposal, that research shall not be considered incompatible with the original purpose for processing under Article 6(1), has not been sufficiently explained in the consultation. In particular it is not clear how this proposal would interact with Article 6(4) which stipulates what must be considered when determining whether processing personal data for a new purpose is compatible. While there may be existing confusion about whether the compatibility principle applies to research undertaken by a different controller to the original controller, ICO guidance is a key mechanism for creating clarity around specific UK GDPR provisions. Indeed, the ICO is already planning dedicated research guidance, and this guidance could provide clarification to the research community on the interpretation of these Articles and Recital 50. Where data is repurposed for research, it is important that existing protections for personal data reused for research are not diminished; this could have a detrimental impact on the public's trust in those organisations that might make data available for research purposes.

Replicating GDPR Article 14(5)(b) exemption in Article 13

The government is considering replicating the GDPR Article 14(5)(b) exemption in Article 13 (**paragraph 50**). This exemption has the effect of relaxing the provisions regarding the provision of transparency information to a data subject where it would be impossible to, or would require disproportionate effort to, supply this information. The government should first consider whether disapplying transparency requirements in Article 13 UK GDPR is compatible with the transparency principle (Article 5(1)(a)). The government should also be mindful of the correlation between trust and transparency. At a time where a lack of transparency has caused important projects that use health data for public benefits to fail or stall due to lack of public trust, this is especially important.

If this exemption were to be replicated in Article 13, there should be clear safeguards to prevent misuse of such a provision. There should be a high bar on what is considered disproportionate effort where personal data has been collected from the data subject. This is because collecting personal data from a data subject will usually provide opportunities to communicate transparency information to them. This is likely to be different to situations where data has not been collected from the data subject. Guidance addressing the concept of proportionality, and the need to remain true to the threat that the information provision requirements would render impossible or seriously impair the objectives of the processing, should be strongly reinforced.

Recommended actions

- Provide evidence to back up statements which claim that elements of the existing regime are creating barriers to responsible innovation
- Any definition of research needs to be carefully considered in an international context to ensure it does not negatively impact collaboration, and should take into account methodological and ethical sector-related standards
- Consider whether the stated aims of legislative proposals could be better achieved through engagement with stakeholders and the provision of guidance from relevant regulatory authorities and sector specific bodies
- Provide evidence as to how diluting transparency requirements will benefit organisations and the public, especially given that attempts are being made in health and social care to bring people closer to their data
- If exceptions to transparency obligations are implemented, a high threshold must be required for what is deemed to be ‘disproportionate effort’
- Legislative changes in this area must be considered in the broader context of UK adequacy, and what a loss of adequacy may mean for the health research community in the UK

2. Legitimate interests

What the consultation says

With the intention of providing organisations with more confidence and certainty in their use of personal data, the government proposes to introduce an exhaustive list of uses that can be considered 'legitimate interests', and for which a 'balancing test' will not be needed prior to carrying out processing (**paragraph 60**). The consultation provides examples of processing that could be covered by this list as follows:

- Reporting of criminal acts or safeguarding concerns to appropriate authorities
- Delivering statutory public communications and public health and safety messages by non-public bodies
- Monitoring, detecting or correcting bias in relation to developing AI systems
- Using audience measurement cookies or similar technologies to improve web pages that are frequently visited by service users
- Improving or reviewing an organisation's system or network security
- Improving the safety of a product or service that the organisation provides or delivers
- De-identifying personal data through pseudonymisation or anonymisation to improve data security
- Using personal data for internal research and development purposes, or business innovation purposes aimed at improving services for customers
- Managing or maintaining a database to ensure that records of individuals are accurate and up to date, and to avoid unnecessary duplication

The NDG's considerations

Legitimate interests is one in a series of lawful bases available that can be relied upon for the general processing of personal data. The NDG is supportive of initiatives that can make safe and appropriate information use easier for organisations – provided the rights of individuals are not diminished. However, the consultation does not make clear whether, and if so how, existing data subject rights (such as the right to object) will be preserved under this proposal.

At **paragraph 56** the consultation states that when "relying on legitimate interests…UK GDPR requires organisations…to document how their interests outweigh the rights of data subjects". This is an oversimplification of the lawful basis and is problematic as it overlooks the requirements, which demand a clearly articulated interest, and a justification for the data to be processed, before legitimate interests can be relied upon as a lawful basis. ICO guidance states that legitimate interest assessments consist of a three-part test, which

considers: purpose, necessity and balancing of interests. The government consultation proposal does not indicate how *all* of these elements of the legitimate interests assessment will be met. The NDG believes that it is important for the principles of necessity and proportionality to be considered as part of a legitimate interest assessment. The government should *not* deem that in particular circumstances such as those listed in the consultation, the principles of proportionality and necessity are automatically met.

There are consequences of processing personal data on the basis of legitimate interests. Of particular significance is the requirement to consider an individual's right to object to data processing on the grounds of their specific situation. Article 6(1)(f) makes it clear that it is the "fundamental rights of the data subject" that must be considered when balancing opposing interests. Recital 47 explains this further, stating that the balance must consider "the reasonable expectations of the data subject based on their relationship with the controller". The government should provide further information on how individual rights would be safeguarded, and how generic processing activities will be considered in the context of individual objections.

There is also a danger that a pre-defined set of legitimate interests removes an important requirement for a balanced consideration and achieves the opposite of enabling a flexible approach that the government hope to achieve. As they stand, the proposals in this section appear to undermine the need for a reasoned assessment, reduce accountability for organisations and could remove important rights for individuals.

Recommended actions

- The government should explain their case for amending legislation with respect to the lawful basis of legitimate interests. It is not clear that the existing regime needs such a substantial change
- A lack of understanding within certain sectors or organisations about a legislative provision, or its implementation, does not equate to that provision being prohibitive. The government should consider whether improved guidance would be more beneficial than legislative change
- The government should elaborate on how individual rights will be protected if this proposal is implemented
- A generic list of legitimate interests would represent a clear departure from EU standards, and this should be considered in the context of the status of the UK's adequacy decision

3. Artificial intelligence

What the consultation says

The government recognises that the UK data protection regime is technology neutral and wishes for it to remain so. However, the government also states that governance of AI is a "live debate" and wants to ensure that the legal framework does not hinder technological developments in this area while remaining fair.

The NDG's considerations

Testing of AI technology

The government asks us to consider to what extent we agree that organisations should be allowed to use personal data more freely to enable responsible AI testing (**Q1.5.5**.). However, as the consultation suggests, "Many AI systems...do not use personal data at all" (**paragraph 67**).

As such, the government should consider whether a change in the law to allow for testing of AI technology is actually necessary. The NDG is supportive of the use and sharing of anonymous data to improve health and care, and while there are practical challenges in ensuring anonymity within datasets, technology in this area also continues to develop. In addition to this, the existing data protection framework already covers the use of personal data in the development of projects which use machine learning and artificial intelligence. Thus, the government should demonstrate why changes to the existing protections for data subjects are even needed for the purpose of developing and testing AI and machine learning systems.

The consultation discusses fairness in some detail in relation to bias monitoring within AI systems. The principle of fairness is often associated with transparency. However, acting fairly also requires that uses of people's personal data is in line with their reasonable expectations. Supporting organisations in this area may best be achieved by the development of harmonised regulatory guidance rather than legislative measures, as is suggested in the Information Commissioner's Office in their response to this consultation.

Article 22 of the UK GDPR provides that individuals must not be subject to solely automated decisions which produce legal effects or similarly significant effects. The government asks, "to what extent do you agree...that Article 22 of UK GDPR should be removed and solely automated decision making permitted" (**Q1.5.17.**) and suggests that the need for human review may become unworkable in the context of increasing use of automated decision-making technologies.

The NDG has significant concerns about proposed reductions to existing protections and the ability of professionals, patients, and the public to be actively informed about decisions that can have significant impacts for them. Further, it may negatively impact people's trust in decisions made about them by solely automated means if the safeguards in Article 22 are not retained. In the health and care context, any removal of the ability to contest or ask for human intervention in relation to a decision could significantly affect the quality of care. As elements of healthcare become more efficiently managed through AI, the importance of the human nature of the relationship through which care is provided must not be lost.

Recommended actions

- The government should more clearly outline the plans for replacement of the rights and safeguards for individuals who might be subject to fully automated decisions which have significant effects. We would want to understand the plans for alternative protective provisions were it removed
- If the plan is to remove safeguards regarding fully automated decision making, the government may wish to consider the risk versus reward ratio if this removal threatened the UK's adequacy status with the EU
- Consider whether changes in legislation to allow data to be used more freely are necessary, and whether a significant reduction in organisational accountability for algorithms that are developed and deployed in relation to personal data processing, would also significantly reduce the rights of individuals in an unacceptable manner

4. Data subject's rights

What the consultation says

The government states that an individual's right of access "is one of the fundamental rights in data protection legislation" (**paragraph 185**) and vows to protect it. The government, however, suggests that some organisations have found complying with existing requirements problematic. In particular, the government identifies the time and resource required to process subject access requests (SARs), and the high threshold for what is manifestly unfounded or excessive, as the core issues to address.

The NDG's considerations

The NDG has previously stressed the importance of people's awareness, understanding and involvement in how health data is used and has called for the draft health and social care data strategy (Data Saves Lives) to be clearer on how it intends to fulfil its commitment of "bringing people closer to their data".

Introduction of fees

The NDG also recognises that across health and care, the resource cost for processing subject access requests can, on occasion, be considerable. This may, for example, include the cost of clinicians' time spent reviewing extensive records to redact any sensitive third-party information, and administration time and environmental costs where printing large volumes of records occurs. The government's proposal to introduce a fee regime for providing information (**paragraph 188**) should, however, be approached with caution. As a mechanism for addressing those concerns, it has the potential to be ineffective, unfair and discriminatory.

While the consultation states fees would be structured so as not to undermine the right of access, the government should consider that any fee is inherently prohibitive, especially for those with limited financial means. The government should also consider the effect that putting up barriers to access may have on people's other data protection rights. For example, an individual's right to have their data rectified is only possible if an individual knows what information is held about them. It is also unclear from the consultation how this will be achieved within the existing language of Article 12(5) without impacting other rights and obligations that require information to be provided free of charge.

This proposal could be seen to be in opposition to the aim within the health and care sector to bring people closer to their data. To reflect the Health and Social Care Data Strategy aim, and the NDG priority of encouraging the health and care system to provide routine online access for patients to view their care records, any proposal to charge fees for subject access requests should be accompanied by obligations for organisations to provide, or improve routine access to the personal data they process (such as enabling people to access their medical records online), negating the need for individuals to formally request their information.

Manifestly unfounded or excessive requests

Reconsidering the threshold for what constitutes a manifestly unfounded or excessive request may be helpful to many organisations. It is important to strike a balance between individual rights and organisational obligations. However, as with the introduction of fees, careful consideration needs to be given to the design of such measures to ensure they only limit rights in exceptional circumstances that represent an unjustifiable burden on organisations.

Introduction of a duty to provide advice and assistance

The government has also asked for views on incorporating a duty on organisations to offer advice and assistance to those making SARs similar to the

duty to offer support contained within the Freedom of Information Act 2000 (such as helping an applicant to modify their request to make it viable). While the practicalities of implementing and enforcing such a duty require significantly more explanation, this could be a valuable means of reinforcing openness and transparency, and encouraging constructive dialogue between individuals and the organisations that process their data.

The government should consider if the development of guidance and standardised documentation could support this duty, encouraging individuals to refine their requests if possible, and giving organisations the confidence to suggest that they do so where it would result in a speedier resolution suitable for all parties. In this way, any issues of resource and time could be tackled, and could have the effect of enhancing the right of access by providing only information that is relevant and useful to the individual for their own purposes, whilst avoiding processing excessive information that they have indicated that they do not require.

Recommended actions

- Consider further whether fees are the most appropriate way to address resource-related issues associated with fulfilling subject access requests.
- When considering disproportionate effort, due consideration must be given to the grounds on which this will apply to ensure this fundamental right is not diluted
- Government should explore further the practicalities of implementing a new duty to provide advice and assistance to those exercising their right to be informed

5. Data minimisation and anonymisation

What the consultation says

The government believes that more could be done to help organisations navigate data minimisation techniques, such as pseudonymisation. They also state that clarity on the test for effective anonymisation of personal data is essential if organisations are to realise the full potential of the data they hold.

The NDG's considerations

The NDG agrees that accurately determining whether data is personal data (including pseudonymous data) or anonymous data is important, as the former is subject to the UK data protection regime and the latter is not. This determination is very rarely straightforward.

The government proposes to try and resolve this by placing a legislative test into the main text of the UK GDPR (**paragraph 121**). The NDG agrees that clarity in this area is crucial in determining the lawful use of personal data. However, the government must consider the implications of enshrining a rigid test into law in what is such a fast-moving environment. The test must be flexible in order to meet the key aims of these reforms, and must not limit the protections for individuals by setting the bar for anonymisation too low.

The test of anonymisation is broadly understood as a legal standard rather than a set of technical requirements. In practice, this means that anonymisation cannot be achieved by simply removing a specific set of identifiers from a dataset. Instead, the test must be applied on the basis of what information may reasonably be accessed or used to reidentify an individual from those data in each case. As recital 26 of UK GDPR sets out, organisations must take account of all objective factors such as the time, cost, and available technology to determine whether data has been effectively anonymised.

The NDG has previously called for clear standards on rendering data anonymous in health and social care to ensure data is handled in line with the UK's data protection regime. The ICO has recently published two (of several planned) chapters of guidance on anonymisation, pseudonymisation and privacy enhancing technologies for consultation, and the NDG is continuing to work with the ICO and other key stakeholders to further develop this guidance. The forthcoming ICO guidance should provide sector wide clarity which is relevant to the health and social care system.

Recommended actions

- Consider whether guidance from the Information Commissioner's Office would help the government achieve the stated aim of providing clarity
- Any legislative test should ensure that a high level of protection for individuals is maintained
- Consider the suitability of equating anonymisation to a set of technical standards rather than a context specific legal standard which requires all objective factors to be considered so as to ensure a high standard of personal data protection.

6. Data intermediaries

What the consultation says

The government supports the use of data intermediaries and is considering how it can best support the various data intermediary activities such as data sharing, processing and pooling to "ensure responsible and trusted data use, empower

data originators, enable low-friction data flows, and support the development of healthy markets".

The NDG's considerations

Data intermediary is a broad term that covers a range of different activities and governance models for organisations that facilitate greater access to, or sharing of, data. An example of a data intermediary in health and social care is the NHS Digital Trusted Research Environment (TRE), which provides approved researchers from trusted organisations access to data for research.

The NDG is supportive of mechanisms which safeguard personal data by providing secure environments for access to data, rather than downloading and exporting the data. The NDG also recognises that the TRE model of data stewardship has the potential to earn greater public trust in the use of health and social care data for reasons other than individuals' own care, and which benefit the public. Existing citizens jury research demonstrates that the public puts more trust in data access through software platforms such as OpenSAFELY, where those accessing data cannot make additional copies.

It is not clear from the consultation that all data intermediaries will operate in ways that enhance privacy and protect individual rights. The government should provide evidence regarding how intermediaries (such as data exchanges where data can be advertised and sold) will enhance the rights of individuals (**paragraph 129**). There are clear benefits to secondary data use; however, as we have seen recently with the public reaction to the planned GP Data for Planning and Research Programme, this must be approached carefully and sensitively to ensure the reasonable expectations of the public are met.

Throughout the discussion on data intermediaries, the government raises concerns about risks of missed opportunities because of a lack of an established framework, meaning organisations lack the confidence to use such services. However, the consultation does not evidence how the current regime inhibits the use of data intermediaries. Additionally, it does not state a clear use case, or a potential framework for intermediaries to work within, but rather states only that one does not currently exist. The government should explain the clear benefits they see in the use of intermediaries, elaborate on what they define as responsible uses of data, and provide specific examples of best practice.

Recommended actions

- Provide evidence as to how the existing regime is prohibitive in relation to the intended uses of data intermediaries
- Provide clear examples of the intended uses of data intermediaries
- Outline a framework for which they are intended to operate within, including how the protection of individual rights will be maintained

Use of personal data in the COVID-19 pandemic

What the consultation says

In Chapter 4 (delivering better public services), the government discusses the use of personal data throughout the COVID-19 pandemic. The consultation states that whilst the existing regime has allowed personal data to be shared throughout the pandemic, considerable time had to be spent ensuring data processing activities were lawful (**paragraph 279**).

The NDG's considerations

The government cites difficulties for private organisations in identifying a lawful basis for the processing of personal data which has been vital for the COVID-19 pandemic response. To resolve this, they propose allowing private organisations to rely on Article 6(1)(e) (processing is necessary for the performance of a task carried out in the public interest) when they are asked to process data at the request of a public authority (**paragraph 282**).

Powers that permit data use and sharing in the health and care sector have a purposefully narrow scope and are rightly subject to stringent safeguards. This ensures that public bodies that rely on such powers are accountable and can justify their data use. Appropriate and proportionate data use is important to ensure high standards of health and social care are maintained. However, the government has provided little evidence that the existing regime has presented any barrier to information sharing through the pandemic. It is also not clear how the accountability mechanisms that public bodies are subject to would be applied to private organisations in this instance. The government should consider whether the lack of organisational understanding they note could be overcome by advice and guidance from the regulator.

In its discussion of the processing of health data in an emergency (**paragraphs 284-286**), the government cites issues with "occasional complexity" in identifying a lawful basis for processing special category health data. They state this is a problem because:

"the legal ground for processing data for public health purposes currently requires the oversight of a healthcare professional or for the processing to be carried out by a data controller acting under a duty of confidentiality"

The government states that this is problematic for non-healthcare bodies who have been required to process special category health data throughout the pandemic. This statement is problematic for two reasons. Firstly, it fails to recognise that there is already an exemption available for non-healthcare bodies to process special category personal data where the processing is necessary for

reasons of public interest in the area of public health (Article 9(2)(i)). Secondly, while doctors are subject to legal and ethical obligations of secrecy, the obligation to uphold the common law duty of confidence is applicable to all who process confidential patient information, whether or not they are healthcare professionals. This should, and does, apply to non-healthcare bodies. The UK GDPR and DPA 2018 (Schedule 1(3)(b)) make it clear that this is a necessary safeguard when processing special category data for public health reasons.

Respecting the confidentiality of health data is crucial not only for the individual who is the subject of the data, but also for the preservation of confidence in healthcare professionals and the health and care service more generally. The ramifications of eroding this duty are well known and understood. Therefore, the NDG is opposed to the government proposal to "clarify that public and private bodies may lawfully process health data…irrespective of whether the processing is overseen by healthcare professionals or undertaken under a duty of confidentiality" (**paragraph 286**). Upholding the common law duty of confidence is an irreducible minimum in ensuring that a trustworthy confidential health and care system is safeguarded.

Recommended actions

- The government should reconsider proposals that are in direct conflict with common law confidentiality principles
- Consider whether guidance could achieve the desired outcomes to improve data sharing in emergencies
- If legislative changes are to be incorporated, the government should first provide evidence as to how the existing regime has been prohibitive. Occasional complexity is a low bar for significant legislative reform

Conclusion

The NDG's response has concentrated on the areas of the consultation that may impact the health and social care system. While supportive of the overall aim of building an improved data protection regime and appreciating that there are undoubtedly challenges in implementing certain elements of the existing data protection regime, the government has thus far provided insufficient evidence to support many of the issues they have identified in this consultation as needing legislative fixes. Furthermore, information regarding the real-world impact of the government proposals is sparse, and the benefits of these changes have not been sufficiently quantified.

Some government proposals, such as amendments to research provisions, rules on automated decision making and changes to data subject rights, would represent a significant departure from EU data protection law. Any altering of

existing legal provisions in an effort to provide clarity should be carefully scrutinised, especially if they will affect adequacy. For example, in the research context, any positives derived from an attempt to clarify rules on consent, where consent is not the usual lawful basis, will be far outweighed by a loss of adequacy that would see UK research organisations having to implement standard contractual clauses to receive data from the EU in pan European clinical trials and digital research projects. The risk to our status as adequate needs to be carefully considered in each of the proposals laid out in this consultation.

The NDG encourages the government to provide further evidence to support the proposals in the consultation, so as to be clearer about both the nature and degree of the current problems that it is seeking to address, and thereby to ensure the balance is in favour for any proposed solutions against their potential risks. The government should take an iterative approach and engage with key stakeholders within the heath and care system. This will help the government to understand the issues that are of significant importance, and ensure any unintended consequences are avoided.