

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 business consultant involved with the concepts and practice of information sharing.

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

Question 2.

Comments:

Individuals can often be provided with more efficient service when an agency knows more accurate information derived from a number of sources.

Society benefits from a greater knowledge base and has the potential to reduce fraudulently supplied services

Question 3.

Comments:

a) individuals may have personal data exposed to unauthorised agency officers - with the potential for misuse.

b) Society loses confidence in agencies if data governance policy is not applied.

Question 4.

Comments:

The greatest risk is created by not separating index data from personal data. Indexes should only include items that are publicly available. This should be limited to what is in a passport plus an address. I shall call this the IDBase, see Question 21.

Single operational systems should be allowed to combine IDBase data and personal or transactional data. I consider that system identifiers such as a NINO, NHS No or UPRN to be personal data and not exposed to the general public.

Joined up systems should use indexes, or an index of indexes, before being given access to personal data items under strict protocols. See Question 27.

The big risk is a lack of understanding of the index separation and bypassing agreed data governance processes.

Question 5.

Comments:

There is no issue about the amount of data held. It has to be sufficient to provide a service.

The problem is that no index of IDBase data is available to all agencies.

Insufficient data is held about the relationship of individuals, eg parents, siblings, close family, step families. This could be vital for the safeguarding of children.

Question 6.

Comments:

Affinity cards, such as Tesco, hold too much information without public scrutiny of usage and governance procedures. Granted that the information is given with consent and some benefits may accrue to individuals.

More could be done to ensure there are no opportunities for misuse of the data.

Question 7.

Comments:

Children continue to be killed because data is not shared.

The technology and governance infrastructure to enable safe data exchange is inadequate.

Re-engineering is required using matematically sound concepts.

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments:

The Government is toothless. Even if trangressions are identified the is no effective recourse.

It sets good guidelines. It keeps agencies aware of their responsibilities of data controllers. Some people are too zealous and can make business processes too complicated - or impossible.

A weakness is that it does make clear how consent to share can be used. It does not embody the concepts of the Context where data can be uses or the Roles of people who might legitimately view personal data.

Question 10.

Comments:

They generally adhere to the Principle - but that is not necessarily in the best interest of the citizen or society.

It is too restrictive to allow beneficial data sharing.

Question 11.

Comments:

Identity Management of both the data user and the data subjects is currently uncontrolled and uncontrollable.

Question 12.

Comments:

Agencies (public and private sector) should publish metadata of the data they are holding. This could be published on web sites.

There should be some redress to the citizen for any agency sharing data without consent and providing data to others that is inaccurate. More emphasis should be placed on data quality. Correction should be a citizen's right and implemented within a month.

Question 13.

Comments:

Acts that appear to restrict the ability of Councils to share data, such as Council Tax data, should be amended. Most of the general public think it happens, because it would be dumb to not share such data.

Question 14.

Comments:

Published meta data would expose data sharing opportunities. There should be a set for identity management and a set for personal data.

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

All data should be collected with the expectation for data sharing can be subject to citizen consent. This should be at the single attribute level and capable of being modified by role and context supplied by the external party.

Many of these conclusions have been drawn from research work done on the FAME (Framework for Multi-Agency Environments) and Child Index national projects.

Question 17.

Comments:

The administrative overhead for attribute level consent is large. Much can be avoided by blanket consent processes.

It would be eased if consent was self-administered by citizens. The cost of such an infrastructure would be large, but it could be a shared service that covers all sectors.

Question 18.

Comments:

1. Published meta data
2. Self-administered personal data viewing and correction.
3. Strong authentication relying on biometrics.
4. An index of all IDBase data and all agencies holding records
5. Enforced e-GIF standards

Question 19.

Comments:

Section 5: Technology

Question 20.

Comments:

Master Data management should improve the accuracy and interoperability of systems. Some of these carry clear field level security indicators.

Question 21.

Comments:

There should be two classes of data; Public and Personal. NOTE: I regard data as raw data items and information some useful collection of data items. For the record; knowledge must involve a human element wisdom is knowing how to use knowledge effectively.

Public data is what you would be obliged to give to a policeman - the IDBase. I don't know the law, but is probably name, address and date of birth. I would also include passport requirements eg place of birth and citizenship.

All other data is Personal

Question 22.

Comments:

Such techniques are a waste of effort in most circumstances . Encrypted personal data may be allowable in medical research if the citizen could be identified and helped. Work would proceed anonymously but a data processor could identify the person with a suitable governance protocol.

A public fear are fishing trips to identify target groups. This should be forbidden unless individually authorised by an officer of the law. Most people believe that the security services do this - it should be made transparent.

Section 6: International comparisons

Question 23.

Comments: The Liberty Alliance has some good examples.

Question 24.

Comments: The Liberty Alliance has some good examples.

Question 25.

Comments: The Liberty Alliance has some good examples.

Question 26.

Comments: The Liberty Alliance has some good examples.

Section 7: Additional questions

Question 27.

Comments:

Look in detail at the FAME generic framework. It has nine sections: Business Case, Governance, Legal Issues, Identity Management, Information Sharing, Federation, Infrastructure, Sustainability and Messaging. The value is that it puts information sharing in a total context. In practice we operate in a very complex environment and should not focus on one small sub set. With variations, the guidance could be applied to any sector.

FAME also created a Roadmap process that build practical implementation plans that consider all the Framework guidance.

Question 28.

Comments:

There is a set of ISO Standards that define an architecture and methodology for:

- integrating data from different sources
- sharing data among applications
- mapping data with different coding structures

By using the standards, developed by the private sector, different agencies could cooperate more efficiently. Using an integration model and standard reference data can reduce interface cost by 60% - 75% (Prof Matthew West 2003)

A safe information sharing architecture based on these principles has been devised. Following the principles of ISO 18876, it avoids the need for a single unique identifier; it manages multiple identities. Such a system could be built that conforms to data protection legislation.