

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: As an NHS organisation information sharing with partner agencies is vital to the provision of co-ordinated and seamless health and social care services. It extends to all types of information sharing relevant to the provision of both adult and children's health and social care services in both multi-agency and multi-disciplinary service provision

The kinds of personal information we collect, hold and share are:

a) patient information viz

patient's name; address; full post code; contact telephone number; date of birth; community health index number; details of home doctor; clinical information re medical condition and treatments; religion; ethnicity; nationality; next-of-kin.

b) staff information (including those who are seconded to agencies) viz full name; address; full post code; date of birth; sex; contact telephone number; job title; grade; work permit status; qualifications; ethnicity, disabilities, criminal convictions and nationality.

The information is collected during face to face interviews in electronic format or manual submission of forms. The information is held securely within the computer system, or, if held manually, in secure locations or secure filing cabinets. The information is shared internally on a "need to know" basis or with external agencies through information sharing protocols. All staff have a duty of confidentiality for personal/patient identifiable information.

The purpose for the collection, holding and sharing personal/patient identifiable information is for employment, healthcare, social work, education, housing and research purposes.

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? Please provide examples.

Comments: The key benefits to

a) individuals are:

to assist the management teams in the partner agencies with planning and management information; to improve the quality of services for the individual ; to support a single point of access for the individual; to enhance the robustness and effectiveness of systems to protect the individual from harm; and to satisfy the legitimate expectations of the individual.

b) society are:

to support national initiatives on multi-agency working and information exchange; to support joint care planning and commissioning; to support statutory reporting functions and effective use of resources; to provide professionals with the information they need to deliver integrated services; to produce consistent services and information.

Examples are; common assessment frameworks for children and vulnerable adult protection, single shared assessment, as well as carrying out benefit assessment work integrated with financial assessments of contributions for community care.

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 key risks to

a) individuals are:

information security issues; abuse of access permissions and individual's confidentiality requirements; technology failures.

b) society are:

more parties mean more contracts which leads to greater risk; organisational structure and working practices; information being collected unnecessarily or used inappropriately; accuracy and security of information; poor document integrity processes; lack of understanding within organisations of how document integrity can be compromised; hacking and security storage; ownership identification; loss of faith in service leading to mistrust.

Examples are the loss of healthcare information contained on laptop computers which are stolen and H M Revenue and Customs recent loss of 25 million records.

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: The biggest risks are legislation and Government attitude, the intrusion into personal privacy, the accuracy of the data collected and the sharing of information collected for one stated purpose and then sharing it with other organisations/agencies for it to be used for entirely different purposes. e.g. within a Healthcare environment, the 'Single Shared Assessment' for Community Care Needs - Local Authorities have knowingly used information collected for Health Care needs for other assessments in breach of the 'fair processing' rules. The amount of information collected and the number of agencies involved (e.g. Healthcare, Housing Support, Drug Support, Social Work, Community Care Groups etc), and the lack of single point responsibility make it almost impossible to control.

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: You are referred to Question 4 above.
In this example, information is collected once to serve a number of purposes. The risk is that individual partner agencies who have access to the information will, over time, use it for their own purpose(s) and not for the purpose(s) for which it was originally collected. The risk is also that too many people will get access to more information than they need to. With so many different agencies involved for so many purposes, there is a higher risk to information quality (not being accurate and up to date) and of security breaches. In other words, out of proper control and very difficult for retrospective control measures to be introduced.

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: Banking organisations are an example of a business sector that holds too much personal information.

For example, if you wish to open a bank account, why the need to give details of marital status, number of dependant children, employment status and gender etc. Banks invariably do not state 'up front' why they need this information and thus are in breach of the 'fair processing code' under the DPA.

If you wish to apply for a bank loan, they may wish to know some of these details. The information should therefore only be collected at that time, and the Bank should state why they need it.

Also, commercial businesses hold too much information for marketing to or profiling of their customers

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: No comment offered.
Already feel information use is out of control.

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: Within the NHS Patient Identifiable Information includes the CHI (Community Health Index) number. This contains the patient's date of birth, a number to indicate their sex and a personal identifier.

The official guidance issued by NHS Scotland on the use of CHI states the CHI number is an administrative identifier created and owned by the Secretary of State to enable the reliable linkage of healthcare records held by health service bodies. It should not be shared with agencies outside the NHS unless both bodies are working together to deliver a joint health service and the patient has been informed and has consented.

The CHI number was given to Local Authorities by NHS Scotland for inclusion on Citizen Entitlement Cards ((which can be used as a free bus pass) which are issued by the Local Authority), without the individuals having been informed or their consent sought. This is contrary to the official guidance.

The risk is this information can be used not for purely health purposes, or, it can be a misuse of purposes for which it was gathered. Also, along with other information, it can be used for identity theft.

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: With the development of technology a vast amount of personal information can easily be amassed about our personal lives from our day to day activities. The opportunities for the abuse of this information across all business sectors are immense and indeed it has rapidly established itself into a multi-billion pound industry. The DPA works reasonably well in trying to control the use of this information, but its powers are limited.

Its main strengths are:

- it serves to protect us from our personal information being treated, used or applied in a harmful manner and in breach of the basic human right of privacy
- It provides us with a clear framework on how personal data may be treated and used
- It gives the data subject greater control over how his or her personal information is gathered, used, housed and shared
- It provides the data subject with a number of rights and remedies

Its main weakness is that the Information Commissioner has been granted only limited powers to take action against organisations for breaches of the Act and therefore it is perceived as being weak in real terms.

Until the Information Commissioner is given similar rights as, for example, the FSA (who recently fined Norwich Union Life £1.26m for exposing its customers to the risk of fraud) the Act will continue to be flouted by business organisations and only lip service paid to it by senior management.

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: By in large public authorities do not adhere to the second principle of the DPA.

In theory, the second principle is valuable in that it forces organisations at the outset to define in general terms what they are collecting the information for; to whom they will be disclosing the information and the purpose for the disclosure. A judgement/check can then be made comparing what the information is to be used for with the purpose for which it was collected. The second principle therefore goes to the heart of Data Protection. When linked with the first principle, it should give the individual control thus protecting them from the wholesale use of their data for any purpose.

Invariably, over time, within large organisations the original purpose for which the information was originally collected is forgotten about.

An example is within the NHS where patient information is collected for research purposes and then used for remote teaching.

Question 11. What technical, institutional or societal barriers stand in the way of the

effectiveness of the DPA? Please provide examples.

Comments: Societal barriers to the effectiveness of the Act are the limited powers granted to the Information Commissioner.

Question 9 refers

Also, within large organisations there is little or no control in the use of information.

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

Comments: At present, the Information Commissioner can only carry out information audits within businesses by invitation. The Information Commissioner should have the power to enter business premises to carry out information audits following a complaint or as he sees fit and legally enforce measures for non-compliance.

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: Local Government Acts stipulate wide ranging 'duty to share' with other organisations with no constraints. This has been used by some to justify any form of uncontrolled sharing.

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: Some sort of 'Information Sharing Act' which would stipulate boundaries would enable better and more secure sharing of personal information. This would be better than the present situation which relies on individual interpretations of the Data Protection Act when sharing information across organisations.

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: See question 14

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: In a healthcare environment the guidance issued by the Information Commissioner titled "Use and disclosure of health data" is most helpful. This document makes it clear when explicit consent is required to share information e.g. for teaching and research purposes.

In other environments it is not clear when explicit consent is required and so the view is that to prevent any ambiguity, explicit consent to share information should always be required. Implied consent is invariably misused to suit the organisation's purposes.

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

Comments: There is no barrier to the sharing of information without consent in the "vital interest" of the individual.

In all other instances, gaining consent is an inconvenience for business. However, it is essential, in our view, if information is to be processed fairly, and to demonstrate there is choice. If there is no choice there can be no valid consent.

If consent is not obtained at the outset, the main barrier is the logistics of retrospectively having to contact individuals to get consent. Thus, it will force businesses into thinking what information flows are necessary and get consent at the outset.

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: In order to gain the trust of the public, organisations should be expected to do more to explain their use and sharing of personal information to the public by way of fair processing notices. Organisations should consider at the outset the best method of communicating to the data subject in an understandable form what the information is to be used for.

The Information Commissioner should be able to award individuals compensation for the wrongful use of their personal information by organisations without the individual having to pursue a claim for compensation through the courts.

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 Information Commissioner's recently published Framework code of practice for sharing personal information is a valuable tool. It provides the comprehensive clear framework necessary when information sharing is required. If properly adhered to, it will go a long way in maintaining public trust in respecting personal privacy. By following the code, organisations will have confidence that they are being transparent and properly accountable when they need to share information with other organisations.

This organisation has yet to undertake a privacy impact assessment as outlined in the document, but the concept is supported.

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: In our view legislation will always lag behind technological advances and never be in a position to catch up. Whilst there have been major improvements by its use, it has also opened up greater potential for misuse and wrongful disclosures.

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: It is our view the law should mandate specific technical safeguards for protecting personal information and there should be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard.

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: There is a strong public interest in maintaining confidentiality so that individuals will be encouraged to seek appropriate treatment and share their

information for research. Holding records electronically increases the ease with which data can be anonymised or pseudonymised. Anonymisation and pseudonymisation techniques can go a long way towards protecting privacy and preventing the casual identification of individuals by those legitimately using the records. Some research relies on records which include information from which individuals can be identified e.g. unusual occupation or disease and pseudonymisation of records can assist with this.

General advice about the deployment of such techniques is available; whether it is sufficient remains to be tested and it is unlikely to cover all circumstances e.g. while digital imaging can distort features, distinguishing features such as tattoos, body piercings, posture and gait may still be capable of identifying an individual to others. For this reason, there should be nationally agreed anonymisation standards.

This organisation is confident about using anonymising techniques.

Barriers to using them are both cost and time related and in the case of pseudonymisation the further linking of the information to the anonymised record. Non-clinical staff involved in the anonymisation process will require access to confidential patient-identifying data for reconciliation purposes. There is a risk that this could be challenged as a breach of confidence under common law.

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: Not aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context.

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 examples can be offered.

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 knowledge of other jurisdictions.

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: Not aware of significant differences in public attitudes to the sharing of personal information in other countries.

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: Within a healthcare environment, it is hard to see that massive patient databases, which can be accessed by thousands, would actually be beneficial for the patient – more for the benefit of the Health Department administration process.

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

Comments: No other suggestions

