

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 am Information Policy Manager for Education Leeds (a company wholly owned by Leeds City Council providing education support services).

Many types of personal information are collected about staff, pupils, parents and governors from across the city. The data fields are diverse and include sensitive and non-sensitive. The sensitive personal information includes matters of health, ethnicity, religious belief, offences and alleged offences, union membership and sexual life.

The core data set (about pupils and parents) is collected electronically as part of the government's annual schools census. Much additional information is also collected via paper forms or other processes (including statementing of special needs). Information about staff and governors is generally collected via paper forms. The majority of information is stored electronically although there is also a large volume of paper storage alongside this.

Information is shared with other children's service authorities; we have a duty in accordance with the Children Act 2004 to promote the wellbeing of children and young people through cooperation. Information sharing is regulated through a common city-side protocol and subordinate information sharing agreements.

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

Question 2.

Comments: One of the Key benefits to individuals is ease of access to services and also avoidance of the need to provide the same information repeatedly. Generally there is a perceived expectation that basic information is shared in order to facilitate services. Sharing information does allow for the provision of better services, more tailored and responsive to individual need (e.g. through the Common Assessment Framework introduced under the Children Act 2004). For society at large the benefits include more efficient practice and hence more effective disbursement of public funds. In some specific instances the benefits to society are related to increased safety (e.g. in relation to Anti Social Behaviour investigations) and probity (in relation to benefit fraud investigations).

Question 3.

Comments: The risks of sharing information arise from three broad areas; the actual mechanism by which the information is shared (e.g. lost CDs sent via unsecured mechanisms); subsequent compliance with the DPA by the recipient (recipient may not have robust procedures compliant with the principles or may re-use the data without due regard for proper process) and destruction of trust amongst data subjects or withdrawal from interface (if data is shared against their will, even though compliant with schedules 2 & 3).

Question 4.

Comments: The scope of the sharing should be proportionate to the purpose of the sharing; wholesale sharing poses the greatest risk because this is likely to involve information which is irrelevant to the purpose. In terms of methods, information sharing agreements drawn up in response to specific sharing needs and setting out purpose, mechanism, supporting processes, training needs, data fields, justification and contact

information provide the best method as these are specific considerations to the sharing exercise in question. Methods whereby information is simply provided with no supporting agreement leave room for exploitation and no agreed procedures for rectification.

Question 5.

Comments: It seems peculiar that the Inland Revenue do not know how much tax an individual has paid through their employer and frustrating that they frequently ask for this information.

Question 6.

Comments: Banks and supermarkets are the two main private sector organisations which hold too much information, the purpose of which is vague at best. Banks are known to ask questions which appear irrelevant to the activity (e.g. asking how much your property is worth when you are trying to open a savings account). Supermarkets collect information about your shopping trends whenever you use their loyalty card however it's not clear what happens with this information. Certain utilities appear to have insufficient systems through which to record relevant information (such as changes to marital status or amended account holder details).

Question 7.

Comments: Although I can think of no relevant examples, I am aware of cultural conflicts between organisations which follow the Caldicott Principles and those whose first consideration is the Data Protection Act. It is confusing to have to address both considerations whereas it would be much better if health and social care bodies focussed solely on the DPA.

Question 8.

Comments: I am not certain of the legality, but would question the practice of access to personal details overseas by organisations such as banks. I am unconvinced that personal information is secure when being accessed in countries (such as India) beyond the EEA. I'm not sure that the UK based data controllers always ensure that conditions from Schedule 4 are satisfied and neither am I convinced that fair processing requirements are always met with.

Section 3: The legal framework

Question 9.

Comments: Generally the DPA works well but in practice there are areas for improvement. One of these is that the secretary of state should be more receptive to use of his/her powers under schedules 2 & 3 in response to specific issues. Also, the punitive measures under the Act are woefully inadequate and should be strengthened (in terms of size of fine and potential custodial sentences) in order to drive home the importance of proper processing of personal information.

Question 10.

Comments: The second principle is perhaps the most often overlooked, potentially because not all uses can be perceived at the time of collection. It may that a privacy impact assessment could be conducted prior to re-use of information for alternative purpose in order to ensure that the proposed re-use is not inconsistent with rights and freedoms conferred under the DPA and other statute such as the Human Rights Act and common law duty of confidentiality. The second principle is made somewhat superfluous by the First which state

that consent must be obtained for the proposed processing in any event thus is an alternative purpose is to be pursued the onus is already on a data controller to notify the data subject.

Question 11.

Comments: Certainly in respect of subject access rights there are still some long serving officers in the public sector who find it difficult to accept that an individual has a right to see information held about them (in most cases). Poor records management practice is another institutional barrier not only in terms of effective subject access handling but also in terms of compliance with the third, fourth and fifth principles. Technology makes it far too easy to copy data quickly from one media to another and even to transfer virtually anywhere in the world with ease. This latter risk is especially relevant in a public sector which faces increased demand with fewer resources and where practices such as remote working are increasing as technology develops.

Question 12.

Comments: As mentioned to earlier, there should be much stronger punitive sanctions under the DPA for wilful breach; this could either be in the form of higher fines or custodial sentences (or both). Also, the Commissioner would benefit from the power to be able to inspect organisations without invitation and at short or no notice. This would encourage data controllers to place more importance on compliance whereas currently there is mixed practice in this regard. Similarly there should be a requirement to notify the Commissioner of all significant data losses as currently once this happens there is nothing to prevent the matter going unaddressed unless a complaint is made. Although this may require additional resources, the charge for notification could be raised to £50 per annum to contribute towards this.

Question 13.

Comments: It is sometimes difficult to navigate through schedules 2 & 3, then test against the common law duty of confidentiality and the Human Rights Act (article 8). The common law duty of confidentiality in particular is difficult to in that one of the methods through which this can be disapplied is if it is in the public interest to do so; this is a subjective test in most cases and thus it is difficult to strike a proportionate balance. The directive itself does not often come into play in connection with data sharing (although obviously it is concerned with the processing of personal information); however, there may be potential for conflict if the strict definition of personal data under the Directive was followed, rather than that under the Act. The Act's version is subtly different in that it includes the phrase "*and other information which is in the possession of, or is likely to come into the possession of, the data controller*" whereas this is absent from the Directive.

Question 14.

Comments: It is frustrating working in a Children's Service authority that you need to share information yet the supporting statute does not explicitly permit this. For example, the Children Act 2004 (section 10) lays down the duty to cooperate and it has to be assumed that this covers information sharing; however this section could have made specific provision for information sharing. Under current arrangements it is far from certain whether the sharing of sensitive personal data (without consent) about a child is permissible.

Question 15.

Comments: I'm not aware of any unreasonable burdens. The protection of personal information is of paramount importance hence any burden encountered (such as subject

access) is proportionate.

Section 4: Consent and transparency

Question 16.

Comments: The rules surrounding consent are clear. I have been involved in the development of the Leeds Interagency Protocol for Sharing Information and guidance on consent has been included in this (<http://www.leeds.nhs.uk/infoshare/protocol/>)

Question 17.

Comments: This adds time to the process of information sharing hence it is always simpler to share information using some other justification for doing so (notwithstanding the need to satisfy fair processing requirements). Furthermore, it is often difficult to gain replies from individuals so the process of gaining consent in every scenario would be prohibitive.

Question 18.

Comments: Organisations could be required to have a "publication scheme" type arrangement (perhaps through privacy statements) through which details of information sharing agreements should be made available. Perhaps the publication of such agreements should be listed as a mandatory requirement in relation to the current publication scheme rules under FOI. This could also be addressed through the distribution of an annual leaflet setting out what agreements are in place (this is something that is in place across schools as a requirement of the DCSF); in Leeds we distribute a leaflet to new pupils in either the Primary or Secondary sector each year explaining how information is shared, with whom it might be shared and for what purpose. This includes details of our subject access procedures in order to make clear how to make such requests.

Question 19.

Comments: The approach taken in respect of the protocol discussed earlier was to involve user groups in the protocol's development. This ensured (so far as possible) that their concerns were taken into account). User groups also helped to disseminate news about the protocol's ongoing development. The steering group is still established and user representatives still invited though regrettably interest has waned. Privacy impact assessments are very useful as they ensure that all considerations are taken into account before proceeding with the sharing exercise.

Section 5: Technology

Question 20.

Comments: Technological advances have undoubtedly made it easier to share information both lawfully and unlawfully. The convenience of technology also lends itself to complacency; for example many people still email personal information but unless this is done using encryption, data is vulnerable in transit. Similarly technological advances allow for more and more methods of data transfer on mobile devices such as PDAs, data sticks, laptops, DVDs etc whereas the adoption of encryption on such devices does not keep pace.

Question 21.

Comments: Yes. The recent enforcement notice against Marks & Spencer's is a timely reminder of and useful driver in the fight to have resources allocated to such security measures. If the law had mandated minimum standards then such data losses might not

have occurred and resources may have been easier to attract to put encryption in place.

Question 22.

Comments: I am unaware of privacy enhancing techniques. If we are asked for data for research or statistical purposes we already remove personal identifiers and also take measures to round up small cohorts in order to avoid easy identification from certain data (e.g. it may be possible to identify an individual if they are the sole person with a specific ethnic origin or religious belief.

Section 6: International comparisons

Question 23.

Comments: No knowledge of any.

Question 24.

Comments: No knowledge of any.

Question 25.

Comments: No knowledge of any.

Question 26.

Comments: No knowledge of any.

Section 7: Additional questions

Question 27.

Comments: The list appears to be comprehensive.

Question 28.

Comments: None.