

# 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 the nominated data protection officer within my organisation but am also regarded as a useful source of information on FOISA even though that is not my role.

As a part of the NHS Scotland we capture and share the full range of personal and sensitive data of staff for employment purposes as well as collecting personal and sensitive health related data on patients. We may also share patient information (both personal and health information) with other agencies particularly if the patient is at risk of further harm.

Information is collected via phone, facsimile, in writing and personally then directly inputted into computers or onto a paper medium. The information may be held on individual computers, hard drive storage devices, CD-ROM discs, Audio tapes, CCTV tapes, web based data warehouses and "flash " storage devices.

Personal Information is only ever shared in compliance with the DPA or where it is required under other statute or justified in the vital interests of the data subject.

Information is collected for a wide range of purposes including, Staff administration, Health Administration, Accounts and Records, Research, Public Health, Crime Prevention, Education and training, Advertising/Marketing and public relations.

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

Question 2.

Comments: Sharing information within a care setting is beneficial to a) individuals; as in times of crisis there is nothing worse than the individual having to answer the same questions three or four times as they are passed from one agency to another. The single shared assessment is a good example of how to avoid this through a simple process.

to b) society: sharing information protects society in ways we cannot imagine particularly in relation to crime prevention and terrorism. It also allows for the provision of targeted healthcare services, prevention of disease, collection of taxes and not least the identification and protection of vulnerable adults and children.

Question 3.

Comments: The major risk to sharing information to both Individuals and Society has been recently highlighted by the recent loss of 25 million records by the CSA leaving the entire population of parents within the UK vulnerable to identity theft and any other devious practices. For me that sums up the real risk as I am sure it will happen again.

On a smaller scale there is always the risk of breaches of confidentiality, non compliance with the DPA on an individual or organisational level, poor contractual monitoring of data processors allowing for illegal processing, ignorance of the DPA, poor training and awareness within the organisational context and the exporting of data processing functions to countries that do not have the same data protection standards as the EEU/UK.

Question 4.

Comments: As an emergency service (Ambulance) our scope for sharing information is generally restricted to other health services (continuation of emergency care), the social services (vulnerable adults and children), local authorities (ASBO's etc) Police/Procurators Fiscal (Prevention/detection of crime etc) Media (only for "public interest" events )

The opportunity to share information is I think essentially a positive one as it allows for us as an emergency service to pass on information about an at risk individual directly to the appropriate agency rather than simply make it the local Accident and Emergency' Department's problem e.g. Mental health issues. In this way targeted support for the individual can be much faster.

The risks to sharing information in our environment is very low and should always be viewed in the context of an emergency situation in which the information obtained may not always be accurate or complete.

I don't think any one method of sharing information poses a greater risk than another as it is not the method that is the problem - it is people who do not abide by laid down procedures that inevitably causes the failures.

#### Question 5.

Comments: Starting with Local authorities, I do not believe they hold too much information as they have to provide an enormous range of public services to a given population. It is my experience that they are generally very good at obtaining only the information they need to provide a specific service. An example of this is where I recently applied for an improvement grant. While the information they required was essentially of a financial nature I did not consider the application intrusive.

Public authorities like the DHSS are another matter. Appreciating the fact that they need to be aware of fraudulent claims their application forms are a complete nightmare. I recently assisted a friend to complete one and not content with asking the usual personal data questions they venture into the realms of deeply personal and sensitive information. The application form for disability living allowance for example asks questions relating to how many times a night the applicant needs to get out of bed, how many seizures they have and when they have them, do they wash/bathe themselves or does someone do it for them, can they control their bowels etc, etc. AND they then require the GP to confirm these facts. These questionnaires are far too intrusive.

#### Question 6.

Comments: Private sector organisations generally have, in my view, a vested interest in obtaining as much information about the individual as possible and are constantly pushing the boundaries of acceptability. I recently tried to purchase an electrical item over the internet. On completing my address details I was asked to respond to questions relating to my occupation, how much I earn and my email address. When I did not answer them I could not "check out" and pay for the item so I had a choice - give them the information and get the item or go elsewhere - I chose the latter.

Banks are another sector that collects far more information than is needed to safely run an account. Under the guise of money laundering regulations they demand passport details/driving licence details/utility bills of the parents - to open a bank account for a six month old baby! Then you are usually bombarded with junk mail from them.

#### Question 7.

Comments: The routine sharing of health information between the health service and social services should be permissible under the DPA rather than under the specific

DPA exemption of in the "vital interests" as it is often the case that following the initial emergency there is more information needed to implement a longer term care plan for the individual but under present law requires the express consent of the individual.

Question 8.

Comments: One area of information sharing that irritates me greatly is the National Fraud Initiative requirement that obliges my employer to provide Audit Scotland with all of my personal employment details (salary etc) and my personal details (name address etc) and my bank account details so they can cross check to see if I have defrauded the government somewhere. While I accept that my details should be shared IF I was suspected of fraudulent activity I greatly resent that my details are shared IN THE HOPE they will find some. Worse, is the fact the it was the ICO that approved this arrangement.

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

Question 9.

Comments: The DPA, on balance is working very well - where it is understood! It's strength is that in the main individuals are protected from the excesses of the private sector who otherwise would make life a misery through bombarding them with telephone calls and junk mail. One only has to look at the origin (USA) of the hundreds of spam emails I get every week to see what would happen in an unregulated environment.

Its weakness is that the DPA is, in enforcement terms, a toothless tiger and the penalties for clearly criminal activity (as opposed to breaches of the Act) need to be beefed up. (The loss of data relating to 25 million families is clearly an act of negligence - and should be a criminal offence resulting in at least the case going to a criminal court)

Question 10.

Comments: It is my experience that few organisations, private or public, clearly specify why they are collecting the data and what they are going to do with it. They may include this information on their forms but it is always in VERY small print and/or buried away in two pages of terms and conditions

The second principle of the DPA is vital to the protection afforded under the DPA - without P2 the DPA would be pointless as data processors could collect what they want for any spurious reason they deem fit.

Question 11.

Comments: There are no technical barriers that I can see to the effectiveness of the DPA. Society as a whole appears to want seamless public services but fail to understand that to do this many organisations need to collect and share information. An example of this is the Community Health Index (CHI) project where health services will have access to an emergency care summary (record) of every individual in Scotland. The general population does not

understand the concept or its advantages, the Health Service in Scotland is dragging its heels in getting the information out to the public and no one seems to know exactly who will have access to the database. In this regard the Scottish Health Service is clearly failing in its duty to inform.

Question 12.

Comments: There should be more criminal offences established under the DPA. One I would particularly like to see is Internet Service Providers being made legally responsible for filtering out spam email being sent from outside the UK along with a legally enforceable "unsubscribe" facility that means what it says and not be a route for even more spam.

I also believe strongly that the DPA should stipulate that the data subject will "opt out" of their data being used for any other purposes unless they specifically request to "opt in". At the moment many organisations bury their "opt outs" in privacy policies or as more often happens, do not mention how data will be used at all.

It would be helpful if the obligation to gain consent in the emergency setting is relaxed in that it is very often the case that information is unavailable (unconscious or incoherent patient) incorrect and/or misleading and often the "vital interests" (i.e. life and death scenario) cannot be applied

Question 13.

Comments: Not that I am aware of

Question 14.

Comments: If applied correctly, P7 is more than adequate for security purposes

Question 15.

Comments: In my area of operations the application of the DPA is no more a burden than say the application of the Health and Safety at Work Act.

**Section 4: Consent and transparency**

Question 16.

Comments: the DPA is clear enough about the issue of consent and when it should be obtained and the exemptions applied to this.

Question 17.

Comments: In the emergency setting it is not always possible to gain consent to share information and would like to see an exemption from consent in the pre-hospital care setting. While the "vital interest" exemption may apply in most cases it is not always appropriate to ask other non-emergency but nevertheless very poorly patients whether they consent or not

Question 18.

Comments: Every organisation should be legally compelled to provide each data subject

with a clear summary of what data is collected, why it is collected and what uses it will be put to. There should also be a section, listing in full, every other organisation they will share information and in particular listing those that they SELL the information to.

Question 19.

Comments: By complying with the DPA!

### **Section 5: Technology**

Question 20.

Comments: Technology has clearly had huge impact on sharing/protecting information. Vast quantities of data can be collected and stored in very small areas. Data can be easily accessed and manipulated. The transfer of data electronically is becoming easier by the day. Encryption is becoming standard in most applications improving security a hundredfold.

Question 21.

Comments: Encryption should be a legal requirement for any data being sent via ANY electronic or digital medium (CD-ROM or via email) and for all portable devices containing personal data. The encryption device used should be to an agreed minimum industry standard.

Question 22.

Comments: Research should never be at the expense of the identification of the individuals concerned as some of the research fraternity believe the ends justify the means. Accepting that research is vital to a rapidly developing world any method of anonymisation is acceptable and should always be applied - except of course where explicit written permission to identify and publish is obtained.

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

Question 23.

Comments: No experience outside of the UK

Question 24.

Comments: No experience outside of the UK

Question 25.

Comments: No experience outside of the UK

Question 26.

Comments: No experience outside of the UK

### **Section 7: Additional questions**

Question 27.

Comments: The sharing of confidential health information with the Police is of particular concern. As I understand it they are entitled to personal data under section 29 of the DPA but not Confidential health data (sensitive information). It has long

been practice that in the investigation of a "serious" crime (murder, terrorism) they can ask for confidential health information as well. Some clarity on this aspect of providing sensitive information under section 29 and the "for the administration of justice" exemption might be helpful

Question 28.

Comments: Once the fundamental principles of the DPA are understood it can be seen to be a fairly well balanced piece of legislation. As with any law there are always anomalies but what I would not like to see is the DPA tampered with to the point it becomes a weapon to beat organisations over the head with.