

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: Our fundamental interest is that only through data sharing can our finite resources be used to target the most vulnerable in our society. In addition, Cheshire Fire & Rescue Service enters over 50,000 properties in Cheshire Warrington & Halton every year to undertake safety checks. We aim to undertake these checks in the properties of the most vulnerable from fire. These same individuals often have social needs, health needs, drink or drug problems etc. We feel that it is essential that these people are provided with links to other agencies who can deal with the wide variety of their issues. Therefore, we have entered into data sharing agreements with organisations such as Social Services and Age Concern which with the homeowner's permission allow us to undertake and share the information from a wide ranging contact assessment

As a Fire and Rescue Service looking to implement innovative working to a modern agenda with partners, we perceive that there are 2 main requirements to improve information sharing

- There is a need for clarification of the perceived barriers to data sharing amongst organizations in order to give individuals and organizations the confidence which will enable the benefits of data sharing to be delivered,
- There is a need to ensure that processing, monitoring and security for personal data is improved in order to detect and deter future failures

Overall, while we believe the benefit and public good from sharing data must be progressed, we accept that in general current standards are inconsistent and open to failings, which will

damage privacy and confidence if not adequately addressed.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- What kinds of personal information do you collect, hold and share?

a) Cheshire Fire and Rescue Service collect data and supply from public and private partners about individuals who may benefit from or need our own or partner services. The information is presently restricted to contact details (name, phone number and address) for referrals where possible, and normally supported by consent. This includes data on children and young people, the elderly, and other vulnerable groups.

b) Information is collected and supplied with the Police relating to arson and Road Traffic Collisions, under the Crime and Disorder Act. This data can include incident details, findings of investigations, previous suspected crimes and history in addition to the contact details.

c) Information is supplied to us by the Domestic Violence team in the form of violent marker flags, and by Air Products to identify the locations of oxygen cylinders. In addition some case details are shared, where there is an identified risk from fire and fire prevention work can be undertaken.

d) Internal payroll data is supplied to our data processor.

- How do you collect, hold and share such personal information?

The information is supplied and held in various formats depending on the urgency of the case, and the format and sensitivity of the information. We use a number of methods to transfer data including –

- VPN supported by security token
- Secure e-mail
- Encrypted email
- Personal collection of encrypted CD ,
- Verbal communication at case conferences,
- Email, telephone and radio during incidents.
- We plan to implement secure access to the web based shared Social Care and Health Single assessment Process (CSAP) database.

We are conscious of the privacy and security risks arising from personal Data Sharing, but also recognize the need to balance this with our duty to target the delivery of public safety, to people who may not be aware of their level of risk to fire and injury. We restrict our employee access to information using technology and organizational controls, and generally only share information where we have consent, or meet another DPA conditions of processing.

- For what purposes do you collect, hold and share such personal information?

Information is shared in order to deliver services to those who require them, to improve our services, to deliver services in an effective and efficient manner, to reduce the number of fires and deaths and injuries resulting from fires in homes, to prevent and detect crime.

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

Question 2.

Comments: In 2005, four out of the five fire fatalities in Cheshire, were individuals who were known to “other agencies”. This situation has been repeated in 2006-2007, and so far we have had 4 fatalities – all of which were known to “other agencies” A referral from other public agencies for a Fire Home Safety Assessment may have resulted in reduction in the number of fatalities.

We have examples of individuals who have benefited from contact assessments by not just being safer from fire but also getting more benefits, help with cooking & gardening, help shopping, help keeping mobile and assistance in remaining active and independent in their own homes

a) Individuals can benefit from improved services, response time and targeting, easier access to other services, reduce the duplication of supply of data, coordinated service delivery, joined up services.

Examples have been widely reported for example through the Soham and Climbie inquiries where the safety of vulnerable individuals was not prioritized above the possible privacy issues.

b) Society will benefit from improved targeted interventions rather than “blanket cover” which should mean reduced risk, for example less fires and injuries, and hence reduced demand for public resources, including partner agency resources such as Police and Health.

Information sharing will enable a preventative approach and holistic care, helping to support older people in their own homes for longer in support of the LAA agenda.

Early identification to allow intervention with individuals involved in crime or anti social behaviour can reduce the risk of increasing crime and corresponding penalties.

In order to further develop shared services, and maximize use of resources it will be necessary to share data, in order to manage processes and activities.

Question 3.

Comments: In 2005, four out of the five fire fatalities in Cheshire, were individuals who were known to “other agencies”. This situation has been repeated in 2006-2007, and so far we have had 4 fatalities – all of which were known to “other agencies” A referral from other public agencies for a Fire Home Safety Assessment may have resulted in reduction in the number of fatalities.

We have examples of individuals who have benefited from contact assessments by not just being safer from fire but also getting more benefits, help with cooking & gardening, help shopping, help keeping mobile and assistance in remaining active and independent in their own homes

a) Individuals can benefit from improved services, response time and targeting, easier access to other services, reduce the duplication of supply of data, coordinated service delivery, joined up services.

Examples have been widely reported for example through the Soham and Climbie inquiries where the safety of vulnerable individuals was not prioritized above the possible privacy issues.

b) Society will benefit from improved targeted interventions rather than “blanket cover” which should mean reduced risk, for example less fires and injuries, and hence reduced demand for public resources, including partner agency resources such as Police and Health.

Information sharing will enable a preventative approach and holistic care, helping to support older people in their own homes for longer in support of the LAA agenda.

Early identification to allow intervention with individuals involved in crime or anti social behaviour can reduce the risk of increasing crime and corresponding penalties.

In order to further develop shared services, and maximize use of resources it will be necessary to share data, in order to manage processes and activities.

Question 3

What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

a) We recognize that the risks for individuals include potentially detriment arising from security failures -

- Loss of privacy,
- Decisions influenced by data which may not be accurate or appropriate for that purpose, and
- Loss of trust where individuals cannot identify and understand where their data is held and for what purpose.
- Identity fraud

Examples include the recent HMRC and Defence data losses, and other instances of identity fraud.

b) The risks for society are potential loss of trust from the individuals, which could cause withholding of data or opting out of necessary services. Anecdotal evidence suggests that where data collection is seen not to be justified, then data subjects will opt out or provide inaccurate data.

Society will also face the risk that privacy will be disregarded in order to deliver services. It is important to balance individuals’ privacy with the wider public good, and ensure that a risk assessment considers the risks and controls available before instigating data sharing.

The nature of modern Fire Service work means that we are aware of some vulnerable people who not only pose a risk to themselves but also to their immediate neighbours, and to our own employees. This information must be shared with other agencies whose staff could face similar risks, and with agencies that can help the individuals concerned.

This also requires us to make the public aware of the many advantages to them from sharing of their data.

We believe that fear of risk often leads individuals and organisations within society not to share data. Clearly both fear the risk of financial and reputation damage. The danger for society is that the fear of this risk will result in at worst another Climbié case or even at the other end of the spectrum people just not getting the help they deserve.

Question 4.

Comments: Recent data losses have clearly demonstrated that some methods and actions of transferring data are inadequate in terms of security. With all data handling there should be an appropriate package of controls to reduce those risks, identified by a robust risk assessment. We suggest that guidance on data security is available through the ISO information standards and from the Information Commissioners Office for example.

From our experience within our sector we would comment in broad terms that -

- Access to shared databases provides valuable targeting opportunities and efficiencies and technological and organizational controls can be implemented in order to manage the risks.
- Adhoc data sharing that is not documented or risk assessed, carries a higher risk of security failures. This may occur through lack of awareness on the part of individuals, or be intentionally motivated in order to circumnavigate what is seen to be unnecessary bureaucracy.
- Information is shared verbally or by email where dynamic responses are important. This meets an urgent business need, but may result in a lack of evidence or due consideration and safe processes for data handling.

However we suggest that the balance to be struck between benefits and risks is different in these “urgent” cases where risk to life is usually concerned. The issue for organizations is to ensure that these decisions are taken correctly, and that lack of knowledge or lack of provision of systems and processes is not the primary influence.

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments: In order to target initiatives and manage our “customer relationships”, it would be beneficial to have access to an up-to-date complete data set of local residents. The Council tax list and complete electoral roll would be of benefit, but the lack of clarity in guidance mean these are not consistently released.

For example recent guidance from the Information Commissioners Office stated that – “the legal advice given to the ICO in 2000 and since taken as read by many in local government was 'probably at the restrictive end of the spectrum' and that his Office 'had probably moved on'.”

However due to the complexity of the legislation, and lack of expertise within some organisations, it is difficult to alter or revise existing policies.

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments:

The DPA provides guidance on how to handle data, and provides a route for enforcement.

The weaknesses

It was implemented prior to the rapid development in technology, information, and need for data sharing which is part of current business practice.

It is open to interpretation and provides guidance and principles, but does not determine the level of actions which are essential and which are optional. This causes confusion and deters organizations from establishing data sharing, and conversely may result in individuals/organizations not applying adequate standards.

The notification requirement is currently a generic form grouped by data classes. This does not provide clear information to the public to enable the individual, or an enforcing body to monitor. Notification could be developed to require organizations to be more specific as to their activity, and this would support the DPA requirement for Fair Processing. This would have some similarity to Freedom of Information publication schemes, where the public and the ICO can refer to a public record for broad based information classes and examples.

The penalties for deliberate non compliance and poor management are not a strong deterrent, nor are they widely publicised or accepted throughout all levels of organizations. We have concerns that media reports suggest that there are no powers to take action following the recent data losses, despite basic failings in security procedures.

The Freedom of Information Act was introduced after the DPA. There needs to be an assessment of how well the two acts work together or overlap and contradict each other, for example when senior managers earnings become public interest and overrides privacy.

There is no statutory requirement which would raise the profile and ownership for data security, such as inclusion in the audit programme, or a statement within annual reports or business plans, or the requirement to have a similar role to the Caldicott Guardians in the Health sector.

Question 10.

Comments: We believe that organizations are generally aware of the need for data to be processed for one or more lawful purposes, and not to be further processed in any manner incompatible with that purpose or those purposes. We suggest that the interpretation of this principle is difficult, and that realistically only DPA officers have this level of knowledge. Given the increase in technology and quantities of information there is a need for simpler guidance for the majority of employees. We also suggest that more effective support, monitoring and enforcement is required.

We recognize the value of compatibility of additional uses of data, but see it is open to interpretation, and would benefit from clarity. Broad groups or principles relating to the conditions of processing could be developed as guidance. In addition we support the more recent views and guidance from the Information Commissioners Office, which look at whether there is any "detriment" and any private information in deciding whether data is regarded as personal data under the DPA.

Question 11.

Comments: Barriers to the effectiveness of the DPA are the reputation and profile, as the DPA is commonly regarded as a bureaucratic obstacle. The DPA was created before the changes in business requirements and development of technology.

This is reinforced by the format of the legislation which is dated and open to interpretation rather than detailing specific requirements.

Finally there is a lack of monitoring and accountability for data security risks and breaches. This results in a lack of individual and organisational confidence in the DPA

Question 12.

Comments: We would support the Justice Select Committee proposals for a package of measures for enforcement to protect data and to strengthen the criminal penalties for significant security breaches. This could include a requirement to report losses of data, increased penalties for reckless or repeated significant security breaches, enforcement powers including monitoring by either the Audit Commission or the Information Commissioner. This would be in line with the enforcement of the Regulation of Investigatory Powers Act (RIPA). We found the RIPA regulatory visit supportive and informative.

We query whether the powers of the Information Commissioner have been sufficiently ranging and proactive. We refer in particular to his warnings during 2007 of the dangers of extensive future security breaches and of what the acting Chairman of HMRC has now admitted were "systemic" failings in the handling of personal data.

This apparent lack of some organisational commitment or control could be resolved if the DPA required roles of Data Guardians, in a similar function to the Health Caldicott Guardians, at a suitably senior level, in addition to independent external monitoring and enforcement powers.

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments: The DPA includes conditions which refer to the need to take consent and ensure "Fair Processing". We believe that we now understand our obligations clearly, but our knowledge has grown over a period of time. This is due to additional guidance issued by the Information Commissioners Office and from working in partnership with other agencies which rely heavily on personal data, and seem to be more advanced in their approach.

We would agree that the subjects of consent and Fair Processing are not always clear, and guidance should be simplified and updated

Question 17.

Comments: Gaining consent may cause several issues –

- a) Organisations may feel the need to provide evidence of the consent in the form of retaining and accessing large quantities of mainly paper documents
- b) It will be necessary to ensure that clients understand what they are consenting to /signing for.
- c) There is a cost in establishing procedures to allow people to opt out at a later stage
- d) The cost and administration of gaining consent in traditional paper signature form may deter organizations from following requirements.

Question 18.

Comments: While guidance is available on information sharing from a number of sources, such as the ICO, the Management Of Police Information, the Every Child Matters Information guidance, ISO standards for Information security, there is no requirement to implement the guidance proactively, and no clarity as to which guidance to follow. It would be useful to have a broad framework like the ICO Information framework, supported by more detailed data class based guidance.

The DPA notification seems to be an underused facility, and could be developed to drive more detailed information about data sharing, access rights and retention periods.

Organisations could be required to provide leaflets and summaries on web sites which improve the transparency of data sharing activity.

If these proposals were adopted, there would then need to be appropriate monitoring and enforcement powers to ensure compliance.

Question 19.

Comments: The ICO framework provides clear overarching advice and has benefits as a framework. We suggest that there should be a requirement to follow this, and some means of future monitoring. There needs to be more publicity to raise awareness of this type of guidance, as in our experience colleagues can be uninformed.

We believe that more detailed requirements will still be necessary in practice.

The ICO framework recommends that each organization develops their own Code of Practice. This has the potential for inconsistency and excessive bureaucracy which could lead to many Codes of Practice being applied to a single data sharing activity. We suggest that the framework could require an appropriate existing Code of practice to be applied where possible.

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December (www.ico.gov.uk)?

The Privacy Impact Assessments are comprehensive and will be of use. Again we note that there is no requirement to use them, no monitoring, and to date little publicity and awareness.

Section 5: Technology

Question 20.

Comments: Developments in technology mean there are now various measures which can be implemented to improve data security. However this is not consistently applied, which causes issues for cross organizational working.

The provision and availability of technology alone was not effective in preventing the loss of data by HMRC. This reinforces the need for a package of organizational, procedural and technological measures, including senior management responsibility for security of information, and effective external monitoring and penalties.

Senior and executive managers are not necessarily experts in technology, and some may not accept or understand the need for

In some sectors and smaller agencies the responsibility for technology may not be fully funded or accepted at senior level.

Question 21.

Comments: There is benefit and consistency in clear guidance for technology and organizational matters. Whether it is possible to mandate specific standards in all instances is difficult to comment on, but a requirement to risk assess and adopt a suitable package of measures would seem reasonable, with specific minimum examples where possible.

We see encryption as the last line of defence and there is a more pressing need for adequate robust IT security procedures and policies, access restrictions and educating staff and management.

An explicit requirement to meet defined standards would assist organizations to meet security standards without feeling obliged to make judgements based on costs in the interests of the taxpayer.

Question 22.

Comments: We support the use of these techniques where appropriate. We have made limited use of this, but are aware that it is relevant in other sectors

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments: The impact of partnership working, and the role of modernization means that traditional areas for Health and Social Care are now areas where Fire and Rescue Services work. In addition the Local Area Agreements require agencies to work together to deliver improvements to communities in a cross cutting manner. This means multi agency delivery, requiring data sharing to plan deliver and performance manage. Legislation has not taken account of this, and guidance requires updating.

There is also a more general need to increase data sharing for all the reasons given within this consultation response and to achieve the potential benefits to society in targeting our resources at those most vulnerable in our communities.

Question 28.

Comments:

