

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.

Comments: Within any local authority role, the primary concern is that data should be used for the right purpose, controlled and adequately risk assessed

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

Question 2.

Comments: (a) to benefit the individual and (b) contribute to crime prevention

Question 3.

Comments: (a) release of information to inappropriate individuals, and,
(b) subsequent use or unknown use or security of the data

Question 4.

Comments: Control of the data gathered, as it could be used for system testing or even sold on for profit

Question 5.

Comments: The storage of data in various medium beyond its useful retention date

Question 6.

Comments: Data used for direct and indirect marketing purposes

Question 7.

Comments:

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments: The DPA works well and adequately if implemented properly

Question 10.

Comments: This is an area that could be improved. The Second Principle is very important since it is a persons personal data and it should be used in a way at least protects the individual

Question 11.

Comments: The costs associated with ISO 27001 and implementation of PCI DSS

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments: Implementation of secure email for exchanging personal data

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments: The clarity is not always readily identifiable. The form of consent should be in writing, especially for minors or disabled persons

Question 17.

Comments: SEN subjects - clarity by the requester should be stated

Question 18.

Comments: It should not be made more transparent. It is the data subject's information and should not therefore be used by third parties at their will

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments: The advances in technology are available to utilise, however, the uptake by Local Authorities is questionable due to costs. It can be particularly simple to share information but protection can be extremely poor, especially given the multiplicity of records held by an organisation across its services/systems instead of a single customer record.

The downside to this is the misuse or loss of media. It would have been impossible for the HMRC to lose 100 x 4 drawer filing cabinets, whereas the equivalent volume of data on CD's can simply vanish. In theory, technological advances should have helped personal data to be shared more securely. A good current example would be the ability to move encrypted data over a high bandwidth secure network connection rather than having to copy it on to CDs and send them by post.

Even with the latest technology in place, people have to know how to use it and have to have the correct processes in place to enable / enforce them to use it. At Sunderland, we have access to a data vault product (Cyber Ark) which allows data to be shared securely over the web between us and our partners, who may be public sector organisations such as the police, or private suppliers. Such transfer of data is about to be trialled between the NHS and Sunderland Register Office for sharing birth and death information which is currently transferred by courier service.

Question 21.

Comments: Yes. The law needs to be improved with mandating for protecting ALL data, more especially for the data that is held on portable devices or is being transferred electronically. However, good or improved legislation will never rule out negligence and active misuse. There should be guidance / advice and penalties for obvious negligence. Establishing particular standards may be useful but difficult to keep up to date. For example if the law were to mandate a particular standard and technology moved on, would the law have to change to reflect this?

Question 22.

Comments: These techniques have been used by the IT Department in Sunderland for some years. An example is for testing new systems with 'live' data. However it is quite complicated adds time and cost to a project. The problem arises when it is the personal data which is the point of the testing, for example where you might be looking for members of the same family (whose surnames would be the same on the actual data but different on the anonymised data).

Section 6: International comparisons

Question 23.

Comments: Safe harbour in the USA, though this is not a key factor since the USA are more interested in Freedom of Information

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments: