

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 a management consultant working in public sector modernisation, in both central and local government. I'm also a non-executive Director of DVLA. The ability to share - or better still, not share but validate - data often underpins a customer-focussed, efficient service design; data sharing therefore vitally affects both me, and the government services I work with.

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

Question 2.

Comments: 2 Sharing or validating data enables customer-focussed, efficient public service design; it should allow us in government to change the way we do business with the citizen to minimise intrusion and cost, and maximise one-stop service delivery – or even better, no-stop service delivery using continuous payment methods for continuing service provision. Data sharing also enables customer self-service where this is appropriate.

Examples:

1) I led a project to deliver an e-Benefits process for London Borough of

Southwark where, by getting access real-time to DWP's CIS, our e-Benefits officers complete the benefits application form, carry out the assessment and put the claim into payment during the initial interview. As part of the One-Touch service that has just gone live, this can be offered over the phone to some customers where, by validating the fact that they are already in receipt of passported benefits, we know they are entitled to housing and council tax benefits – so they don't even need to visit in order to get a claim into payment. In this instance, the claim is paid after a 20 minute phone call, the first time they ever contact Southwark – clearly exceeding customer expectations, and a very efficient process for the council.

2) The One-Touch service is designed to offer all the relevant services for certain life events, and it also shares proof data across the various potential council services. This minimises the bureaucracy necessary to set up services eg for a mover-in to the Borough who would perhaps need to make a benefits application, register for council tax and the electoral roll, join the library, etc and maximises the chance of offering all relevant services.

3) I am in the process of implementing a pilot Tell Us Once project where we will securely transmit death notification to other council departments and potentially central government when a death is registered, eliminating the need for the bereaved to send death certificates to multiple departments, and ensuring a systematic and improved post-bereavement service is offered to citizens.

These are generally providing benefits to individuals and to government; there is – should be! – a knock-on effect to society in the longer term of reducing the cost of government through effective, simple services.

I have other examples if required – contact me!

Question 3.

Comments:

Risks to individuals tend to be around misappropriation of identity data. In general, the more linked systems are, the quicker bad information propagates through them – so the more important it is that data should be visible and validated at all possible opportunities, while being held securely from misuse.

Risks to society are posed when data is kept or shared unnecessarily or excessively without a specific, measurable aim – I am uncomfortable with some of the sharing being proposed at present as I don't see it leading to better service, security or effectiveness/efficiency, merely to increasing bureaucracy 'because we can'. I am very unconvinced, for example, of the benefits of putting biometric data onto cards – this increases the value of the token, and therefore increases the risk around the system. Nobody has yet provided a convincing argument that it increases security in any of the applications I've seen promoting it.

There is a risk around the general growth of the 'surveillance society' – I will leave comment on this to the experts aside from saying I don't like it much.

Question 4.

Comments:

There will always be risks as well as advantages from data sharing, but in general, this risk can be reduced by validating data rather than sharing it. By this I mean that instead of transmitting and sharing data, we use trusted partners who already have the data to confirm it. See also Q28. For example, a Local Authority knows that if someone is on DWP

passported benefits, then they are entitled to housing benefit, since DWP will already have checked their income etc. So we don't need to see/share this income data, it's validated already by DWP's act of paying a benefit. Similarly, in order to issue a parking permit, we might ask DVLA to confirm that someone's car is registered to them, taxed and insured – we don't need to see or share any data other than a 'yes' from DVLA in response to our business rules.

My view is that this is the sane approach to government data sharing – ie have single owners for information, and get them to validate rather than share data wherever possible.

Question 5.

Comments:

In principle, systems should be designed to hold the minimum data, and not to duplicate that which is held elsewhere by government – in practice we're a long way from that at present! In particular, though, I suggest that a place to start might be with any system which deals with payment, eg the EVL system records and keeps customer card details – an unnecessary and insecure piece of design. Generic standards could be promulgated to improve the approaches overall.

Question 6.

Comments: Not my expertise.

Question 7.

Comments:

7 See Q1 for examples of work-in-progress on Tell Us Once – this should be extended to all changes of circumstance – address, marriage etc etc. Legislation prevents this from happening on a mandatory basis, but with consent it could happen immediately – it just needs to be implemented securely. All that prevents is the government departments agreeing the protocols and implementing it.

Medical history/records is another area where data is not joined up – I have experienced this from a personal rather than professional perspective and it was clear that basic information simply does not get to the point of requirement.

Question 8.

Comments: No information on instances of this.

Section 3: The legal framework

Question 9.

Comments:

My anecdotal observation is that it tends to be used as a reason for not providing perfectly lawful data. I think however that the legislation is about right – but government could sensibly obtain data for a more generic purpose – eg 'government address records' rather than 'DVLA vehicle keeper', 'DVLA licence holder'. This would be a simple redesign of data collection forms. I really don't think we need any more legislation to be enacted right now!!!

There are issues around audit trail of data use which need to be developed – I suspect at present that there are many unlogged uses of public data which a citizen cannot find out about – I base this view on their being no systematic architecture for doing this in most IT systems, rather than on any intention of any body to withhold information.

Question 10.

Comments: As above, I think it's a very reasonable principle to have. My experience is of conservative application of the rules by public organisations. Example: the GRO refused to even give us overview numbers of deaths of local residents in one local authority even though they are part of the team to develop the Tell Us Once project.

Question 11.

Comments: Many existing systems do not have a systematic means of providing a data access audit trail; this needs to be built into developments to improve the effectiveness of redress of the private citizen as data sharing becomes widespread.

Question 12.

Comments: I do not consider there is a compelling case for modifying the DPA; rather we should learn how to use the existing legislation in a pragmatic but secure way.

Question 13.

Comments: not my expertise

Question 14.

Comments: not my expertise

Question 15.

Comments: Given that my advice is that data can be shared with consent, then if we set up secure, consent-driven systems and they are seen to work, there should not be insuperable barriers to responsible data sharing.

Section 4: Consent and transparency

Question 16.

Comments: With respect to Tell Us Once, we have received legal advice that data can be shared with consent. We will be transparent about what data will be shared, with whom, and why, and with what security.

Question 17.

Comments: The requirement for consent does make it more complex to develop a process where nationwide data gathering drives local action, as with Tell Us Once – it implies that all other LAs must have the identical process in order for data to be seamlessly shared. In practice we believe that, at least initially, we will have to introduce another step into the process once we know about an event of interest, so that we go back out to the citizen (living in other areas) and get the same consent from them as we would from our own residents.

Question 18.

Comments: See also 11 above. Transparency of data use is paramount.

Question 19.

Comments: I didn't know about these even though I am interested and active in these areas.

Section 5: Technology

Question 20.

Comments: not my expertise

Question 21.

Comments: it should not be possible to post and lose discs of unencrypted personal details!!!

- a) Encrypted electronic transfer must be the preferred route for transmission – if we REALLY need to transmit, but...
- b) wherever possible data validation rather than sharing should occur
- c) if the raw data needs to be seen, then secure access to the base systems should prevent the need for transmission of the data.
- d) only if b and c don't pertain should we send data.

Question 22.

Comments: not my expertise

Section 6: International comparisons

Question 23.

Comments: not my expertise

Question 24.

Comments: not my expertise

Question 25.

Comments: not my expertise

Question 26.

Comments: not my expertise

Section 7: Additional questions

Question 27.

Comments: None known

Question 28.

Comments:

I'd like to reiterate the strategy of validating rather than sharing data wherever possible. Often a process does not actually require data to be shared, it simply requires that data elements are confirmed by a trusted partner to meet certain business rules.

Let's consider the hot potato of road-user charging. The worry is that the in-car box will download route information to a charging centre, and people are very concerned about the civil liberties implications of a box that will tell the government every detail of their movements - the 'Big Brother' face of data sharing. However, an alternative approach is to design the system so that the box knows the charging schema and instead of passing route information to a charging centre, it merely says 'I know where he's been and he owes you £50.32'. Both system designs require a tamper-proof in-car unit, but one shares raw data while the other validates against a set of rules and shares the minimum necessary to

achieve the required outcome.

Not only is this potentially more secure for the citizen, an overarching strategy of this type would drive government organisations to collect and hold data only once – ie no repetitive (and conflicting) address records, name records etc.

And finally

Remember, most citizens think of government as one organisation and can't understand why data is not shared. We should design secure services accordingly.