

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: I have worked numerous jobs within the NHS which dealt with sensitive patient information, which included the address and detailed medical information. The information is held both on paper, as well as on a computer system (Cerner Millenium) that is now being created to cover the entire country.

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

Question 2.

Comments: Done properly, and with strict controls, it can benefit a person in cases where the participation of multiple agencies are needed to resolve a situation (i.e., over child custody). With regards to society, the case made is far less clear.

Question 3.

Comments: A major risk to both persons and society is lax data security, as evidenced by the recent flood of cases to do with both military and civilian information. Such inability to properly guard such vital personal details of soldiers and benefits recipients does nothing to enhance the government's case for a more comprehensive single system. Secondly, the supposition that the gathered or

shared information will only ever be used for benign purposes is a serious risk; it is based on a premise that simply cannot be substantiated, and in these febrile times, is likely to be proved very wrong.

Question 4.

Comments: The wholesale sharing of large amounts of personal details is a very risky practice, as it depends on every 'link' the the 'chain' being scrupulously honest at all times - a situation that cannot be guaranteed absolutely. A system where the information needed to resolve a single case (and only this information) is shared between two agencies and then only kept by the original possessor would engender more public trust.

Question 5.

Comments: At the moment, the National Identity Register and DNA Database are prime examples of the government holding far too much data on its citizens. The DNA database is a particularly pertinent example, as it now holds details of thousands of people that have never comitted a crime. This gives the impression that the government desires to criminalise its population, or else exert greater control for some nebulous reason.

Question 6.

Comments: Databases involved with 'customer loyalty' cards are prime examples of private corporations holding too much personal data. They may very well help said company (to a certain extent) to suit the customers' needs, but they are far too open to abuse, especially as they are not owned by an entity that is required to deal with said information (i.e., its sharing) in a manner that complies with governmental standards of data sharing.

Question 7.

Comments:

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments:

Question 10.

Comments:

Question 11.

Comments: A major societal barrier is the inability to properly practice discretion with regards to personal information. I have often observed hospital workers ask patients to verbally confirm details, even though the workers have been instructed not to do so. This inability appears to stem from a belief that following the guidelines as stated is somehow 'inconvenient', and that shortcuts are needed in order to 'speed things up'.

Question 12.

Comments: A further safeguard would be greater education, linked with harsher

punishments if the guidelines of the Act are not followed Further, less pressure to achieve targets (in the case of the NHS) is crucial, in order to give those workers that deal with sensitive information the time needed to deal with things in the proper manner.

Question 13.

Comments:

Question 14.

Comments: There are two powers that are crucial to public trust in interagency information sharing; a strict use policy, and a strict enforcement of that policy. The public must be assured, beyond reasonable doubt, that the information held by its government is both secure, and not being used in ways and by individuals that do not have the public good as their prime motivation. The practice, in particular, of 'fishing expeditions', cannot be condoned or allowed. In an emergency situation (the definition of which must be stringently defined), allowing a person's information to be concentrated is acceptable, but such a practice cannot be allowed to become commonplace.

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments: In my positions within the NHS, the concept of information security, and how it applied to me, were very clearly spelt out - I was left in no doubt as to what information I could divulge by which means and to which persons, as well as what 'consent' in each situation meant.

Question 17.

Comments:

Question 18.

Comments: Individuals should be given stronger access rights; the definition of 'consent' should be made more explicit, and individuals made a larger part of the process, by having agencies that require information from other agencies either ask permission of the person, or notify them of their intent to request such information and give the person a certain amount of time to give their permission for the data to be shared. This second method could be adapted for the explanation of data use; the organisation would notify the person of their intent to request or use personal data, and in that communication explain fully the need for and method of data-sharing, and give the person affected a suitable length of time to give their permission - after which, and after a second communication and further waiting period, it would be supposed that the person had given permission, and the data would be shared.

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments: The major impacts of technological, not to mention ideological, advances, have been that there is too much information held, in too few and obviously sign-posted sources (i.e., the DNA database, the National Identity Register, Cerner Millenium, the NHS 'Spine' system). Such a concentration of data in so few places makes it far more vulnerable to loss, theft, or abuse, as recent cases have shown.

Question 21.

Comments: The law should certainly mandate specific technical safeguards for data protection; technology may change, but a set of 'rolling' safeguards, made to deal with security and its application to newer forms of data storage and sharing, including the present forms, would create a greater sense of trust within the public. A mandated standard of encryption on all storage devices, handheld or stationary, should be advocated and instituted as a matter of course.

Question 22.

Comments: 'Privacy enhancing techniques' would be a welcome addition to data security and personal privacy. Certain information is crucial to medical studies, but it must be used with the certainty that the patient from whom it comes is assured that only the most pertinent details are being used, and not more personal ones open to abuse. Sufficient information about the deployment of said techniques is not properly available, and I would not have sufficient confidence about using them if I were called upon to do so presently. The barriers to using them are, at present, centred around insufficient education and information about them.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments: With regards to the NHS, information-sharing issues that have not been previously raised by this questionnaire are of the lack of speed to adopt new information systems (i.e. Cerner Millenium), said new systems' inefficiency,

and the effects that these problems have been having on the public. In general terms, the review should thoroughly consider the public's right to privacy (even in the face of 'terrorist threats'); the current government's record with both computer data security, and the creation, adoption and maintenance of computer systems, specifically the lack of speed and inefficiency in adoption; and the current government culture of over-legislation and 'headline-grabbing', which has done little but create confusion and ill-thought-out 'solutions' to a wide variety of problems. (i.e. ID cards)

Question 28.

Comments: The ID card system, along with the National Identity Register, should be removed. If a system can be proposed that can be implemented quickly, and within the original budget stated, then the matter can be revisited. If a system cannot be found that satisfies these criteria, greater resources should be put into current policing efforts. A major step in that direction would be the augmentation of the 'Border Police', giving them proper policing powers to allow them to give Britain greater security, without having to criminalise, even merely by implication, the general, law-abiding public.