

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: My interest is as a potential victim of over-government and bad policy making. A 'consumer' of government as it were.

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

Question 2.

Comments: There is obviously apparent benefit to government. To individuals it is much less obvious. Do the risks to personal liberty out-weigh the benefits to society? I believe so. The collection and collation of data of such fine detail would allow a functioning police state to evolve. What the STASI in East Germany tried to do, the ID, NHS, HMRC etc databases would allow to occur.

Question 3.

Comments: Key risk: progressive evolution of a repressive State with continued erosion of individual freedom of choice.

Question 4.

Comments: Having data on electronic form makes it easy to copy and abuse. In paper

form, ironically, it is much more secure. The recent data loss incidents are more cock up than conspiracy; imagine what a real criminal conspiracy would do. If a clerk can copy without oversight all the data held on half the people in the country, imagine what is possible with a targetted theft programme.

Question 5.

Comments: All children in the country on a database by default - risks to identity theft and credit rating etc. Police DNA database & refusal to remove people there who are innocent (DNA taken for process of elimination of victims of crime...). Medical records shared to readily....

Question 6.

Comments: Store loyalty cards. Any information beyond name & address to fulfill orders.

Question 7.

Comments: I have no comment.

Question 8.

Comments: The objection is one of principle: the more the information is shared the greater the potential of data loss (into the public domain). The greater the State oversight, the greater the risk of encroaching loss of freedom with no recourse to justice.

Section 3: The legal framework

Question 9.

Comments: The State will over-ride the DPA whenever it chooses. Unless the DPA has equal standing to the judiciary then it will remain effectively powerless and subservient.

Question 10.

Comments: It is a form to fill in; otherwise it is not taken seriously.

Question 11.

Comments: Lack of ability to enforce anything strongly.

Question 12.

Comments: Unlimited fines and ability to close organisations that abuse their position.

Question 13.

Comments: No comment.

Question 14.

Comments: Do not use computer data for ID authentication. Go back to the old system of an accredited professional doing this. Computers can and do make mistakes and these seem to be oncredibly difficult to unwind.

Question 15.

Comments: Unreasonable burdens will be ignored routinely - people get on with the job as best they can.

Section 4: Consent and transparency

Question 16.

Comments: Any data sharing should take place only with the informed consent of the person involved.

Question 17.

Comments: The presumption should be that data sharing is the exception rather than the rule. Explicit barriers should be in place; to make data sharing routine and easy is open to abuse.

Question 18.

Comments: An individual should have absolute right of access to all and any data held about them by any organisation and a presumptive right of correction of that data should any error be found. Any sharing of information should be pro-actively sent to the individual concerned.

Question 19.

Comments: Irrelevant to the great majority of people.

Section 5: Technology

Question 20.

Comments: Database technology has made gathering and processing of data on individuals enormously easier; with the increased volume of data the risk of loss of confidentiality has risen exponentially. It does not seem to have increased effectiveness particularly of State agencies.

Question 21.

Comments: Portable devices is missing the point. If data is not held securely on the master ,machine, then it can be stolen easily enough by a sufficiently motivated person.

Question 22.

Comments: This already happens with properly conducted medical trials. The risk of ID theft from medical trials is not a high risk factor. The problem is where there is a specific need for ID linked across many organisations and applications.

Section 6: International comparisons

Question 23.

Comments: No

Question 24.

Comments: No

Question 25.

Comments: China. Loss of personal liberty.

Question 26.

Comments: China. Fear of persecution by State bodies.

Section 7: Additional questions

Question 27.

Comments: Why is it necessary that all children in the UK have a tracking number (except those of politicians of course).

Question 28.

Comments: Take a precautionary principle. Assume that function creep will happen. Avoid giving the State oversight. Make data capture and use as important as the judiciary in the functioning of the State. Avoid progressive erosion of freedom in the name of "If you've got nothing to hide, you've got nothing to fear".