## Call for Evidence on the Current Data Protection Legislative Framework

### General

**Question 1.** What are your views on the current Data Protection Act and the European Directive upon which it is based? Do you think they provide sufficient protection in the processing of personal data? Do you have evidence to support your views?

### Comments:

1. The Research Councils welcome the opportunity to respond to this call for evidence. The seven UK Research Councils all hold or have an interest in personal data for various reasons – these include human resources and the personal data of Research Council employees; application processing and personal data relating to researchers and peer reviewers and also uses of data for research purposes which includes social, economic, medical and health related information about individuals. The latter is the main focus of this response.

2. The MRC was represented at a workshop along with the Ministry of Justice in September 2010 which aimed to highlight issues relevant to research and data protection.

3. The Research Councils support the recommendations of the Thomas / Walport Review[^1] which aims to facilitate use and sharing of data for research.

4. The Research Councils consider that the DPA principles do provide protection but interpretation of these and of the Act can vary and be difficult to apply, particularly in relation to specific research settings, for example such as generic consent for research as discussed further below.

5. The Act does not allow for a risk based approach to processing, consent and security requirements. An example is large-scale data processing of de-identified data: such data are rich enough that it would be difficult to prove that all records are not personal data (as a small number may indeed be identifiable with sufficient work); however, it is impossible to know which specific records may be high-risk. It is the case that the individual contribution from each record is low (as power of investigation is from large numbers); however, the cost of explicit consent is comparatively high.

6. There is a need for a greater clarity within the Act with respect to the meaning of ‘research access’. The Act should define such access and outline the framework of a risk based approach to be used in deciding upon access to personal data for research purposes. This would enable data guardians to make a more effective assessment of risk and cause them to be less risk averse in making their assessments, because the guidance would be clearer. At the moment guidance is available, but it is not enshrined within the Act.

7. Collection, storage, use and sharing of biomedical research data sits in a complex framework which also includes the common law duties of confidentiality and consent and, when derived from health records, s251 of the NHS Act 1996[^2] and the Statistics and Registration Service Act 2007[^3]. The appropriate consent and use of data requires review by ethics committees, local hospital R&D offices, Caldicott guardians (for patient data). Consent may also be reviewed by National Information Governance Board Ethics and Confidentiality Committee and by funding bodies. Many studies collect, store and use both human data and linked tissue samples –

with associated requirements of Human Tissue legislation (which differs in Scotland).

8. In practice, this often leads to confusion\(^4\) as to the relevant standards and requirements. This is a particular issue for consent, where there may be a lack of clarity around what is required for compliance with the DPA as compared with common law or other statutory requirements as well as codes of practice and other guidance from bodies such as the General Medical Council or funders such as the MRC or ESRC. This has led to a risk-averse culture in which researchers are required to obtain individual consent, even for data collection and use that may be unidentifiable or with very low risks of disclosure or harm for research participants, in a manner that is overly bureaucratic to the disadvantage of both the research and the members of the public. This also means that potential exemptions in the Act are very rarely applied due to concern as to when they can be lawfully used.

9. A growing area of research interest in recent years is the use of administrative datasets (collected and managed by Government Departments and other service providers) for research purposes. Such datasets, because of their size and universality, have enormous power and range of potential uses. At present this is mainly linked to enhancing the value of existing longitudinal studies, through linking a current cohort with administrative datasets and thereby expanding the range of data that is otherwise routinely collected through surveys. For example, this might include educational records or benefit records. Issues of ownership, data control, security standards and consent are unclear for linked datasets, leading to an inconsistent approach in the application of the DPA. Specific guidance for linked datasets would be welcomed.

10. An area that is set to grow significantly over coming years is the use of electronic health records for scientific research. With the significant investment by the Department of Health in the Research Capability Programme, a secure infrastructure will be provided to access a range of federated NHS data sources in a safe and anonymised way. Such access is also being provided by similar infrastructure in Wales (Secure Anonymised Information Linkage) and Scotland (Scottish Health Informatics System). The volume of reliable real-life data available through this infrastructure will greatly facilitate both epidemiological research as well as social and health-related research.

11. Clearly when utilising such data there is an imperative to ensure that it is used in a secure manner and that the proper consent has been obtained from the data owner and the individual. The project teams managing the infrastructure described above are clearly responsible for ensuring that this complies with current legislation. From the Research Councils perspective, any research project funded that utilises this data would also be expected to comply with all relevant legislation. In addition it would need to ensure that the MRC\(^5\) and ESRC’s published guidance and Frameworks\(^6\) for Research Ethics as well as guidance from any co-funders is fully adhered to. Nevertheless, it is also important that the clear research potential from using this data are maximised to the fullest extent possible within the constraints that are outlined above.

12. One further example is where data are collected for medical purposes, e.g. in an NHS setting, this is fairly processed provided that patients are told in the fair collection information that data collected can be used for medical purposes, service management, education and sometimes explicitly research. Research is included within the definition of medical purposes and so members of the care team have

---

\(^4\) [http://www.bmj.com/content/332/7534/165.extract](http://www.bmj.com/content/332/7534/165.extract)

\(^5\) [http://www.mrc.ac.uk/Ourresearch/Ethicsresearchguidance/index.htm](http://www.mrc.ac.uk/Ourresearch/Ethicsresearchguidance/index.htm)

\(^6\) [http://www.esrcsocietytoday.ac.uk/escinfocentre/opportunities/research_ethics_framework/](http://www.esrcsocietytoday.ac.uk/escinfocentre/opportunities/research_ethics_framework/)
legitimate access to process this data for their own research, whereas a research nurse employed by a collaborating university is deemed unable to do this without further explicit research consent. This position has arisen because of interpretations in how wide the duty of confidence extends, although this is perceived by many investigators and research managers as a DPA requirement.

Definitions

Question 2. What are your views of the definition of “personal data”, as set out in the Directive and the DPA?

Comments:
13. The definition of ‘personal data’ relates to whether data are ‘identifiable’ or likely to be due to information available to data controller.
14. The definition is ‘binary’ i.e. data are or is not treated as under the DPA. However, research data or health data may be difficult to categorise in this way and the definition therefore depends on the meaning of whether the data controller possesses such information. When data become more distant from original identifiable records and undergo processes for de-identification it may be difficult to determine at what point they cease to be ‘personal data’ and hence cease to be under the remit of the Act.
15. The further definition of medical and sensitive data can be difficult to identify – this is a particular issue with cross-EU and other international collaborations where it is critical to ensure mutual understanding of such terms.

Question 3. What evidence can you provide to suggest that this definition should be made broader or narrower?

Comments:
16. The definition of personal data should be more explicit, not necessarily broader or narrower. For example, it is difficult to assess whether NHS number is identifiable. To the data controller, who has ready access to information which can identify individuals based on NHS number, it is readily identifiable. However to the general public, an NHS number is not identifiable. Although the NHS number under the definition of personal data with in the DPA is identifiable, it does not appear to researchers to make sense when it is considered from a confidentiality and disclosure view-point.
17. The Act also needs to take into account the changes in technology and information systems that have occurred and will without doubt continue to occur in relation to availability of large-scale datasets as discussed above.

Question 4. What are your experiences in determining whether particular information falls within this definition?

Comments:
18. Much research is conducted with anonymised or de-identified data. However, in some cases such data may lose its scientific value. The legislation should clearly define that where research data are considered to contain personal data that are not going to be anonymised, consent for data processing must be sought.
19. A difficulty is that under the Act data are either classified as non-personal and can be shared freely or as ‘personal data’ and consequently very restricted as requirements for consent cover all ‘personal data’. This is not an issue for clearly identifiable data, but de-identified or properly pseudonymised data, provided they are shared under appropriate restrictions should not require consent unless there is quantifiable risk to data subjects. Further restrictions relating to confidentiality (as opposed to data protection) may also need to be recognised by researchers.
20. When linkage to original records is retained the link may or may not be held by the
researcher in person. In the case of medical records that person could also be involved in the clinical care of the patient and thus have access to the clinical record through a different role. Therefore identification may be possible but could be far removed from the researcher or from the research activity and very unlikely to occur, even though the link may be held by the data controller. There may be a theoretical possibility of re-identification of just some records in a data-set, but with local controls (both technical and contractual) this risk can be mitigated. There is no mechanism in the Act to recognise this. Often the test is whether the data could be made publicly available rather than only to a controlled secure environment.

21. The Human Tissue Authority treats linked tissue samples as anonymised even if linkage available to the researcher, thus in the Code of Practice for Research:

- 'There may be occasions when a clinician involved in research may also have access to a secure database that would permit identification of a sample used in research and the identity of the patient whose material is being used. Providing the research material is not identifiable to the researcher (e.g. coded by a laboratory accession number) and the researcher does not seek to link the sample to the patient, it will still be regarded as non-identifiable and the research will be permissible without consent if approved by a recognised research ethics committee.'

22. This is a potential discrepancy between the approach to data and tissues which is difficult for researchers to understand and manage.

23. Therefore, the Research Councils propose that the Act should recognise that identification of data is not binary in research use. It should adopt an approach that does not force artificial demarcation but allows a proportionate risk-based approach.

24. Issues relating to identification also arise in relation to small populations, for example rare diseases or ethnic minorities. However, researchers in these areas are used to dealing with such situations and ensuring that confidentiality is maintained unless appropriate consent is available where such results will be in the public domain. However, the issues relating to data protection requirements around identifiable data may be more difficult for researchers to interpret in this scenario. This highlights the overlap for medical research between meeting the requirements of the DPA and the common law of confidentiality.

Question 5. What evidence can you provide about whether biometric personal data should be included within the definition of "sensitive personal data"?

Comments:

25. The nature of biometric data needs to be more clearly defined but the consultation documents raise the issue of biometric personal data as a source of identification of the individual rather than a source of medical or sensitive information and indeed we are not aware of any evidence to counter this for the types of data quoted. As such, biometric data would not appear to be more sensitive than other identifying data. The aspects that would be sensitive would, in our view be those that link to other information that could be viewed as sensitive – for example disease risk or behavioural characteristics.

26. Thus, the biometrics described may provide more specific identification than, for example, a name alone but are not being considered to carry more information than identification.

27. A further issue would arise if it became the case that the biometric data, in itself could contain more sensitive information about an individual, this would need to then be

---

7 [http://www.hta.gov.uk/legislationpoliciesandcodesofpractice/codesofpractice/code9research.cfm?FaArea1=customwidgets.content_view_1&cit_id=763&cit_parent_cit_id=757](http://www.hta.gov.uk/legislationpoliciesandcodesofpractice/codesofpractice/code9research.cfm?FaArea1=customwidgets.content_view_1&cit_id=763&cit_parent_cit_id=757)
considered in the same way as other data containing information relevant to health or other relevant areas.

**Question 6. If as a data controller you process biometric data, do you process it in line with Schedule 3 of the DPA which imposes an additional set of conditions?**

**Comments:**
28. We are not aware of examples of this being done.

**Question 7. Are there any other types of personal data that should be included? If so, please provide your reasons why they should be classed as “sensitive personal data”?**

**Comments:**
29. It seems difficult to determine what information an individual would deem sensitive. There are widely differing attitudes to personal information such as marital status, sexual orientation, contraceptive use and financial information.
30. In some instances ‘sensitive personal data’ can be applicable not only to the data subject, but also to related persons (e.g. family members, partners) and data categories such as ethnic origin, religious beliefs and sexual life to an extent. Such personal data of the data subject could be disclosed quite easily with information on their family members.
31. For some people, information relating to, for example, debt or divorce could be deemed much more private than that relating to their health such as having a chronic condition like asthma or diabetes. The difficulty in defining sensitive data lies in determining what an individual would regard as private and distressing if disclosed.
32. While it seems reasonable to concur that health information is ‘sensitive’ there will be information contained in the health record that may not be deemed as such by an individual. The record will also include identifiable but non-sensitive data.
33. It may be more helpful to consider risk of harm or distress and provide examples, such as certain health information where disclosure would be highly likely or unlikely to cause such harm. This would support a move towards a risk-based approach – although could lead to more subjective decision making. The risk with a ‘one size fits all’ approach is that it invites misinterpretation by data guardians. It is much easier to resist a request for access to personal information for research purposes, because you cannot be reprimanded for denial of access if unsure about an access request (and unsure about the interpretation of ‘research access’ within the meaning of the DPA), whereas a mistake in granting access when this should not be the case can result in loss of one’s job (or worse penalties).
34. The documentation does not specifically consider genetic data which could provide both identity and health or behavioural information. If such data are to be considered we believe it is important that it is recognised that not all ‘genetic data’ is identifiable nor does it necessarily contain information about specific risks to an individual. The type of information will depend upon the amount and nature of material held and analysed and the additional information associated with it. Equally where genetic data is identifiable it must be treated with appropriate security and confidentiality.

**Question 8. Do you have any evidence to suggest that the definitions of “data controller” and “data processor” as set out in the DPA and the Directive have led to confusion or misunderstandings over responsibilities?**

**Comments:**
35. These definitions impose at times a distinction that is difficult to apply in practice, for example when research data are shared between researchers or Institutions.
36. It would be more practical and achieve the desired aim more effectively if the legislation set out the functions that need to be met for lawful data processing.
Research teams and Institutions could then agree who will perform and take responsibility for each function.

37. This would mirror the approach to responsibilities set out in the Research Governance Frameworks of the Departments of Health\(^8\) and the Medicines for Human Use (Clinical Trials) Regulations 2004\(^9\)

38. The term Data Controller is widely misunderstood. Researchers (who are technically data processors) are in control of collection, validity, analysis and publication of the data, and therefore believe themselves to be data controllers. It is the experience of the MRC Regulatory Support Centre that many draft ethics approval submissions incorrectly name the Data Controller as the Chief Investigator.

**Question 9.** Do you have any evidence to suggest that the separation of roles has assisted in establishing responsibilities amongst parties handling personal data?

**Comments:**

39. The current separation of roles is confusing and the terms are frequently misunderstood, the fact that in much research the data controllers are dissociated from the processes under which the majority of personal data held, adds to the confusion and complexity.

**Question 10.** Is there evidence that an alternative approach to these roles and responsibilities would be beneficial?

**Comments:**

40. The ability to share responsibilities across different groups or organisations is beneficial, for example in sponsorship of clinical trials or other research. It allows multi-site research to take place with appropriate responsibility being taken for local processes and procedures. This offers better protection to participants as one single body or person does not need to assume responsibility for processes it does not directly operate. In addition, it reduces the need for additional, and often unnecessary, review and inspection by the third party that would need to take this central role.

41. Thus an approach setting out clearly defined responsibilities that need to be allocated may be more beneficial in achieving the desired aims.

42. UK organisations have advocated this approach to the EC in their review of the Clinical Trials Directive as it would allow improved conduct of multinational research. A parallel approach in data protection legislation is essential to ensure harmonised approaches to clinical trial data and liability across Europe.

**Question 11.** Do you have evidence that demonstrates that these definitions are helpful?

N/A

**Data Subjects' Rights**

**Question 12.** Can you provide evidence to suggest that organisations are or are not complying with their subject access request obligations?

**Comments:**

43. Data Subject Access Requests received by the Research Councils are most likely to be from current or former employees and research funding applicants; research centres and institutes supported by the Research Councils may also receive Subject


Access Requests from research participants. To inform this call for evidence ESRC has consulted with the National Centre for Social Research (NatCen) and Institute for Social and Economic Research (ISER) who are data processors for a number of ESRC data resources. Neither reported many requests relating to participation in data collection. This is largely because much of their work involves anonymous research and the exemption from Subject Access Rights would apply. The NatCen position on requests is that where they get these they do not refuse on the basis of the exemption, but aim to have a reasoned dialogue with people in that context, and also about the difficulty/impracticality of providing them with an intelligible record of what they said in an interview. Most people are satisfied as a result. ISER occasionally oblige people, at no charge, if it is relatively easy for them to generate a record of what they've said (paper questionnaires, self-completion questionnaires, short computer aided interviews with little routing where answers can be transcribed onto a print-out of the question listing).

**Question 13. Do businesses have any evidence to suggest that this obligation is too burdensome?**

**Comments:**

44. The obligations relating to Subject Access Requests are not seen as burdensome.

**Question 14. Approximately how much does it cost your organisation to comply with these requests?**

**Comments:**

45. The cost of complying with Subject Access Request and related queries from current and former employees, research investigators and research participants is low, for example in the case of ESRC it is approximately half a day per month effort from a Band E (SEO).

**Question 15. Have you experienced a particularly high number of vexatious or repetitive requests? If so, how have you dealt with this?**

**Comments:**

46. The Research Councils have not received a high number of vexatious or repetitive Subject Access Requests. Some Research Councils, such as ESRC, have received some repeated requests; this is believed to be due to the fact that ESRC does not release assessment grades (the personal information being sought) as part of normal business. Other Research Councils, who release such information routinely to research applicants in confidence, do not receive such requests.

47. Neither NatCen nor ISER has received vexatious or repetitive requests, however requests would be time-consuming and expensive to respond to if the number became significant given the way the data is held.

**Question 16. What evidence is there that technology has assisted in complying with subject access requests within the time limit?**

**Comments:**

48. Internal Research Councils systems have been developed to support the efficient retrieval of personal information requested relating to Human Resources and research funding proposals.

49. Comments from ISER and NatCen suggest that the advent of Computer Assisted Interviewing technology has made it more difficult to respond to requests from research participants, since the storage format is much less intelligible/accessible than that of a paper questionnaire.

**Question 17. Has this reduced the number of employees required and/or time taken to**
| Question 18. | Is there evidence to suggest that the practice of charging fees for subject access requests should be abolished? |
| Comments: | In some cases the Research Councils do not apply charges for responding to Subject Access Requests, this is largely where the information request can be easily accessed and retrieved. |

| Question 19. | Do you have evidence that the £10 fee should be raised or lowered? If so, at what level should this be set? |
| Comments: | N/A |

| Question 20. | Do you have evidence to support the case for a “sliding scale” approach to subject access request fees? |
| Comments: | The Research Councils would support a sliding scale approach in cases where providing the information requested would be onerous; this may apply to extensive health records, or large amounts of printed material. |

| Question 21. | Is there evidence to suggest that the rights set out in Part Two of the DPA are used extensively, or under-used? |
| Comments: | These are the rights to request data but also to request processing is stopped, with facility for enforcement through Court and compensation if distress caused. |
|  | It is unusual for research studies to receive requests to stop processing data. However, it is standard practice for consent to participate in research to include the option that participants can withdraw at any time if they wish. |
|  | Some longitudinal studies, which collect data on a long-term prospective basis, will offer additional options as to what subjects would wish withdrawal to mean – i.e. all data can be removed with no further contact; data to date can be retained with no further contact or collection or variations of this. An example is UK Biobank[^10] which describes these options as ‘no further contact’; ‘no further access’ and ‘no further use’. |
|  | It may not be possible to remove research data that have already been completely anonymised (with no link retained) or published/backed up on remote systems where access is not possible. |

| Question 22. | Is there evidence to suggest that these rights need to be strengthened? |
| Comments: | The Research Councils are not aware of such a need in the research arena although care needs to be taken when dealing with international transfer of data to ensure the same rights are respected. |

---

[^10]: [http://www.ukbiobank.ac.uk/docs/BIOINFOBK14920410.pdf](http://www.ukbiobank.ac.uk/docs/BIOINFOBK14920410.pdf)
58. For Research Councils there would be an expectation that data breaches are notified to subjects unless there are exceptional reasons where this is not appropriate, proportionate or reasonably practical or if there can be absolute confidence that no harm will arise – for example lack of confidence in old contact details which could lead to inadvertent breaches of confidentiality when trying to contact participants. Guidance on such cases would be from the Information Commissioner’s Office (ICO), a research ethics committee and/or NIGB Ethics and Confidentiality Committee.

59. The reputation of the Research Councils is of utmost importance as is public trust in research and use of data for research, therefore the default expectation would be to inform participants of any such breach. While informing the ICO is not necessarily required as an additional step unless there is evidence that other research does not meet these standards, the ICO can support communications with participants.

60. The Research Councils support the current system whereby only serious breaches require reporting and are therefore of the view that this does not require additional statutory regulation. In the context of sample surveys we would also be reluctant to support the idea of routine notification of respondents about breaches. Research Councils would want to be satisfied that the breach could be associated with a named individual and that the data were sensitive - many survey questionnaires would not meet this threshold. Another criteria which could justify notification is where data subjects may need to take steps to protect themselves against breaches (e.g. against identity theft).

<table>
<thead>
<tr>
<th>Question 24.</th>
<th>What would the additional costs involved be?</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 25.</th>
<th>Is there any evidence to suggest that data controllers are routinely notifying data subjects where there has been a breach of security?</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 26.</th>
<th>Do you have evidence to suggest that other forms of processing should also be exempt from notification to the ICO?</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 27.</th>
<th>Do these current exemptions to notification strike the right balance between reducing burdens and transparent processing?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments:</td>
<td>61. Each request must be considered on its own merits and a level of judgement would be required.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Powers and penalties of the Information Commissioner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 28.</td>
</tr>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Question 29.</th>
<th>What, if any, further powers do you think the Information Commissioner should have to improve compliance?</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Question 30. Have you had any experience to suggest that the Information Commissioner could have used additional powers to deal with a particular case?
N/A

The Principles-based Approach

Question 31. Do you have evidence to suggest the current principles-based approach is the right one?
Comments:
62. In general the principles do not give rise to difficulties for research although further explanation of the terms would be useful. However, Councils agree with the accompanying documents that it is interpretation and application of the principles 'on the ground' assessments which can be difficult.

Question 32. Do you have evidence to suggest that the consent condition is not adequate?
Comments: See below

Question 33. Should the definition of consent be limited to that in the EU Data Protection Directive i.e. freely given specific and informed?
Comments:
63. Medical research has a strong underlying principle of requiring consent for participation and this has also been adopted in many other areas of research. This is of key importance when the nature of research is a specific intervention for which consent would be required if it were a medical treatment. However, as research moves into other areas such as data collection and large scale or broad purpose studies specific consent may not be possible or appropriate. There are also existing mechanisms, such as s251 of the NHS Act to allow access to records for research without individual consent.

64. The Research Councils do not agree, for the reasons below, that ‘specific’ and ‘informed’ are the correct limitations and they strongly oppose this proposal – which would certainly be detrimental to current practice of research without an obvious need for such damage to occur. Use of the term specific limits the data subject’s ability to make a perfectly reasonable broad agreement for uses such as ‘medical research’. This would seriously undermine models based on sharing of anonymous data with large numbers of researchers/teams pursuing different lines of enquiry. Indeed one of the particular strengths of the model is that it provides opportunities for important new research which was not initially anticipated.

65. The concept of ‘informed’ consent is difficult to apply in its fullest sense to research – consent is often sought to hold data for a particular study and to retain it for future relevant research approved by an ethics committee. This ‘generic’ consent is supported by the MRC and was also endorsed by Parliament in debates on the Human Tissue Act 2006 and by the HTA. In addition there will be times when ‘opt-out’ consent is also ethically appropriate and important for conduct of a study and the proposed approach would prevent this.

66. Consent to participate in research, including storage of data will always be supported by information provided to the participant or communities and this is an important component to obtaining freely given consent.

Question 34. How do you, as a data controller, approach consent?
Comments:
67. Research participants will often be asked for individual consent to take part in a particular specified study. In the case of longitudinal studies, consent is re-sought when further information is requested, in addition many studies have regular
communications to ensure participants remain appraised throughout the course of the study.

68. There are limited exceptions to this; any projects using such exemptions would need research ethics committee approval to do so. For example, access to health records without consent is lawful with NIGB ECC approval.

69. Information sheets for participants will include information relating to the specific research project and likely use conforming to DPA fair processing information requirements.

Question 35. **Do you have evidence to suggest that data subjects do or do not read fair processing notices?**

Comments:
70. Where relevant these are contained in the information sheets which participants are provided with before consent is given. There will often also be dialogue with researchers or clinical staff involved in the research where this information is discussed in detail.

71. The Research Councils would strongly encourage the use of notices and leaflets to educate patients/public on the potential benefits to research from the uses of their data; and, in the case of medical research, that this is in accordance with fair processing in the NHS.

Exemptions under the DPA

Question 36. **Do you have evidence to suggest that the exemptions are fair and working adequately?**

Comments:
72. The research exemption is not well understood. Some believe it exempts from all of DPA requirements and potentially related confidentiality requirements.

Question 37. **Do you have evidence to suggest that the exemptions are not sufficient and need to be amended or improved?**

Comments:
73. The Research Councils support the conclusions of the Thomas/Walport Review of data sharing. The exemption for ‘research’ is poorly understood and difficult to align with other relevant areas of regulation in this area.

74. Often researchers are prohibited from applying this exemption by interpretations of their common law duties; by regulatory guidance from other bodies or by local approval mechanisms.

75. Lack of clarity has led to a lack of confidence to apply this exemption and a default approach that specific consent must always be applied to any research project involving personal data (often even that which will be non-identifiable).

76. Although consent should be the rule, there is room for exceptions that should be clearly defined. When data are going to be anonymised without losing their value for re-use, such consent may not be a requirement. Legislation should therefore consider scenarios, as exceptions to a rule.

International Transfers

Question 38. **What is your experience of using model contract clauses with third countries?**

Comments:
N/A

Question 39. **Do you have evidence to suggest that the current arrangements for transferring data internationally are effective or ineffective?**
<table>
<thead>
<tr>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>77. Many studies require or would greatly benefit from international collaboration including data sharing. This is the case for large scale work, for example in genetic links to disease or epidemiological studies or for work in rare diseases.</td>
</tr>
<tr>
<td>78. However, such sharing is very difficult as researchers are unclear as to standards outside the EU and whether these are sufficient to comply with the Act.</td>
</tr>
<tr>
<td>79. A greater harmonisation of legislation on DP across the EU is an absolute requirement. However the need for harmonisation includes other countries with which the UK is engaged in research activities that require data sharing. This would particularly apply to the US, but also Canada, Australia and New Zealand. Given the internationalisation of a research agenda that is driven by global challenges, there will be a growing demand for data sharing, including microdata. Therefore the benefits of harmonisation are more important than ever before.</td>
</tr>
<tr>
<td>80. Greater clarity and guidance with case studies would assist this, specifically addressing issues arising from working with countries which do not have similar legislative frameworks in place or which only operate voluntary codes of practice. The Act should also cater for a consistent and proportionate approach in breaches of data protection and the penalties that can be applied across other countries.</td>
</tr>
</tbody>
</table>

This evidence is submitted on behalf of Research Councils UK (RCUK). RCUK is, the strategic partnership which aims to champion the research supported by the Research Councils and to enable them to work together effectively to enhance the overall impact and effectiveness of their research, training and innovation activities, contributing to the delivery of the Government’s objectives for science and innovation. Further details are available at [www.rcuk.ac.uk](http://www.rcuk.ac.uk). This submission represents the independent views of the Research Councils; it does not include or necessarily reflect the views of the Department for Business, Innovation and Skills. The submission is made on behalf of the following Councils:

- Economic and Social Research Council (ESRC)
- Medical Research Council (MRC)
- Science and Technology Facilities Council (STFC)