

# 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: Leicestershire IMAG member organisations (terms of reference attached to the covering e-mail as a separate document) cover all aspects of public service and hold information in its many varied forms to provide the citizens of Leicester and Leicestershire with the full range of public services.

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

Question 2.

Comments: The public sector is increasingly required to share information to improve service delivery. Varney (2006) supports the view that transformational government must increase the focus on the users of public services:

- In recognition of citizens growing expectations that they should not be expected to provide the same information to government on numerous occasions
- Joined up services yield efficiency by reducing duplication, and
- The most vulnerable citizens have to do the most joining-up between public services

The new performance indicators and Strong and prosperous communities: the local government white paper emphasises the importance to protect vulnerable people and respond to community need. This is reflected in the new performance framework we are seeking to align across all public authorities.

The Data Protection Act creates statutory barriers to enabling sharing to take place more efficiently and effectively, greater flexibility is required to facilitate the sharing of personal data where there is a strong business need. The expectation should be that we will share information with other public authorities where it is in the interest of the citizen.

It is important to acknowledge that there is a fundamental difference between sensitive business data and core personal information, with the latter acting as a major facilitator for information sharing and joint service provision. It is envisaged that the governance framework for managing core personal information will not be as stringent as that required for sensitive business data.

The Comprehensive Area Assessment proposes to implement a risk assessment framework that will tackle the issues around increasing the flexibility of public authorities to share information, moving the burden from a legislative to a statutory framework, and requiring governance in place to ensure information is shared in accordance with appropriate safeguards. The risk assessment therefore has potential to enable a more flexible approach to sharing personal information with other public authorities.

### Question 3.

Comments: There is a risk that individuals or groups might be prejudiced if personal information is shared and there is a lack of contextual understanding about how and for what purpose information was originally collected for and how it will be used. There were reports in autumn 2007 of individuals who had been refused employment because they had a criminal record, on further investigation it transpired that they were for minor offences committed 20 years previously.

Without clearly defined agreed guidelines for sharing information between partner organisations, there is a risk that organisations will lose control of the information customers have entrusted them to hold.

The main risks continue to be intrusion on privacy, loss of information into the broader community (eg HMRC) and human error. Most things can be removed - human error can only be reduced.

Other key risks include fraud and misuse - leading to concerns over safety etc. This means a high level of security and the associated controls are required to minimise the occurrence of these risks. Similar issues include the potential for misuse by less than benevolent individuals. There is also the potential for massive public disruption if the underlying information sharing systems are compromised. Also sharing of incorrect sensitive personal data concerning medical conditions, criminal records etc. may cause major detriment and distress.

Another area of concern is where there is scope for information sharing and such sharing is clearly in the public interests, but does not take place - perhaps because of a perceived legal restriction, a lack of knowledge on behalf of the organisation holding or receiving the information, a lack of understanding about the value of the information or just a reluctance to share. This is clearly illustrated by such high profile issues, as SOHAM, but life could be improved drastically for all citizens if full sharing did take place.

#### Question 4.

Comments: The greatest opportunities lie in our ability to join-up services through working intelligently with our partners. An example, is the sharing of personal information relating to young offenders with a variety of partners to allow provision of a better service with involvement of all relevant agencies.

A major risk is uncontrolled sharing approaches, where information is shared without knowing the information needed to address the issues being tackled. This can lead to information being shared that is not needed and other key information not being shared. The solution is not in complete sharing of all information, rather in a structured identification of what is required to best meet the needs that the sharing seeks to address. It is important to maintain public confidence that sharing will only occur when it is needed to meet a specific objective and such sharing will be limited to the minimum of information needed to best achieve the objective.

#### Question 5.

Comments: All organisations, public or private, probably hold more data than is needed to meet their functions. This is a result of collecting either too much data through not properly specifying requirements and collecting information on an "in case it is needed" basis or the collection of the same or similar data through separate approaches by different departments. It also arises from a "silo mentality" where information is seen to be power and therefore not shared elsewhere - either inside or outside the organisation. Often the holder of the data shelters behind the claim that legislation, typically the DPA, precludes such sharing. This means other departments or business areas will also collect the information with few of these being linked so there will be discrepancies and duplication.

A systematic co-ordinated approach by Public Authorities to information would ensure information is collected in a controlled manner and the organisation collects only what it needs for the tasks identified, takes all reasonable steps to ensure the accuracy of the information it collects, minimises duplication of requests of the information providers (ie the public), and knows what it holds, where it is held and adequate steps are taken to ensure completeness, accuracy and the integrity of the organisation's information stores.

#### Question 6.

Comments: This is answered in part at Q5. There is no reason to suppose the private sector is any better or any worse than the public sector in its collection and sharing of the information it holds.

The private sector does, however, generate a large amount of junk mail from using information incorrectly. This may well indicate too much information is being held and this information is being used appropriately - for example information collected for a specific purpose is then shared and used for other totally disparate purposes. Clarity in legal requirements is still lacking here and the law could be enforced more rigorously as in the case in countries such as Spain and Italy.

On the internet, Google and other online services, collect and distribute information far too readily, every time we surf we are being surveyed by Google Analytics or similar, all without being informed in advance. Meaningful fair processing notices are noticeable by their absence.

One of the constraints private industry faces in its ethical and legal use of data is that, in the main, its prime imperatives are to maintain business edge and to maximise profits. The preception appears to be build data high and don't bother so much about the accuracy - this costs too much. In essence the latter is a fallacy. Processing poor data leads to poor decision making, poor targetting and a loss of consumer good will.

The law does need to be precise and contain sufficient force to ensure organisations will comply with it. This on its own however is useless without proper enforcement by an adequately resourced regulatory body and the courts ensuring penalties are properly and consistently applied. The enforcement regime in England is poor and virtually toothless - the FSA seems to have more powers and be more willing to exercise them. This is not the case in other EU countries, for example Spain.

#### Question 7.

Comments: There are instances where it would be beneficial for private organisations such as utility companies to share information with public organisations. For example, if a utility company disconnects a customer's electricity supply for non-payment for services, the risk of house fires in the customers home increases if they need to use alternative sources of energy in the home. An alerting service between key utility companies and public services would provide early warning of citizens requiring support from public authorities.

Some personal data held by public services is ring-fenced and other public services are charged or prohibited to access the data, For example, council tax data and register of deaths. Where it is in the citizen's interest that personal information is made available to other appropriate bodies, the information should be made available.

There are several areas where sharing would benefit, but is not happening. This is for a variety of reasons such as perceived limitations by the law, professional ethics or a lack of understanding how data held can benefit society by sharing with another organisation for it to address issues under its powers.

The way the NHS, both hospitals and GP, interpret Patient Confidentiality is particularly

restrictive. It is recognised that there is a need to maintain doctor/patient confidentiality, but no more so than that in other professions such as lawyer/client, teacher/pupil, counsellor/confidor or social worker/client.

The limiting factor appears to be Caldicott, which was in place before the new DPA came into force and has not been reviewed since. Clearly if the additional restrictions inherent in Caldicott are valid to sensitive personal data covered by the NHS, they also apply to that sensitive information held by other bodies. If the Caldicott principles are not valid for these other bodies, it can be argued they are not valid for the NHS. This is not to say that there are not a lot of good points around the Caldicott agenda, there are but the rigid adherence to confidentiality, over and above that applied by other organisations who process similar sensitive personal data, is confusing and mitigates against effective sharing.

#### Question 8.

Comments: Information sharing does only take place where there is a need. The concern is more that insufficient sharing is taking place where there is a need because of perceived obstacles such as legal impediments. What is required is clear and more precise legislation, coupled with an effective staff education program.

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

#### Question 9.

Comments: The DPA works well. There is nothing in it that precludes effective data sharing where there is a clear requirement. It is often the unclear or weak statutory bases for information sharing in other legislation that cause the issues coupled with a basic lack of understanding of both the DPA and the Human Rights Act 1998 (HRA).

There is a need for a clear statutory base where sharing is expected, rather than a vague "may" occur, which opens such disclosure to challenge and, in an increasingly litigious society, it is of little surprise that organisations are not willing to undertake the risk.

It is accepted that there is a need to ensure that sharing only occurs where it is both proportionate and necessary, but in a lot of cases the onus is placed on people who do not understand the need for the sharing or appreciate the consequences should it not occur, again SOHAM is a prime example.

A lack of understanding of the Act and what it is intended to do also limits effective sharing. Consideration should be given to making training a statutory obligation on employers where personal data is concerned, over and beyond the current ambiguous situation. Understanding is key in promoting the sharing agenda.

#### Question 10.

Comments: Public organisations have often, mistakenly, been cautious about the second principle and see it as restrictive. This is not the case and they are becoming increasingly aware of the potential and need for partnership working, and also the flexibility in the phrase "not used for incompatible purposes" or to put it

more positively "may be used for compatible purposes. This is perhaps the main weakness of the DPA in that it is couched in negative terms which then leads to a restrictive interpretation. More positive wording is likely to lead to a more positive approach..

Experience shows that the Private and Voluntary sectors are also beginning to understand the benefits of collaborative working and responding accordingly. Again the profit motive of the private sector to some degree is seen as a limiting factor, for example the publicised British Gas case some years ago.

In practice, a clear lack of understanding of lawful bases for action and absence of properly considered fair processing notices with conditions of use of the information is what prevents not-incompatible use of data in most cases.

#### Question 11.

Comments: Technical barriers are inherent when it comes to sharing information either internally or externally across different systems. The nearer organisations can get to common standards and agreement on processes, the easier sharing will become. Pan-organisational groups working collaboratively to joint agendas provide the best long term method of addressing this.

Societal barriers include fear of litigation/personal liability , which has the effect of limiting staff use of information, lack of understanding about sharing and partnership working, little publically available and clear guidance and education. All of this fuels the public and media concerns over "big brother". Concerns also arise around identity fraud and a lack of understanding as to how the information will be used and the benefits to the individual arising from such use - education again.

Perhaps the greatest concern is the distortion and sensationalist approach adopted by the less reputable members of the media. Issues are sensationalised and blown out of all proportion to sell copy. There is a need to report effectively and properly, for example the recent problems experienced by HMRC, but the picture presented was less than balanced and by no means objective. The issue behind this is people believe what they see and hear in the media, at least to some degree, and this requires those undertaking the reporting to maintain ethical standards.,

#### Question 12.

Comments: The statutory overseer needs proper powers with deterrents appropriate to the offence that will act as deterrents. This is not the case in England, with the FSA leading on several high-profile cases and gaining the plaudits, when the agenda should have been led by ICO. This is not the case elsewhere in the EU and should be addressed, as should the provision of proper resources

There is also a need for better legal drafting and provision of guidance for specific cases. It is likely that if ICO was in the position of being the provider of guidance, with the ability to recommend (require?) the Secretary of State to enact the necessary secondary legislation, there would be a much more positive environment. The long term effects are likely to be better

understanding and compliance, but also a better understanding of what can be achieved under the law and more effective sharing of information.

Question 13.

Comments: The relevant EU Directive, 95/46, provides a clear direction to share information to improve economic and other well-being. That this is not being appreciated and acted upon is an indicator of failure - the legislation may be drafted poorly and incompletely, promotional work is lacking or has not conveyed its message adequately, education is similarly missing the target or issues are being mis-represented by the media to sensationalist effect. The DPA is not alone, similar concerns also exist around the HRA, but proper funding is needed to address the issues.

Question 14.

Comments: The guidance produced by the Information regulator seems to be unique in its lack of statutory force. Other Codes of Practice, for example those produced by the Office of Surveillance Commissioners and the interception of Communications Commissioners' Office, are brought into effect by Statutory Instruments. It would be more beneficial if a similar regime were adopted for the DPA.

The situation could be helped by much clearer and binding guidance. The Information Tribunal, through Durant, clearly defined what is and is not personal data; the Commissioner's latest guidance is at odds with Durant. The loser is the data controller, in either sector, who has conflicting guidance and hence uncertainty. It is of no wonder that people are choosing the safest option, often at the expense of effective information sharing.

The support the Highway Code gives to and receives from the Road Traffic Act is considerable, and the two work well together and complement each other. It is a pity the same cannot be said for the DPA and the Commissioners Codes of Practice. People know of the Highway code and understand it.

Question 15.

Comments: Proper handling of information (including collecting what is need for the purpose, ensuring it is complete, accurate and up to date, and disposing of it when it is no longer required) is good business sense. It ensure decisions are reached with the best available information, operating costs are minimised and consumer satisfaction and trust are maintained.

The DPA is very succinct in its requirements in this area, perhaps too much so because it does not provide any real guidance. The National Archive COP, produced under the Freedom of Information S46, goes a long way to address this, but lacks the force of statutory effect - it is optional. Accepting that the then government wanted to avoid undue burden and the associated costs on it, it still raises uncertainties and allows those who wish to to opt out of the COP.

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

##### Question 16.

Comments: Consent is a concern. It is often taken as the be all and end all of processing, and is frequently used as a barrier to effective sharing. There are a variety of other reasons for processing in Schedules 2 and 3, which can and should be used. Consent is uncertain in its application - it is not easy to evidence and can be withdrawn at any time the data subject chooses. It also entails checking on a regular basis to ensure consent is still valid.

Definitions of consent are perhaps unclear (especially the age of consent and parental rights under it). How to deal with incapable people is even more uncertain, eg learning disabled or the mentally unwell, and the thresholds and legal protections of such. Here again, legal clarity regarding issues such as Mental Capacity and the DPA would be helpful.

##### Question 17.

Comments: If consent was needed before sharing took place, sharing would never happen. There will always be people who refuse to share, putting personal interest above the well-being of society. The cost of separating out data covered by such refusals, linked with the costs of evidencing consent and maintaining it are enormous.

The EU Directive recognises the barriers that relying solely on consent would cause in that Schedules 2 and 3 both provide reasons for processing where consent is not needed. The HRA is maligned but article 8.2 provides clear guidance in that it recognises the right to privacy of the individual can and should be subsumed where there is an overriding need to the wider society.

##### Question 18.

Comments: The Commissioner has started the process and produce guidance on the sharing of information, especially in the public sector. Again this suffers because of the lack of legal certainty, which can only inhibit effective sharing. It is one thing to say that prosecution will only occur where there is a clear legislative breach and the processing is not in the public interest, and another thing to be believed. Perhaps this stems, in some part, from the conflicting advice received from different areas of the Commissioner's Office on the same issue. This just builds on the general atmosphere of legal uncertainty.

Awareness raising and public education are key in promoting the sharing agenda, but the message must be positive. Highlight the benefits that can be made from effective sharing. Eradicate the concerns such as security of information. Provide leadership and certainty in what is expected - both of organisations and the citizen. Show people how consideration is given in balancing the rights of the third parties, offenders etc., when they are involved. Provide effective guidance, eg capacity issues, with a greater degree of certainty of effect.

##### Question 19.

Comments: More guidance provision is needed. The ICO guidance is very basic, but useful however as has been highlighted it does not have the legislative impact that COP issued by other regulators have. This must be addressed.

Privacy Impact Assessments, if compulsory, would place a massive burden on any organisation undertaking data sharing that would probably outweigh their value if people follow the DPA principles and lawful obligations anyway. An overall business risk assessment would, however, be prudent.

## **Section 5: Technology**

### Question 20.

Comments: Information can be controlled better with new technology. It provides more security and greater ease in locating information, even that poorly labelled. One of the major work costs is the unnecessary time people spend searching for information. Even so difficulty still exists in finding electronic information which may be held on e-mails, in archives or back-ups or a variety of other sources. The great improvements made in information search and retrieval technologies, such as the continuing growth in search engine capabilities, is helpful, but should not be accepted as a potential universal panacea - the paperless office springs to mind.

Much of the information held by organisations hold is in paper form. A presumption exists that information should be available electronically. This is unrealistic. The costs of back-scanning all information are immense and business considerations will take priority. Difficulty exists nevertheless in finding information as they may be emails, backups, archives etc which might be inaccessible or timely to recover. To legislate otherwise would cause undue burden and should only be considered if adequate funding were made available.

Use of Electronic Document Records Management Systems (EDRMS) with proper retention/disposal policies and metadata should enable timescales for provision of information to be reduced. While information should always be provided in as timely a manner as possible, reductions in legal timescales should be resisted as they provide a reasonable time to consider disclosure issues properly.

The main issue the public raise when sharing their data is the security of transmission and handling by the receiving organisations. To this end, in spite of the issues that have been raised over the past few months, technology has a major role to play - it is more cost effective and more secure to keep information in a professional manner electronically than it is to hold the same information on paper. However mistakes happen. It is important that when they do they are handled with total honesty and transparency, and the public can see effective action is being taken. Several US states have laws that require loss of data to be reported and publicised. Consideration should be given to such a step in England. It is likely to build public confidence in the handling of their data, which was recently reported to be the second most important issue to them.

### Question 21.

Comments: Yes - if it mandates specific standards and processes. Not if it mandates

specific products or systems. Some degree of choice to meet differing business requirements is needed. Specific options should only be mandated where there is some choice, say a list of 3 similar to the process in use by the police.

Any mandate is likely to give rise to undue burden and adequate resources must be made available where there is an imposition rather than things left to choice.

Question 22.

Comments: PET do work and can be very effective, not only in protecting the security of information but also in improving information quality.

There is a very limited amount of information available, such as what the options are, where they are most effective and where care is needed in their deployment, most of which emanate from suppliers with a particular axe to grind. As a result the general understanding of the technology and the appreciation of the benefits PET can bring are limited. Again clear guidance and awareness raising are the keys.

It must also be remembered that PET application is limited. Most information held by most organisations is still paper-based, and attention should also be paid to providing guidance and awareness raising here.

## **Section 6: International comparisons**

Question 23.

Comments: Notifying data subjects of breaches, as in the USA, is a useful feature that could be adopted. Also forcing data controllers to publicise breaches and what has been done to address them at the time of occurrence would at least assure the public of the transparency and effectiveness of the process. However, this would need accompanying by education to highlight that no security is 100% safe - manage expectations effectively.

Greater powers to the Commissioner and the associated resources would also help. Until the Commissioner is seen to be acting proactively and positively the DPA, and associated legislation, will remain problematic.

Question 24.

Comments: No comment.

Question 25.

Comments: Italy, and Spain have restrictive approaches to Marketing. This is being fought by industry, but does ensure the inhabitants of these countries do not receive the same amount of junk mail as happens in other countries .

Question 26.

Comments: England shares information better than most. The DPA reflects the spirit of 95/46 more closely than comparable law in other jurisdictions. This spirit of openness is understandable when considering history and the impact of occupation on mainland Europe. It is likely the more restrictive approaches in

force on the continent tend to stem from mainland Europe's (and Eire, under De Valera!) experiences with dictatorship in the 20<sup>th</sup> century.

This enlightened approach to information sharing is not entirely a good thing, however, as this could lead to a "sleepwalk" into a very controlled society, at the cost of the erosion of personal liberties and freedoms. The burgeoning growth of CCTV systems and the surveillance society is of distinct concern.

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

Question 27.

Comments: Given the profile of DPA, CCTV et al, the popular view is that the public sector shares information now to a great extent. If the correct arrangements are in place and adverse reporting of DPA/HRA is challenged effectively, then multi-agency data sharing may occur more often and with greater public confidence.

Question 28.

Comments: No comment.

