

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:

Cornwall County Council holds various personal data ranging from social care records to consultation responses. It processes personal data as per the 12 purposes in the standard local authority template. The reference for the Council's notification is Z5464625.

Data is collected through various means, face to face, third party, collection forms, telephone, Internet, Email, depending on the purpose.

Examples:

- The Council is actively involved in Partnership working with Health and Police
- The Children, Young People and Families (CYPF) department shares child records (basic details only) with the Health Service (Child Health Department and Primary Care Trusts)
- Child record data is used to populate the national ContactPoint data base. This includes demographics and practitioner involvements, though strictly no case data.

The national system will be used to allow authorised children's services practitioners to identify who else has been working with a child. Data will be drawn from existing local authority systems. Other child agencies including Health, Connexions and the Voluntary Sector will also become a data source.

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

Question 2.

Comments:

A – Individuals

- Improved service delivery
- Respond to problems quickly, using the correct expertise
- Improve the safety of an individual e.g. in social care arena
- To plan policy and identifying trends
- Accurate provision of services to individual e.g. ensuring benefit take up is accurate

Examples:

A key benefit to individuals and to society is the planning of sufficient school capacity, based upon child data collected by GPs and hospitals

Data sharing via Contact Point will speed up identifying children's needs, planning single assessments and delivering services and outcomes. Efficiencies should allow practitioners to spend more time working with children.

B – Society

- Cost effective
- Fraud Prevention
- Crime reduction

Question 3.

Comments:

A – Individuals

Information may be:

- Used maliciously, e.g. for crime
- Used inappropriately
- Incorrect when transferred
- Lack of control over where the data is sent
- Lack of control over how data is processed once it is sent out
- Transferred without the knowledge of the data subject
- A risk assessment should be completed each time that data is shared

Privacy of the data subject could be at risk

Information not adequately safeguarded by the third parties

Increased sharing leads to a multitude of small pockets of information

Example:

The Information Sharing and Assessment agenda requires consent for sharing data in nearly all cases of intervention. Inappropriate sharing risks undermining this fundamental element of the process.

B – Society

- Loss of confidence in organisations
- Hacking big data stores for criminal purposes
- Possible for data matching to take place, and increased surveillance/interference in public lives
- an organisation may rely on data from another organisation without having any control over whether the data is up-to-date or is rigorously validated

Question 4.

Comments:

Opportunities

- Using new technology to bring information together for positive purposes e.g. contact point, child protection, law and order
- Using information to provide effective services to service users, in particular those that are vulnerable or unable to identify themselves

Example:

For ContactPoint, Data sharing is to be managed through encrypted files and from 'system to system' eliminating risks posed by use of external organisations (couriers etc)

The only information to be shared is that actually required. Ancillary data is to be eliminated from shared files.

Risks

- Partnerships
- Partnership working and data sharing which relies on consent, rather than legislative support
- Transfer of bulk data, rather than on a 'need to know'
- Storage of bulk data presents a higher risk for hacking, therefore more people will be affected than should the information be stored on a 'need to know' basis
- Increased number of information sharing protocols and agreements to govern the information sharing causes confusion

Question 5.

Comments:

Public Authorities possibly hold too much data, due to their diverse activities and the levels of control that need to be in place to regulate data collection are costly.

This is unlikely to be challenged, unless a complaint is received. In terms of risk, for the whole of the Public Authority this is not deemed high and the penalties are relatively low.

A lack of Public awareness when completing forms leads to organisations potentially collecting information from individuals when they have not fully understood the implications of checking the 'opt-in/out' boxes.

Multiple copies of information are circulated, which leads to a risk of various versions of a document being kept.

Example of too much information – the DCSF requires schools to collect information about children of Service Families. This has caused concerns amongst parents that schools are being too intrusive, especially because data is not collected about the occupations of other parents; also the Armed Forces already has this information but is not allowed to share it with the DCSF.

Example of too little information – the education service and the DCSF needs to know which children are from low income households so that additional resources can be provided and the effects of poverty reduced. The DCSF uses entitlement to Free School Meals (FSM) as a proxy indicator, but this is a misleading proxy in Cornwall because so many of our small businesses (e.g. tourism, fishing, and farming) are disqualified from claiming FSM because they are self-employed.

Question 6.

Comments: Potentially as per question 5

Question 7.

Comments:

Information sharing between the County Council and District Councils e.g. for financial assistance for disabled service users. It was not known to the individual when their information was collected that this information sharing would take place. As there is no statutory power to share, it would rely on consent.

If an individual moves house, they may alert the district council that their address has changed but this is not automatically shared with the county council, or other departments within the organisations.

It would be very helpful for planning purposes if the health service would provide information about pre-school children who are likely to have special educational needs when they reach school-age (due to physical, health or mental problems). The data is not shared because of confidentiality concerns (e.g. patient-doctor confidentiality) and the belief that the Data Protection Act does not allow it. A change in legislation, that allows sharing of data for very specific purposes, would help.

It would be very helpful if the Department for Work and Pensions/Tax Office would provide the DCSF with a low-family-income indicator for each child, because the currently used FSM proxy indicator is misleading. The DP Act prevents sharing of data between government departments in this way.

Information sharing between the Local Authority (Children's Services) and the local register for births, deaths and marriages would be advantageous. This would help clarify new births as a check against health data and incorporate the early identification of child deaths.

Question 8.

Comments:

From our Local Authority perspective, there is no information sharing taking place which we know about that causes concern. We have information sharing protocols in place where information sharing is identified. The difficulty is identifying all information sharing which takes place.

Section 3: The legal framework

Question 9.

Comments:

We think that the DPA works reasonably well.

Strengths

- Gives an individual rights in respect of what organisations can/cant do with their data
- Promotes openness with a data subject

Weaknesses

- There is more to the legislation than just subject access requests. Getting the control into a diverse organisation for all of the eight principles is an ongoing challenge.
- Staff don't understand what legislation supports their work
- There is no definition in the act of the level that you need for the term 'specified'. E.g. information could be collected from a service user for the purpose of 'social care provision' or 'a single assessment'.
- Subject access requests are allowed to be too broad and this can impact on an organisations ability to carry out daily functions. If we are to continue with allowing clients to submit such broad requests, there should be a costing mechanism attached with that
- Staff don't understand the term 'incompatible' and allow sharing in the widest sense.
- Not enough enforcement – ICO should have stronger powers in respect of persons who breach the act
- There should be an auditing system of the data protection principles to ensure compliance.

It should be made mandatory that organisations document the legal basis for capture and information sharing.

It should be mandatory for organisations to produce an information flow-chart to show how information is being shared and stored. This should be made available as part of subject access requests.

A weakness of the DP Act is that it appears to prevent the sharing of data between government departments even where there is a valid purpose that would benefit the individual. A change in legislation, that allows sharing of data for very specific purposes, would help.

Question 10.

Comments:

Our Council currently identifies the purposes for which information is collected. There are no corporate checks to assess whether the information is in fact used for any further purposes.

Cornwall County Council places as much importance on complying with the second principle, as much as any of the others. The second principle enforces the first, in placing importance on informing the data subject of the purposes for which their data is processed. It also means that the decision about how and why the data will be used must be made before the processing takes place.

Question 11.

Comments:

Historically, "Government" has been made up of separate legal entities covering central departments, local government, police and health for instance. Given the technological advances, it is now possible to join up "Government" and in doing so remove the legal barriers. By classifying "Government" as one organisation, you would remove the need for information sharing protocols and/or agreements for a given "Government" purpose e.g. social care is currently part of the remit of Local Authorities, Department of Health, Department of Children, Schools and Families. There would only be one data controller and there would be the potential to create one database for all participants to access. So for instance, projects like 'Contact Point' would be the norm and would have been constructed without the issues which are being faced now. Careful consideration would need to be given to what constitutes "Government".

Currently there is duplication across the authorities in respect of the personal data which they hold. By joining up "Government" it would be beneficial to create single data sets which agencies could all access and maintain to provide consistency. This would mean that retention would be consistent, along with the accuracy and the security of the data. The data sets would have set purposes agreed by the parties and the public could be made aware of and actively communicated with about the data. This would in turn reduce inconsistencies and discrepancies in data supplied as a result Subject Access Requests.

It seems that the management of data is not given enough importance by society. The public do not ask questions about how/why their data is being collected, and therefore data is collected without challenge. It is only when something goes wrong that the profile is raised and action is taken. In order for organisations to act more appropriately, people need to take more of an interest.

Question 12.

Comments:

An inspection regime is needed to enforce the rules set out in the act. While there is no inspection regime, organisations do not put the necessary resources into meeting the requirements of the legislation. This regime could be controlled by the ICO.

For Government agencies, compliance with the act could become part of the corporate performance assessment (CAA).

A tougher stance is needed in respect of the existing penalties.

Question 13.

Comments:

Question 14.

Comments:

For Government, the legislation could mandate the use of certain government services such as GovConnect, which would enable individuals to authenticate themselves in a consistent way.

By also making the use of the national data standards compulsory, data would be held more consistently and errors when sharing data would be more easily identified.

Question 15.

Comments:

Notification

Other than giving the public an overview of the types of processing that an organisation carries out, it is of no real value. There is an administrative overhead in maintaining the registration and yet it is not audited.

Partnership working

This is another area where resources are assigned to ensuring data protection is appropriately managed and it is very complex given that there can be many partners in a single partnership many of whom are regulatory.

Subject Access Requests

The subject access request process can take a lot of staff time if a client asks for 'all information held'. For example, should a social services client request 'all information held', the volume of documents will be large and often to provide a copy of all paperwork would be very time consuming. We would then apply section 8(2)(a) and invite the client in, rather than provide a copy of the information. However, the data will still need to be reviewed and redacted before allowing the client to have access. Therefore the 'disproportionate effort' aspect does not assist in a case of large volume. It would be better to have an 'appropriate limit' set by the legislation, as per the Freedom of Information Act.

Section 4: Consent and transparency

Question 16.

Comments:

If the Council was required to share data with another organisation which was collected initially because of a statutory duty, and the sharing was for a statutory duty, we would not require consent to share.

If the Council collected data for a purpose based on consent and planned to share this with a third party, then the data subject would need to be told at the point of collection. The data

subject would then be aware and consenting to their data being shared.

If the Council collected data for a statutory function and then wished to share the data for a non-statutory purpose, this would require consent.

It is best practice to inform an individual that their data may be shared, even if you are not relying on consent.

However, the above is our interpretation of the legislation in respect of 'consent'. The legislation does not go into the level of detail needed to immediately understand this. It is not clear what form of consent is acceptable. The need to interpret consent makes consensus difficult within partnership working arrangements. E.g. Partnership working on the single assessment process for vulnerable adults.

Information sharing which has powers vested in legislation, is less complicated. E.g. contact point.

Guidance from DCA on data sharing is useful, however a code of good practice which is attached to the legislation would be useful.

It should specify in the legislation what level of detail organisations are required to go into when informing the data subject about third parties with whom their data is shared. E.g. 'your information may be shared with third parties in order to provide you with this service' or 'your information may be shared with organisations X,Y and Z...'

The Council is involved in an initiative to share information with other bodies in the South West in order to carry out the single assessment process in an electronic environment. (eSap)

Question 17.

Comments:

There is an overhead to contacting service users to obtain consent and recording their response in the appropriate system. There are technical costs and managerial costs in developing a system which takes account of the individual's response to consent.

Individuals are allowed to remove consent at anytime, and should this right be exercised, then there would be a financial cost of complying with this. There is also an impact to the work which is being undertaken as consent allows an 'opt-out'. This may affect the viability of working in a particular way.

It is unclear about obtaining consent from minors, given that there is no 'legal age' for consent.

Example:

The local authority and schools have a statutory duty to provide education to every child of compulsory school age. Currently the sharing of the pupil's data (as defined by the DCSF's Common Basic Data Set) with the LA, DCSF, OFSTED, Connexions, QCA etc is covered by legislation. If the sharing of the data depended upon consent, the current system would

break down and there would be delays and patchy delivery of essential services.

When working with families consent is always sought in Common Assessment Framework (CAF) episodes unless a child is perceived to be at risk of harm. The Fraser Guidelines (Gillett Competencies) are adopted for younger children

Question 18.

Comments:

If organisations were made to document the flow of data in and out of the organisation e.g. for each record keeping system (manual or electronic) then members of the public would be able to access clear information about which third parties had access to Council data and which provide data to the Council.

We refer back to our suggestion of having a limited amount of 'master databases' which government can all access, and the public can submit a subject access request to.

All systems should be able to produce a print out from the system of all personal data held in relation to an individual.

From our current knowledge, information sharing is not currently an issue for our clients as we have had no queries/enquiries/complaints relating to information sharing.

Question 19.

Comments:

The framework COP was useful; however a template and/or inclusion in the legislation would be more effective. Guidance can be ignored. Enforcing a single framework for all data sharing would promote consistency.

We are unaware of any announcement from the ICO on 11 Dec, and a search of their website did not present the relevant documents.

The ICO should be supported with further resources.

Section 5: Technology

Question 20.

Comments:

Sharing is now easier, and because it is 'technically possible' administrators are often forgetting the governance arrangements which are in place to safeguard the information.

Data transfer can be carried out electronically by secure means now, reducing the potential for CDs to be lost.

Laptops should connect to data by secure remote log-in, removing the need for personal data to be held on the laptop's hard drive. 'Mislaid' laptops should not, therefore, pose a risk to the security of personal data.

Question 21.

Comments:

In order to prevent the legislation becoming out of date because of technical changes, there needs to be a supporting document which sets out what the 'technical safeguards' should be.

The downside of setting a specific technical standard is that it would be applied regardless of the level of risk. E.g. sole trader would have the same overheads as a multi-national organisation.

The benefit of mandating a security standard would prevent arguments regarding cost vs risk which is the current practice.

The law should mandate specific technical safeguards to protect personal information. Organisations would then have to find the funding to comply with the law; it would become more of a priority on scarce resources than it is now.

Question 22.

Comments:

If you can complete your work without the use of personal data, then this should be mandatory.

There is not sufficient advice about using these techniques.

The barrier being that you would have to build this into all processes for information sharing and enhancing guidance and training for staff.

It would be difficult to monitor compliance and to enforce organisations to use the same privacy enhancing techniques. These techniques have not been very effective in completely anonymising personal data; research analysts often combine different datasets that make it possible to deduce the identities of certain individuals, even though that was not the researcher's intention.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

In respect of the public sector:

- A review of guidance which is available re information sharing
- ICO given the authority to vet guidance before publication
- Guidance is rationalised and works across the levels of government
- There appears to be a proliferation of guidance from various sources, without an overarching framework for 'government'

There could be a single set of guidance documents for all local authorities to use.

Issue of the interpretation of data – the sharing of personal information with organisations operating in a different field has led to the misinterpretation of the data. This can occur when one organisation does not understand how the other organisation collected the data, or does not understand the limitations of the data in providing a complete picture of what has happened to an individual, how decisions were reached etc. Data sharing protocols need to include guidance on the sourcing and interpretation of the data, stating the nature of the conclusions that can or cannot be drawn from the data provided.

Question 28.

Comments:

Consultation too vague and open ending

Consultation too long

