

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.

The Institution of Engineering and Technology (IET) is the largest engineering body in Europe with more than 150,000 members world wide of whom approximately 25% work in ICT. The IET acts as an independent and authoritative voice for the profession, and aims to provide policy makers and the public with reliable and factual information.

The IET has responded to questions 4, 20, 22 and 27. We also draw your attention to our letter to Professor John Beddington, Government Chief Scientific Advisor on the subject of Information Assurance

<http://www.theiet.org/publicaffairs/submissions/sub798.pdf>

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

Question 2.

Comments:

Question 3.

Comments:

Question 4. As mentioned in the introduction, there are wide variations in the scope and methods of personal information sharing. What scope and what methods, in your view, pose the greatest opportunities or risks? Please explain the reasoning behind your response.

Comments:

There are broadly four business scenarios which require data to be shared. Each presents different opportunities but also different levels and types of risk.

1. Transaction based sharing. One stop citizen service transactions requiring data from one or more departments, agencies or private sector organisations to accumulate reference facts. Examples: Benefit entitlement assessment and Vehicle licensing.

This pattern presents very significant opportunities for improved service delivery and cost reduction but the risks of error are correspondingly high due in large part to poor data quality in most public sector systems.

2. Case management sharing. Accumulation of information, from many departments or agencies, to build a consolidated picture of case facts, often over a relatively long time. Example: Criminal Justice case management – the virtual case file. Intended to provide different views of data for different classes of user e.g. Victims and Witnesses, Courts, Police and Solicitors.

This pattern presents significant innovative opportunities for cost savings, greater efficiency and improved service delivery. Multiple risks are presented by poor data quality, unwanted inferencing from accumulations of data and exposure of restricted systems to the internet.

3. Research, audit and system testing. Relatively large volumes of information extracted from one system and imported to another, with the objective of examining patterns and trends and also testing new system developments. May involve multiple data sources (as in Pharmaceutical research); or single data sources for audit sampling. Requests for sharing are often made on an ad hoc basis.

This sharing pattern is considered to be essential for effective control and management of public sector services but also presents high risk of uncontrolled information exposure through data loss. New standards and procedures need to be put in place.

4. System application and data sharing. As in the propositions for shared services; a single IT resource being shared amongst many departments with similar business requirements e.g. Finance, HR, Procurement or CRM.

This pattern presents huge opportunities of greater efficiency and effectiveness in the delivery of public sector services while at the same time presenting moderate risks from a number of causes but with ample opportunity for risk mitigation.

We have considered our answers to questions 20 and 22 in the context of the identified opportunities and risks above.

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments:

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments:

Question 10.

Comments:

Question 11.

Comments:

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments:

Question 19.

Comments:

Section 5: Technology

Question 20. What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

Comments:

- Advances in the power and capability of personal computers and small servers, coupled with advances in computer networking, have led to significantly increased capabilities to share and manipulate personal information.
- At the same time, threats from hacking, viruses and systematic probing for security weaknesses have led to many well known very serious risks. The small physical size of data storage devices has, at the same time, led to increased damage from physical loss.
- Whilst strong encryption techniques, both within networks and computer storage devices, should be adopted wherever there is significant risk of data loss and personal information exposure there are other new technologies and techniques which should be considered for wider adoption.
 - Data exchange over secure networks should be preferred – GSI2 exists for this purpose
 - Improved data standards and closely aligned data models should be encouraged – as was the original purpose of e-GIF
 - Thin client, browser based user applications should be encouraged to increase the level of central control of information and to restrict user opportunity for data misuse
 - Data quality can be improved through the use of new entity analytic and resolution software techniques
 - Deployment of Mandatory Access Control as implemented, for example, in Secure Edition LINUX (as opposed to Discretionary Access Control as is implemented in other common operating systems) should be strongly encouraged for server based systems. This type of access control demonstrates significantly improved protection from hacking, viruses and other forms of systematic intrusion
 - Trusted Guard technology, as implemented by the US Department of Defense for example, should be considered for the intelligent protection of secure data stores.
 - Layered, service protocol based architectures (as in Service Oriented Architecture – SOA) should be considered for improved isolation and protection from illicit and systematic probing. Message queue protocols between service layers are also useful.
 - Blade technologies, coupled with onboard layer 2 – 7 network switching and deployment of Storage Area Networks can assist with cost effective physical separation of shared resources
 - Portable personal computing devices should use locked down, function restricted operating systems (LINUX is useful here). Ports should be disabled and any abuse or departure from normal operation should result in permanent and irreversible shutdown. Data storage devices should use hardware and software encryption as appropriate together with protection from physical intrusion.

Question 21.

Comments:

Question 22. How, in your view, could ‘privacy enhancing techniques’, such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research?

Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

Comments:

There is no doubt that such techniques can be useful, particularly for research and audit sharing patterns. The technologies are well established but not widely deployed in UK government. The use of anonymisation and pseudonymisation techniques on their own is not sufficient. Assured entity resolution together with operating system and network security measures are also essential to support these more advanced techniques.

It is also important to educate business users in the (non-intuitive) nature of these techniques to ensure their usefulness.

Software deployed to clean data across multiple repositories and produce a “master data” source should use these techniques where possible and where identity information is held for reference.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27. Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering?

The following is the relevant excerpt from the IET’s Position Statement on Information Assurance dated February 2008.

EXECUTIVE SUMMARY

Independence of the Information Commissioner

1. The Commissioner’s organisation should be funded separately from the Government of the day and thus be seen to be clearly and unambiguously independent of the Executive.

2. To reinforce independence, the Commissioner should be appointed directly by Parliament for an extended term of office, say, seven years.
3. The Information Commissioner should be properly resourced to give good customer service.

IA Standards and Delivery Capabilities

4. The National IA Strategy recognises the need for stronger IA standards and delivery capabilities, but it does not acknowledge the magnitude of the task and the need for sustained strategic action.
5. IT systems that protect highly sensitive data (such as health or financial records for millions of citizens) need a level of assurance greater than that required for many safety-critical systems. This is because they need to resist systematic and intelligent probing for possible vulnerabilities.
6. Very few people have the skills, methods or tools that are essential to develop highly assured software. Those purchasing software have a duty to ensure that those skills are available within the supplier company and that they are employed.
7. The National IA Strategy needs to recognise this market failure and to take strategic action to ensure that in five or ten years time it will be possible to procure IT systems that can adequately protect highly confidential data (such as the health records or financial data of millions of UK citizens). Until this time, the IA Strategy should state that it would be most unwise to assume that datastores containing large concentrations of confidential data can be securely connected to widely accessed networks without unacceptable (and unquantifiable) security risks.

Educating Society

8. The benefits of electronic commerce, electronically delivered government services and the social benefits of electronic social interaction will never be realised unless everyone has some basic, jargon free understanding of the core principles of information assurance in the information age. Until Society reaches that state, no amount of job based education will ever prevent the lapses in basic procedure that have been well publicised in recent months.

INDEPENDENCE OF THE INFORMATION COMMISSIONER

9. The IET proposes that the Commissioner's organisation should be funded directly by Parliament or in some other way that is clearly and unambiguously independent of the Executive. The Commissioner should be a 'people's advocate' and should not remain in the invidious position of always looking over his shoulder with respect to the next year's budget.
10. At present the Information Commissioner's function is funded partly from government and partly from the fees collected through the data protection registration process. This registration process, of itself, has little point and should be replaced by a requirement for organisations to publish on their websites the details that they are currently required to register.
11. The Commissioner should be properly resourced to give good customer service rather than running the extensive backlogs of cases as a result of excessive budget constraints. This has sadly become the norm in the 'Freedom of Information' (FOI) area. For

example, in March 2007 the ICO had 147 Freedom of Information complaints over nine months old that had not even been assigned to an investigating officer.

12. To reinforce independence, the Commissioner should be appointed directly by Parliament for, say, a single seven-year term.

INFORMATION ASSURANCE STANDARDS AND CAPABILITIES

13. The National IA Strategy recognises the need for stronger IA standards and delivery capabilities, but it does not acknowledge the magnitude of the task and the need for sustained strategic action.
14. Making IT systems secure is a greater technical challenge than making them safe. This is because security-critical systems have to resist systematic and intelligent probing for possible vulnerabilities whereas most safety-critical systems only fail because the conditions that trigger failure occur by chance during their operation, IT systems that protect highly sensitive data (such as health or financial records for millions of citizens) therefore need a level of assurance greater than that required for many safety-critical systems.
15. It is widely understood by computer scientists and software engineers that testing software is a wholly inadequate way to establish high reliability. In particular, testing is almost useless as a way of showing that software does not contain the sort of obscure errors that lead to breaches of security. (This is an inescapable consequence of the nature of digital systems, which may exist in billions of logically different states).
16. Unfortunately, very few systems companies (and even fewer in-house software teams) have the skills, methods or tools that are essential to develop highly assured software. As a consequence, any systems that are built from commercial off-the-shelf (COTS) products are highly likely to be insecure (and certainly cannot be shown to be secure).
17. A recent study for the US National Academy of Sciences¹ concludes that there is a need for stronger software engineering methods, which are soundly based on computer science and mathematically rigorous. Such methods do exist and they have been shown to be practical and cost-effective² but the methods are not yet widely adopted by software developers.
18. The National IA Strategy needs to recognise this market failure and to take strategic action to ensure that in five or ten years time it will be possible to procure IT systems that can adequately protect highly confidential data (such as the health records or financial data of millions of UK citizens). Until this time, the IA Strategy should state that it would be most unwise to assume that databases containing highly confidential data can be securely connected to the internet without unacceptable (and unquantifiable) security risks.

EDUCATING SOCIETY

19. Security of personal and confidential information within the domain of computer systems

¹ Software for Dependable Systems: Sufficient Evidence? http://www7.nationalacademies.org/CSTB/project_dependable.html

² The US National Security Agency carried out a recent experiment that showed this, described in <http://www.praxis-his.com/pdfs/issse2006tokeneer.pdf>

has become a critical issue for all. Recent losses of personal data and the rise in identity fraud attract a large share of journalistic attention and we are bombarded with advice from every quarter. But most of what we read, beyond a superficial level, contains incomprehensible technical detail and impractical recommendations.

20. Before computer use became the norm, information assurance was simply a matter of managing filing cabinets and the documents within them. The words 'Confidential' or 'Secret', 'Do not Copy', 'For xxx's eyes only' make intuitive sense to us all. Information was assured by the using trained personnel, rigorous lock and key management and the ultimate threat of dismissal or even criminal proceedings.
21. A physical intrusion into a locked cabinet is quickly detectable. However an electronic intrusion may go undetected for ever. Today, the complexity of computer security techniques has led to the state where only a handful of technical specialists have even the remotest idea how to handle the computer equivalent of the locked filing cabinet.
22. The recently reported breaches of information security of personal information within both public and private sectors demonstrate well this lack of basic awareness and understanding. Not only were the procedures inadequate but also the volume of exchanged information was inappropriate.
23. The CSIA Information Assurance Governance Framework, published on 22 November 2007 discusses awareness, education and training on pages 37 – 38. It is aimed at "the general population of users" with an implied tacit assumption that those users are within the civil service and its subcontractors. It correctly identifies the need for 100% coverage of basic education for the whole of this population, not just IT staff. It stresses the need for the establishment of a security culture rather than just providing information. It insists that programmes must include refresher courses to be effective.
24. Such awareness and education must not be seen to be the preserve of the civil service alone. It must extend to all employees in all sectors and to their families. Embedding an information assurance culture needs to be started in our schools and colleges well before employment age.
25. We need to approach, very rapidly, the state where society is as familiar with the risks arising from careless handling of electronic information as it is with paper based equivalents. We need to be able to react intuitively to issues and problems as they arise and to know when our actions are likely to tip us into a risky situation.
26. Until everyone has some basic understanding of the core principles of information assurance in this information age, the huge benefits of electronic commerce, electronically delivered government services and electronic social interaction will not be realised.

Question 28. Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

Comments: