

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

1. The PHG Foundation is the successor body to the Public Health Genetics Unit. Its purpose is to enable and foster the responsible and evidence based application of biomedical science for the benefit of human health. Among its specific objectives is the fostering of a social and regulatory environment receptive to the application of biomedical science for health, but at the same time imposing an appropriate, equitable and proportionate regulatory burden. The Foundation has a particular interest in genetic research and its impact upon clinical and public health services
2. The Foundation contributed to a study carried out by the Academy of Medical Sciences entitled 'Personal Data for the public good: using health information in medical research'¹. This report examines the rationale for and governance of medical research, particularly that which uses clinical data for secondary purposes such as epidemiological research. Such research forms the basis of much public health practice and is an integral part of the development of evidence based care within the NHS.

¹ <http://www.acmedsci.ac.uk/p48prid5.html>

3. Not only does medical research inform health care, but it can also be justified on sound economic grounds as the UK has a well deserved reputation for high quality medical research worldwide.² The introduction of electronic patient records (as part of NPfIT) also has the potential to strengthen this role by combining a unique resource (patient data) with an integrated health delivery system.
4. Evidence provided to the Academy of Medical Sciences as part of their project revealed a more confused and demoralised picture: this included concerns over complex and conflicting legislation, duplication of administrative effort and an increasing rhetoric around privacy and autonomy interests (at the expense of public interests). Our hope is that this data sharing review will help to identify the very real benefits of data sharing in the context of medical research, to clarify existing ambiguities and endorse a pragmatic and proportionate model of data sharing that can accommodate existing legitimate uses of personal data.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2: What in your view are the key benefits of sharing personal information to a) individuals and b) society?

5. Our focus is upon research which uses personal data to frame generalisable results applicable to groups or populations. Examples abound of how secondary research has been used to identify the causes of disease, reduce risk factors and evaluate different types of intervention and treatment. These types of secondary research have benefits for individuals and society.
6. The PHG Foundation has contributed to the Academy of Medical Sciences response to this data sharing review and strongly supports and endorses the points made therein. Similarly in the clinical setting, the sharing of personal information between family members forms the basis for diagnosis and treatment of many inherited conditions. The PHG Foundation has also contributed to the submission made on behalf of the British Society of Human Genetics.

Question 3: What in your view are the key risks of sharing personal information to a) individuals and b) society?

² http://www.hm-treasury.gov.uk/independent_reviews/cooksey_review/cookseyreview_index.cfm

7. Personal information varies in sensitivity: genetic information is often regarded as particularly sensitive especially if it indicates an increased likelihood of developing future disease. Regulations designed to prevent abuse of such information by employers and insurers are in place. However clinically significant findings cannot be inferred from the majority of genetic information: much genetic information is inferentially neutral. To this extent we would not like to see genetic information singled out as a class of information that demands special safeguards. The PHG Foundation rejects the doctrine of genetic exceptionalism and supports a more proportionate view of risks and harms of sharing genetic data. On this basis, provided that systems are secure and staff well trained, most research involving personal data including genetic data poses a low risk to data subjects.
8. In a clinical setting we consider that risks are more likely to arise as a result of poor data security rather than deliberate breach of confidentiality since those processing sensitive personal genetic data are well aware of the requirement to keep patient information confidential.

Question 4: What scope and methods of personal information sharing, in your view, pose the greatest opportunities and risks?

9. Combining data from a range of databases including those held in existing patient records could be a powerful research tool subject to appropriate safeguards. Plans for the Secondary Uses Service to strip personal data of its identifiers prior to use by researchers may be a valuable development especially if it can facilitate and streamline the process by which researchers' access anonymised data. However there may still be instances where particular research demands the processing of identifiable data (such as postcode data to assess environmental susceptibility). Flexible use of other honest brokers and safe havens subject to appropriate governance structures should be encouraged.³
10. In the clinical environment the introduction of electronic patient record systems which fail to properly acknowledge the role of the family as a unit of care is a source of concern. Systems that allow individuals to seal and lock personal genetic information at the expense of sharing that information with family members (at risk of compromising clinical care and causing serious harm) need to be extensively reviewed before they are introduced into a clinical genetics setting.

Question 5: Where, in your view, do public authorities hold too much data

³ Such as the Care Record Development Board (2007) Report of the Care Record Development Board Working Group on the Secondary Uses of Patient Information, Recommendation 5.1 at <http://www.connectingforhealth.nhs.uk/crdp/workstreams/secusesreport.pdf>

or not enough personal information?

11. Registers of cancers, diseases and congenital abnormalities have the capacity to capture public health data unavailable from other sources. Systems which facilitate such data sharing should be encouraged.

Question 6.

Comments:

Question 7: Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.

12. The clinical investigation of some clinical conditions involving the sudden cardiac death of young adults⁴ is sometimes handicapped by a failure of effective data sharing between pathologists, coroners, genetics laboratories and genetics departments. Evidence suggests considerable variability in practice and funding across the UK.

Question 8.

Comments:

Section 3: The legal framework

Question 9: In your view, how well does the Data Protection Act (DPA) work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

13. In theory, the DPA provides a powerful and flexible framework for data processing: it sets out a list of data processing principles and provides for a framework of checks and balances. In practice however, some of the principles are unclear (such as the obligation for fair and lawful processing) and the legislation is unduly complex. In particular practical guidance in respect of the following would be helpful:

- Fair processing and the scope of the obligation to notify (as opposed to seek consent) for secondary medical research;
- Anonymisation of data;
- The extent of the obligation to respond to subject access requests

⁴ Such as Long QT syndrome.

(in the context of family history information);

- The interpretation of S.33 (use for research and statistics);
- Sharing of personal data in respect of incapacitated adults in the context of medical research.

Question 10.

Comments:

Question 11: What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

14. The Academy of Medical Sciences Report already cited reviewed many of the relevant barriers. We share the concern that one of the most pervasive barriers to the effective data processing in the context of medical research is the uncritical application of the 'consent or anonymise' mantra. The combined thrust of the DPA and common law of confidentiality supports a more nuanced interpretation which calls for a proportional balancing of the risks to individuals as against the potential benefits to society.

15. We welcome empirical work that has sought to simulate the role of the Secondary Uses Service in a variety of research settings⁵ and moves to integrate research application systems⁶ however are concerned that these practical developments have been implemented at the expense of the more nuanced approach outlined above.⁷

Question 12: What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA?

16. Our view is that the plethora of applicable legislation and guidance promotes confusion. There is merit in simplified (or codified) legislation which relates to medical research, supported by comprehensive guidance (upon issues such as generic/explicit consent, the process of seeking consent to participate in research, de-identification of data, data encryption and data security) – predicated upon the sensible application of the principle of proportionality.

Question 13: Are there any other aspects of UK or EU law (such as Directive 95/46/EC) that impact positively or negatively on data sharing or protection?

⁵ <http://www.ukcrc.org/>

⁶ Such as the launch of an integrated research application system.

⁷ For example the default option for the processing of identifiable data is an application to PIAG. We would contend that this is not always mandated under current legislation.

17. A variety of UK and EU laws impact upon data sharing. In particular the EU Data Protection Directive 95/46/EC, the common law of confidentiality, section 60 of the Health and Social Care Act 2001 and the Human Tissue Act 2004 are relevant.
18. The EU Directive 95/46/EC differs from national legislation in some important respects. These include:
- The definition of medical research and extent to which the Commission has been notified of UK derogation from the directive;
 - Varying interpretations of 'anonymised', 'personal data' and 'relevant filing system' and the application of relevant case law.
- Guidance is needed which acknowledges these interpretative differences and which offers practical advice in the absence of definitive case law.
19. The common law of confidentiality recognises a public interest in the non-consensual use of an individual's personal data provided that it can be justified as being necessary and proportionate to the protection of health.⁸
20. Section 60 of the Health and Social Care Act (2001) provides for a statutory exemption from the obligation of confidentiality mediated by a statutory authority (the Patient Information Advisory Group). These powers have been reproduced in draft legislation which is currently undergoing Parliamentary review including the draft Human Fertilisation and Embryology Bill (2007) and the Health and Social Care Bill (2007). The scope of these powers lack clarity because there is ambiguity as to the extent to which applicants are relieved of obligations under the DPA (which in fact they are not). Researchers also cite the infrequency of PIAG meetings and time taken for a response as the cause of additional delay which can sometimes jeopardise the research taking place at all.
21. Where inconsistencies are apparent between different sets of legislation (such as between the Human Tissue Act 2004 and the Data Protection Act) which appear to lack theoretical justification, the continuing rationale for these differences should be debated and thought given as to whether legislation should be amended. For example, the Human Tissue Act 2004 provides for the retention, storage and use of existing holdings of tissue to be exempt from the Act. No such blanket provision applies to the processing of historical data.⁹ Different provisions apply to the use of material held for DNA analysis.¹⁰
22. Ambiguities around fair processing, the scope of a public interest defence to data processing have already been mentioned in answer to previous questions. The extent to which explicit consent is also required as a

⁸ See for example *Campbell v. MGN* [2004] 2 A.C. 457, HL and *R (Axon) v. Secretary of State for Health* [2006] 2 WLR 1130.

⁹ Section 33 of the DPA does provide for a limited exemption for processing historical or statistical data but this does not seem to be well used.

¹⁰ Human Tissue Act (2004) Section 45(2)(b).

prerequisite for allowing potential research subjects to be approached for participation in a research project (consent to consent), and for the anonymisation of personal data is also unclear.

Question 14.

Comments:

Question 15: Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples. Please outline your proposals for streamlining the legislation to ensure that such burdens are minimised.

23. We would urge a more proactive approach to public engagement via the Healthspace function of the Connecting for Health scheme, so that individuals could record their interest in participating in research (subject to appropriate safeguards around competence and information provision). Currently patient associations often provide an informal mechanism for researchers to engage with those afflicted by genetic diseases, and for public engagement. Using Healthspace for this purpose would be a way of extending this role.

Section 4: Consent and transparency

Question 16: Is it clear whether and when you need individuals' consent to share information about them? Are you clear what form that consent should take?

24. Examples of lack of clarity abound. They include the following:

- the form and need for consent for the recruitment of patients into a research study;
- the form and need for consent for the process of anonymising or encrypting patient data;
- the extent to which consent must be sought for ongoing research projects which an initial project has expired;
- the extent to which explicit consent must be sought for sharing genetic data within a family;
- whether explicit consent must always be sought for processing genetic information in a research (bearing in mind that this might not be of clinical significance);
- the status of proxies (for example using members of a clinical team as proxies for researchers).

Question 17: What, if any, barriers would a requirement for gaining consent create to the sharing of personal information?

25. Our view is that an approach that demands explicit consent to every instance of data processing is unworkable. Just as some instances of data sharing are justified in the public interest (such as the sharing of personal information between all those providing clinical care – an obligation which extends to support staff and students), many instances of data sharing for the purposes of secondary research can also be justified in the public interest.

Question 18: Do you have any suggestions on how to make the sharing of information more transparent?

26. Posters and leaflets should be available within primary and secondary care settings to inform patients how their data is used. At prescribed points within care pathways, patients should be informed how personal data is routinely shared between care givers and used for the purposes of audit and research. These opportunities might arise when a patient registers for the first time with a GP, attends an antenatal or outpatient's appointment, is admitted as an inpatient or seen in casualty. Recommendations for developing Healthspace also apply in this context.

Question 19.

Comments:

Section 5: Technology

Question 20: What impact in your view have technological advances had on the sharing and protection of personal information?

27. In the context of clinical genetics, the introduction of electronic patient record systems will allow individuals to seal and lock their detailed care records (although these operative details remain unclear).¹¹ This is likely to affect the practice of many clinical genetics units which customarily utilise family pedigrees (a composite record compiled from multiple family members).

Question 21: Should the law mandate specific technical safeguards for

¹¹ Care Record Development Board (2007) Care Record Guarantee at http://www.connectingforhealth.nhs.uk/nigb/crsguarantee/crs_guarantee.pdf

protecting personal information?

28. The stream of well-publicised instances where personal data has been lost, stolen or misused suggests that there is sloppiness amongst those who process data and general public ignorance as to the rationale for data protection. In the health service setting, general guidance on information governance (such as the information governance toolkit and the Information Governance Statement of Compliance¹²) has been supplemented by specific guidance on particular areas of concern, (such as bulk transfers of data). These should not compromise legitimate medical research.

Question 22: How, in your view, could ‘privacy enhancing techniques’, such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research?

29. Although terms such as anonymisation and pseudonymisation are widely used, determining what it means to anonymise data is much more problematic. Although effective anonymisation depends upon the context of data processing, technical processes such as data mining may allow linkage between disparate datasets which may threaten attempts at de-identification. Even those charged with research governance such as research ethics committees have traditionally viewed anonymisation as part of a simple equation as to whether those involved in research are reasonably likely to identify the data subject or not. For the most part this pragmatic approach seems to respect individual privacy. Nevertheless the threshold for advice from the Information Commissioner’s Office is much higher, requiring that the data processor considers the means reasonably likely to be used by a person who is determined to identify the data subject such as a hacker or investigative journalist.¹³ Whilst data processors clearly have an obligation to assess the effectiveness of their data security systems and processes in the context of rapid technical change, our view is that increased sanctions should be placed upon those who deliberately seek to de-identify personal data without legitimate cause, make onward disclosures or seek to profit from selling information to third parties who have an interest in it (for example insurers or private investigators). In addition there is a need for practical guidance as to how data processors can comply with this advice in an environment of rapid technological change.

¹² At <https://www.igt.connectingforhealth.nhs.uk/> and <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/igsoc>

¹³ Information Commissioner’s Office (21 August 2007) Data Protection Technical Guidance: Determining What is Personal Data, page 7 at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/personal_data_flowchart_v1_with_preface001.pdf

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:
