

# 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

InMezzo staff have been involved in providing products for business system security since about 1990. Business system security is focused on controlling who can access information and execute transactions, and who can authorise access. These security solutions tend to be user or identity centric, and, as such, authentication and authorisation are central aspects of their operation.

We have recently been concerned with local authority social services requirements where the protection of personal information is most sensitive. But the approach we take can be applied to much less sensitive areas as well, more easily.

A fundamental principle of our approach is that we do not hold personal information: we collect shared information in real time when needed, to establish access rights

The main purpose of sharing social care information is to provide health and welfare services to citizens, including in their own homes via telecare - this needs significant collaboration (Local authority, NHS, Emergency services, Housing, Voluntary and commercial organisations) and information sharing on

a large scale but very personalised basis.

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

Question 2.

Comments:

The obvious individual benefit of information sharing in our specific example (telecare) is in the coordination of several services to respond instantly to a citizen health or welfare incident, which is probably the most demanding personal information sharing requirement. To society, containing the costs and resource requirements to deliver care in the future is one of the biggest challenges, and it cannot be done without collaborations. Good information sharing will improve response decision making.

Question 3.

Comments:

The risks of sharing personal information is in identity theft for the purpose of financial theft, enabling attacks on vulnerable people by gaining access to their places of residence either virtual or real, access to children's information for paedophiliacs.

The main risk to society of misuse of personal information is in the potential breakdown of financial systems due to identity theft, the potential for increased targeted terrorism, and the misuse by inappropriate government staff to target specific people in personal or group vendettas.

Question 4.

Comments:

The opportunity to deliver coordinated preventive and self care, and respond to personal incidents must rate as the highest opportunity. This should be delivered through telecare. However, access rights should be on a personalised care relationship basis, not just role based. Telecare will not be acceptable if any old nurse or social practitioner can 'break in' to a vulnerable person's home.

Question 5.

Comments:

It is where the information is held that is the problem! Every central database (e.g. ContactPoint, NHS Spine) suffers the same problems: a) they dramatically increase the damage an attack could cause b) they increase the disruption caused if there is a system failure c) it is not possible to manage them in the sense of ensuring that the information is always clean and up to date d) if you tried to manage this it would be too expensive e) there are too many authorised users to keep control and avoid misuse f) they muddy the responsibility of the information owners - if anything goes wrong with the central system which creates a legal issue, (e.g. a death caused by a lack of service or incorrect information) who takes the blame? f) This question is compounded by the fact that most of them are supported by outsourcers g)

They probably take up too much bandwidth transferring information which is never used. The answer is for authorised users to retrieve the information in a controlled manner from the information owners when it is needed - this resolves all those problems.

Each government organisation has a legal and fiduciary responsibility to protect the personal information it holds about citizens. It should only, therefore share information with any other party (government department, agency, private organisation, contractor) when its management team has a) articulated and published its information sharing policies and collaborations, b) can demonstrate that these are enforced in their ICT systems, and c) has them independently audited. Government organisations should be operating access rules on a 'need to know' basis. It should not be difficult for the Ministry of Justice to prepare several best practice templates (based perhaps on the Commissioner's Info sharing Framework) for government organisations to select from and tailor. Perhaps the DPA could also be identified as the auditor).

#### Question 6.

##### Comments:

The private sector should only have access to government information under the arrangement suggested above in Q5. Sharing of information between them could be regulated under similar rules, and licensed.

#### Question 7.

##### Comments:

I believe the most problematic case is the sharing of information between local authorities and their local NHS PCT and hospitals, and the Police. There are only a few that have any level of collaboration in place, but it is vital for citizen safety and care, and this demands real time collaboration. It is wrong that the institutional needs of central government has taken precedence over these local needs.

Information is not being shared because a) the NHS has imposed a centralised security approach which precludes collaboration by insisting on smartcard access, which local authorities (and others) could not implement b) CLG, NHS and Police are all trying to impose their own security approach on the others, but none of them are appropriate for collaboration c) Information sharing agreements are not in place d) data is not clean in any of them so staff are disinclined to share because they have little confidence that their own records are accurate for which they could be held to account (we estimate that 25% of just child identity data in case management systems is wrong) e) even in child care, local authorities can have up to 25 business units with some responsibilities for children, they may each have their own different operational applications bought from different suppliers, which all need 'integration' even before external collaboration becomes of real value and f) without enforced policy, compliance and collaboration management in their ICT systems, executives are reluctant to approve information sharing because of their legal and fiduciary duties to protect the information they own.

To overcome the barriers, the practitioners requesting access to a person's information must be registered and administered on a number of systems. The

local administration processes manage the churn and change associated within the user based ICT system. Practitioner access to personal records must be based on up-to-date details concerning the practitioner, because of his care relationships. This is the responsibility of the practitioner's home organisation.

To resolve all these issues by directly linking the applications together for two or three organisations is a major task. Any larger scale collaboration becomes impossible to manage, both in its implementation and its operation. Such an approach tends to lock in the participants. The hub approach adopted by InMezzo removes this barrier to an extensible solution, and is much more flexible. It addresses the four key information collaboration issues: a) How do departments and agencies demonstrably control the exchange of records in accordance with their own complex and changing information management policies? b) How are individuals identified in a consistent and trusted manner across all the different systems containing their records? c) How can the administration of practitioner access be implemented in a distributed, scalable environment? d) How are systems integrated to provide a scalable personal access solution?

The solution involves a) identity management of both users and citizens, b) federated authentication and authorisation, c) policy management so that each party can set out its own rules, policies and compliance requirements independently of all those it collaborates with, d) data transformations, to enable diverse applications to understand each other's information, e) aids to data cleansing, and f) control of third party remote access to critical business assets. Appropriate data sheets can be supplied if required.

#### Question 8.

##### Comments:

I am particularly concerned about ContactPoint. It contains much information of use to paedophiles. Looking after children is and should remain a local matter requiring only local collaborations. Something much simpler could be devised for transferring children who move outside their area.

Similarly, the centralisation of patient records in the NHS Spine with only role based access controls is a nonsense, for reasons given previously. Too many staff (and contractors) have access (recently exemplified by 60 NHS staff accessing a VIP's health record for sheer gossip reasons!). Access rights should be for care relationship reasons only. For all other accesses the information should be anonymised.

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

#### Question 9.

##### Comments:

The DPA does not seem to have any teeth, there have been too few convictions for violations. One problem is that it must be very difficult to police violations. If the Registrar is able to strengthen the role of developing best

practice information sharing policies and then auditing them for government, also requiring accountants to report on them for the private sector, this might help.

Question 10.

Comments:

There are many organisations that hide behind DPAs rules to avoid doing sensible things. Wadworths refused to put in CCTV in theft vulnerable pub car parks, citing the DPA. The DPA principles are right but the practice is complex and seen as technical. What is needed is a politically articulated very simple vision, that every one can understand (e.g. on half a sheet of paper and only 3 bullets!). This would reduce the confusion, and guide technical details more clearly.

Question 11.

Comments: See 9 & 10

Question 12.

Comments: See 9 & 10.

Question 13.

Comments:

Question 14.

Comments:

It is mainly authorisation capabilities and policy management that are missing from any transformational government debates that I have attended. This could be part of the suggested approvals for licencing information sharing agreements (see answer to Q5)

BS7799 was meant to have been signed off by all government departments several years ago, but quite clearly is ignored by HMRC and many other departments. The difficulty of getting the Government gateway in to local authorities through lack of compliance is a further case in point. It should be mandatory for any organisation proposing electronic information sharing. Government requires this of commercial organisations; why not of itself?

The BSI Code of Practice (PD 0008) 'The legal admissibility of electronic documents' also identifies good practice and should be raised to BSI standards level, to encourage ICT product suppliers to make their products compliant.

Question 15.

Comments:

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

Question 16.

Comments: I do not believe it is clear enough, hence my recommendation in Q10. Consent is vital in our telecare example. All InMezzo products enable consent to be incorporated, and at a very granular level if desired.

Question 17.

Comments: In telecare, clearly, as it is a primary function to respond to emergency situations over which the citizen has no control, where it is essential that there is an emergency override on access controls. All such overrides are reported in the audit trail and compliance officers can be alerted in case of misuse.

Question 18.

Comments:

See answer to Q5. Certainly patients should have much more control over NHS information sharing than just yes or no. Medications and addictions can be very sensitive information that should not be shared with all participants in a collaboration.

Local authorities should move towards making available all information they hold on a citizen to him (only) through their web sites, but this will mean careful authentication, authorisation, and a lot of applications integration. InMezzo provides a registration and authentication product to enable this.

Question 19.

Comments: The code of practice seems thorough but, as suggested, compliance should be mandatory before at least government organisations are permitted to share, and it must be enforced by the system.

## **Section 5: Technology**

Question 20.

Comments: Referring particularly to InMezzo's innovations, we provide a security management framework that enables a) easy integration of diverse applications b) a hub based approach for easy information sharing and collaboration across business boundaries c) identity management of employees and subjects (customers, partners, suppliers etc) d) policy management to enable the management of change e) federated authentication to enable unlimited collaborations f) attribute based authorisation to enable highly personalised and granular access controls, f) management control of information sharing policies g) open ended solutions that avoids having to re-engineer legacy applications to enable information sharing h) a methodology for managers to develop consistent, visible collaboration policies i) control of outsourcers and third party remote access to business critical systems

Question 21.

Comments: Yes, it should mandate openness in information sharing policies and ensure they are enforced, as suggested. However, mandating particular standards for encryption is not sensible because it will be quickly out of date and inappropriate to many requirements. We should avoid identifying technologies and solutions in formulating law, because they will change: the law is for regulating sensible behaviour.

Question 22.

Comments: InMezzo see the key issue as business system security, and policy driven authorisation, which is enforced and audited. This is because government

(being so big, it needs to control both internal and external security) should enforce a 'need to know' access regime and make sure it is enforced, particularly when information sharing.

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

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

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

Question 27.

Comments:

The issue of information sharing needs to be thought through by politicians and senior executives much more carefully, considering the security management, consent and compliance capabilities, the flexibilities and manageability they will need to ensure the public will trust the outcomes. The technologies that best fit should be identified early in the process so that requirements and architecture work together in parallel. All the existing disasters have been caused by someone dictating a business requirement when the technology was not available (NPfIT access management) or a technology selected without a clear articulation of the business need (Government Connect).

Government should focus first on the operational needs of local government, and how to help them a) get their data cleaned up, b) get some decent level of access controls in place and c) integrate their many and diverse applications. The current focus on collecting data centrally is almost a complete waste of time as it will be so inaccurate and out of date that it will have no value. It is also diverting resources (skills and money) from the many things that need to be done. For example, we must have nearly spent the £12Bn on NPfIT by now but still use hundreds of acres of warehouse space to store paper based patient records. Most hospitals would surely have got this under control by now if CfH had not prevented them. Local government generally lacks the skills required for integration and information but central government ICT is continually making demands on them without getting down to really helping them. (It is good to see this improving at GC recently).

Question 28.

Comments:

Three more big questions arise that need to be addressed:

a) contact management centres are usually manned by junior staff but need to view a wide range of information that can be quite sensitive in order to offer informed responses. The technology is too often seen as providing the integration functionality required, but should not, because CRM systems have little or no concern for security. Security management should provide a single point of control for each organisation. Contact management systems should come within its bounds also.

b) Outsource organisations need to be carefully controlled. It is too easy to think you can delegate the operation of all your complex IT systems and all the responsibilities go with it. Not true: if your business is heavily dependent on IT then you need to ensure it is well managed. Your outsourcer may well be a very large company managing your systems remotely possibly from abroad. What personal information about your citizens, customers etc can they gain access to and misuse without your knowledge or control?

c) Contractors fill many government posts, work intermittently in different roles and departments. How do you manage their access rights accurately when there is such huge churn, in a cost effective manner?