

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. Please explain what your interest in information sharing is.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- What kinds of personal information do you collect, hold and share?
- How do you collect, hold and share such personal information?
- For what purposes do you collect, hold and share such personal information?

Comments:

Local authorities are statutorily required to provide auditors and inspectors with data. Personal data invariably forms an element of this. The requirement includes the National Fraud Initiative, with which the Office of the Information Commissioner is already familiar. This information is typically provided to the Audit Commission under the exemption in Section 35 of the Data Protection Act.

Last year (2006/07) the Audit Commission managed the Best Value User Satisfaction surveys on behalf of Department of Local Government and Communities (CLG). The surveys were carried out by local authorities, with CLG providing postal address files for

identifying the sample of households to be sent questionnaires. Each questionnaire had a personal profile section to provide information about the respondent's age range, gender, ethnicity and disability, if relevant. The responses would identify respondents by postcode and personal characteristics, to allow the calculation of levels of satisfaction by authority as well as segmentation by particular groups of respondents. The Commission received the calculated results by local authority and does not hold individual responses as identified by postcode. CLG has ownership of the complete dataset.

In 2008/09 the Best Value surveys are to be replaced with a Place Based survey which is currently subject to consultation. CLG and the Audit Commission are agreeing a similar partnership arrangement for the management of this survey. The responses will be categorised by postcode for aggregation of responses by local authority and personal data will be used for segmentation by ethnic groups, age, disability etc. Ownership of the complete dataset will remain with CLG.

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?

Comments:

For individuals there are benefits around public sector information sharing as this has the potential to improve services delivered to individual citizens and the effectiveness of service outcomes. Users of public services expect more joined-up services, for example in the 'tell us once' initiative.

For society in general, benefits fall into two main aspects. The first aspect is benefits for the taxpayer through improved efficiency of service provision, which can be enabled by data sharing. Shared services are the obvious example of this. The second aspect is for the protection of society and vulnerable groups. This includes protection against fraud and criminal activity, for example our own National Fraud Initiative (NFI). The main aim of NFI is to match data to help identify and reduce the level of housing benefit fraud, occupational pension fraud and tenancy fraud. The Audit Commission liaises with the Information Commissioner's Office on a quarterly basis with regard to this.

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

Comments:

The overall risk would be if personal information were to fall into the wrong hands.

Question 4. As mentioned in the introduction, there are wide variations in the scope and methods of personal information sharing. What scope and what methods, in your view, pose the greatest opportunities or risks? Please explain the reasoning behind your response.

Comments:

No comment

Question 5. Please provide examples of where, in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.

Comments:

No comment

Question 6. Please provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.

Comments:

No comment

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.
Please explain as fully as possible why information is not being shared, detailing what the barriers to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.

Comments:

The following studies by the Audit Commission have identified key areas where information sharing would be beneficial but does not currently take place.

National study – Crossing Borders 2006

National data are not a good enough basis for planning local policy responses. Current local population projections and diversity data do not fully reflect the recent increases in migration for work. There is little evidence on who stays where or for how long, and limited information on the intentions of migrant workers, especially those from the accession states.

<http://www.audit-commission.gov.uk/Products/NATIONAL-REPORT/05CA5CAD-C551-4b66-825E-ABFA8C8E4717/CrossingBorders.pdf>

National Study - Neighbourhood Crime and Anti-Social Behaviour 2006

This report found that establishing neighbourhood approaches to reducing crime and anti-social behaviour required up-to-date information and that local partners did not always have a full picture of neighbourhood problems.

Over two-thirds of local Crime and Disorder Reduction Partnerships (CDRPs) and police Basic Command Units (BCUs) were recording anti-social behaviour within their own agencies, but coverage was patchy from other sources. For example, only 60 per cent were using information from neighbourhood wardens and only 46 per cent had information from housing officers. Even where the data were shared, they were often presented in a form that made risk analysis impossible.

http://www.audit-commission.gov.uk/Products/NATIONAL-REPORT/A51CB5E1-B7F8-46a1-AF8D-12EDFA3DED8F/neighbourhood_crime_PF.pdf

National Study – Better Safe than Sorry

This study found that decision makers were unclear about what data were available and which organisations held them. Data were held and collected by several local agencies including the NHS, the police and local councils that resulted in duplication of effort. Agencies perceived that partners were unwilling to share data, even where it could be anonymised. Consequently, agencies held data in isolation, making it more difficult to create targeted, effective strategies to prevent unintentional injury across a local area.

<http://www.audit-commission.gov.uk/Products/NATIONAL-REPORT/B0354AA7-E411-45f0-8227-B5FDA6EB35A1/Bettersafethansorry.pdf>

Question 8. Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.

Please describe the information-sharing concerned and why you believe it should not be taking place, including the risks involved in such information-sharing.

Comments:

No comment

Section 3: The legal framework

Question 9. In your view, how well does the 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.

Comments:

One of the key strengths of the DPA is that it protects the privacy of individuals, whilst also recognising that there are legitimate circumstances where personal data may, and should, be shared. However, the DPA can be often either misunderstood or misused, which can prevent the effective sharing of information where appropriate. This may be due to the fact

that the DPA is a relatively detailed and technical piece of legislation that at times is difficult for lawyers to interpret, let alone for members of the public to understand. If possible, we would propose simplifying the DPA so it is more accessible and easy to understand.

Question 10. In your view, how well do public authorities and private organisations adhere to the second principle of the DPA? How valuable do you believe the second principle is? Please provide examples and the reasoning behind your response.

Comments:

No comment

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

Comments:

No comment

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

Comments:

No comment

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

Comments:

No comment

Question 14. Are there any statutory powers unavailable that would enable better and more secure sharing of personal information– for example for identity authentication purposes – between a) public authorities and b) public authorities and private organisations? If so, what are they?

Please provide examples and any steps you believe could be taken to improve matters.

Comments:

No comment

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.

Comments:

No comment

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 about the form that consent should take? Please provide examples.

Please provide details of any initiative you have been involved in that has been based on consent.

Comments:

No comment

Question 17 What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.

Comments:

No comment

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

For example, should individuals be given strengthened access rights? And if so, how? Should organisations be expected to do more to explain their use and sharing of personal information to the public? And if so, how?

Comments:

No comment

Question 19. How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?

For example:

In your view, how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information (http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf)?

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December (www.ico.gov.uk)?

Comments:

The Commission believes that new guidance will prove a helpful standard as it will assist the process to get multiple agencies to agree to one way of documenting the principles around data sharing.

The privacy impact assessments statement says 'organisations must consider the impact on individuals' privacy before developing new IT systems or changing the way they handle personal information'. It is important for the data protection requirements of any new system or process to be looked at during the initial stages of a new project. This would comply with the requirements of the data protection act and help ensure an organisation has covered every aspect of the DPA, which would focus on accountability rather than IT restrictions.

Section 5: Technology

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

Comments:

The Commission believes that increased access to technology and the improvements around speed and dynamic interactions have resulted in an increase in individuals providing their data to a wide range of organisations. This can be seen in the in the private sector with social networking sites like Facebook, online ecommerce sites like Amazon and eBay, and the increased use of weblogs (or blogs).

It is difficult to provide technical measures that keep up with the rapid changes around security attacks to ensure protection of the data.

For example, in relation to the NFI, the application of new technology has enabled the Audit Commission to identify fraudulent transactions which have arisen, for example, from stolen identities. This is because we are able to securely collect, process and analyse information more rapidly and provide information for the relevant authority to investigate.

Question 21. Should the law mandate specific technical safeguards for protecting personal information?

For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?

Comments:

In our experience a risk based approach that requires organisations to manage the risk by using robust controls, i.e. the best available method, would be more appropriate. It is difficult to keep up-to-date with changes in technology and the ways in which security is compromised. Standards that negate any possible chance of breach would be out-of-date very rapidly. Other issues would be faced around the monitoring of changes to the legislation.

Encouraging technology suppliers to improve basic security on products will be one way of helping organisations meet the challenges around protecting personal data. However, the global nature of the technology market place will make it difficult to set a standard that fits across international boundaries.

This is not just a technical issue. Organisations should set a baseline for the minimal acceptable standard of how they approach the cultural aspects of information and data standards. The evidence from the Commission's surveys of ICT Fraud and Abuse and work at specific authorities using the Your Business @ Risk diagnostic confirms the importance of the cultural and behavioural aspects of information security if policies and procedures are to be adhered to.

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?

Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

Comments:

Anonymisation and pseudonymisation of personal data are often not understood by the end user who is trying to distinguish them, and they may have a lack of trust in the end result, in other words, whether it is truly anonymised.

Section 6: International comparisons

Question 23. Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Please provide examples.

Comments:

No comment

Question 24. Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

Comments:

No comment

Question 25. Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?

Comments:

No comment

Question 26. Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

Comments:

No comment

Section 7: Additional questions

Question 27. Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering?

Do any of these issues apply specifically to your sector?

Comments:

No comment

Question 28. Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

Comments:

No comment

