

# 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](mailto: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 am one of the officers involved with monitoring and advising on Data Protection issues within West Berkshire Council. I also advise on data sharing and have recently taken over a small data sharing group which is looking at advice and guidance for social care staff around what data sharing is legal and appropriate.

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

Question 2.

Comments: For a local authority, benefits lie in being able to work seamlessly with other organisations and agencies to offer joined up support for clients – for example, sharing data with the local hospital so that vulnerable clients returning from hospital stays have support from the social care staff. Barriers are the misunderstandings around what can be shared and where.

Question 3.

Comments: The main risks lie in inappropriate data sharing, or sharing too much data, or providing data in a way which is not technologically secure for example a fax

sent to the wrong address, or an 'all-users' email which contains sensitive information. It is more difficult to quantify this as a risk to society but the current concerns over 'surveillance society' issues indicates the ways in which society can pick up on an issue and the way in which distrust is generated as a result.

Question 4.

Comments: Greatest risks are posed by the unthinking sharing of data in technological ways – the automatic email or fax which may be inappropriate. However it is my experience that staff generally err on the side of caution, and that some opportunities may be missed where positive results could be gained, by staff feeling they are unable to share personal data. High profile examples would be recent cases where child abuse was not stopped because different services had concerns over what could or could not be shared. An example of this sort of misunderstanding (on a smaller scale) is a current debate being carried on between several authorities who want a shared library database so users can borrow books in several authorities, not just one. It's being stalled by two authorities who believe that they will need specific permissions to share user data (name and address only) in order to issue books. If simple initiatives like this fail because the nature of data sharing is misunderstood I would expect a much larger impact for more sensitive data.

Question 5.

Comments: I suspect that because authorities have, over time, built up parallel databases which duplicate certain personal data (name address etc) they probably hold a lot of duplicate data which could be amalgamated within wider CRM systems. There is also an inclination to retain data even when its 'best before' date has passed, particularly older records from the 1990's which may have been archived before proper and effective records management systems were in place.

Question 6.

Comments: I don't work within a private sector organisation, but it is noticeable that these tend (particularly for marketing) to collect a great deal of data the use of which is questionable. I tend to steer clear of online or hard copy forms which expect you to fill in masses of detail but believe these may be very confusing and possibly unsafe for vulnerable people.

Question 7.

Comments:

Question 8.

Comments:

### **Section 3: The legal framework**

Question 9.

Comments: I believe that the DPA works well, but that it is in general misunderstood by the layman. I think the Principles are a strength of the Act in that they are a very useful checklist which can be explained easily to staff (or the public). From reading through and dissecting the Act (for my ISEB certificate) I do have to say that the majority is very inaccessible to Joe Public and that even staff

familiar with the general conditions of the Act can misinterpret what it enables them to do. I also feel that the deceased persons loophole (plugged so effectively by the Scottish Freedom of Information Act Section 38 (1) (d) ) needs to be addressed – either in DP or FoI – as this is an area which causes a lot of confusion. I don't know what could be done about the title of the Act but the fact that we get requests for personal data from data subjects made under Freedom of Information suggests that most people don't realise that the Data Protection Act gives them rights of access as well as protecting their personal data.

Question 10.

Comments: I would consider that public authorities probably adhere rather better to this than private sector ones, but in any organisation, unless the Act is properly understood, there will be a tendency amongst staff to presume that personal data which the organisation holds can be used in new ways if these are suggested. Public authorities probably manage this sort of tendency better because they will (and ought to) have officers with the legal understanding to point out the pitfalls. Private sector organisations rarely do, particularly if they are small, and can fall into error unknowingly.

Question 11.

Comments: I am best placed to comment on societal barriers, and here understanding of the Act by society in general seems to be poor or to have been influenced by lurid tabloid stories. There can be serious impacts on trust in organisations and authorities as a result. An excellent example occurred just before the Freedom of Information Act came in when one local authority was castigated in the local press for destroying people's personal records before the Freedom of Information Act gave them access to the information. It's hard to know how to respond when the press gets it so completely wrong. However, there is also an institutional tendency to blame Data Protection ("we can't do this because of Data Protection") which is difficult to overturn and tends to add to the myths around the Act. As the example about the library loans system shows, this can be a big issue to joined up working.

Question 12.

Comments: Provisions for deceased person's health records – either in DP or FoI. Stronger powers for the Information Commissioner to enable him to properly regulate use of personal data. A fee structure which more reasonably reflects the actual cost of a data protection request (I know this isn't likely but the difference between the charge which can be made and the actual cost is astronomical – our most expensive subject access request cost £1,950 – at least if we could charge for photocopies it would help). A clause to recognise repeated or vexatious requests as with Freedom of Information (as for example when we received a request from a member of the public for every email, memo or other document which mentioned his name because he thought the staff had been talking about him).

Question 13.

Comments: I'm not an expert on this but I think in general people are less aware that there is other legislation - RIPA, S47 of the Children's Act, S115 of the Crime & Disorder Act, S119 of the Learning & Skills Act, as examples - which provide

for data exchanges between named organisations for specific purposes. This would impact more positively on data sharing if people were aware of them and their uses.

Question 14.

Comments: I can't give a comment on this as I don't have expertise in this area – although from a personal standpoint I suspect ID cards won't make personal data any more safe than it already is.

Question 15.

Comments: The fees structure, as mentioned before, is unrealistic in terms of the actual workload involved. A lot of our requests are for social care records, often old, archived material from twenty or more years ago, and the workload involved in separating out the actual data from what has been retained is enormous. Requests for 'all my records' are also very time consuming. While a rise in the access fee is probably not fair on requesters, some charge for copies of records might encourage them to limit their request to data which they actually need.

The timescale of 40 days for providing the records is fine for small requests but often impossible to attain where the request is for ten or twenty years of material (old records are a case in point). An extension of time to enable complex or voluminous requests to be provided would be sensible, and a change to working days would be helpful in bringing the legislation in line with the provisions in Freedom of Information, the Environmental Information Regulations, the re-use of Public Sector Information Regulations, and the Education (Pupil Information) (England) Regulations. If the timescale was in working days it would be reasonable to suggest 30 working days (equates to 42 days) or an extension to 40 working days (equates to 56 days) for complex requests.

#### **Section 4: Consent and transparency**

Question 16.

Comments: I am usually clear on consent requirements but I understand the Act. Other staff may not be. There have been particular concerns for staff working with mental health clients where data sharing is required, or where they also need to discuss a clients needs with an agent on their behalf. I suspect that the Mental Capacity Act has added to concerns over what is appropriate to share.

Question 17.

Comments: Where consent is refused or not given, staff may be concerned that they cannot take needful action to safeguard a client's well being – for example, sharing sensitive personal data about a mental health client which will ensure they receive appropriate treatment.

Question 18.

Comments: I think more could be done to stop sharing of data being demonised in the press. Some basic explanations of what sorts of data are regularly shared and why might stop this being regarded as another example of the surveillance society or Big Brother. Information about data sharing on public authority

websites could help. Promoting people's access rights and explaining how they can use them might also be a good thing. As I noted before, because the Act is the Data Protection Act, the access provisions tend to get a bit submerged in the public consciousness.

Question 19.

Comments: I find all the IC publications very useful, although I hadn't looked at the framework Code of Practice in any detail until now. My concern would be that if data sharing becomes a major issue, with a lot of guidance and regulation produced it will discourage people and there will be a culture of 'oh we can't do that' which won't be beneficial.

### **Section 5: Technology**

Question 20.

Comments: It's become extremely easy to share data, particularly by email or on the internet, without people really thinking through the safeguards they need. Facebook and similar websites are a particular case in point. An example would be the scam 'bank' emails which encourage you to provide financial data which can be used to access accounts. Identity fraud is another area where the amount of personal data out on the internet has led to a rise in criminal activity. From an organisational point of view, the tendency to accidentally send an all users email containing sensitive data, or to send an email to the wrong person has sprung directly from the regular use of email as a communication tool, and the fact that people don't treat it with the same attitude as they would a more formal process such as a memo or letter. It makes it much more difficult to ensure data is safe and that everyone is taking the correct precautions to safeguard what they do.

Question 21.

Comments: No. Technology moves so quickly that by the time any such provision became law the technology would be obsolete or out of date. Guidance on technology is more use as this can be updated easily and quickly. Mandatory standards would be expensive for small organisations to work to as well, so the less scrupulous would probably ignore them.

Question 22.

Comments:

### **Section 6: International comparisons**

Question 23.

Comments: Scottish law – FoI Act (Scotland) where consideration is made for deceased person's health records. I know this isn't personal information under S1 of the Act but it's an anomaly in our existing legislation because no one knows where it sits.

Question 24.

Comments:

Question 25.
--------------

Comments:
-----------

Question 26.
--------------

Comments:
-----------

**Section 7: Additional questions**

Question 27.
--------------

Comments:
-----------

Question 28.
--------------

Comments:
-----------