

# 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: We own a number of products that are in use within the public and private sector to facilitate the sharing of information across organisational boundaries. Our current focus is on Health and in particular the electronic transfer of prescriptions in support of the NHS Connecting for Health Programme.

Additionally our Consultancy side of the business has been involved in the technical design aspects of the Connecting for Health Programme from the outset.

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

Question 2.

Comments: a) There are a wide range of benefits to be achieved through the controlled and appropriate sharing of information on an individual basis including; avoidance of repeating information using unsecure media (telephone, kiosk interactions etc), improved and personalised access to services, translation error reduction, better continuum of care through improved communications between professionals, faster transactional settlements and hopefully one day reduced

taxation through streamlined public services. Legitimate capturing and sharing of information in support of direct service is not an issue. The issues arise when the sharing of such all encompassing and often sensitive information is shared for reasons that are far from clear to the owner (the individual, citizen or person!). The citizen should be in control of the sharing of their own information and this needs to be done on a case by case basis rather than by blanket cover.

b) Where there is a need to protect life, detect serious crime or ensure national security the sharing of information between institutions is beneficial. Most people would have no problem with invoking national legislation to cover these eventualities. This is far from saying that this data and information should be stored or accessible on each and every individual in systems under the direct control of central government. The same society benefits could be achieved through an appropriate governance and approval process based on proving that an individual or group of individuals are posing a 'society risk'. Data could then be 'pulled' from the necessary systems in such approved cases.

### Question 3.

Comments: a) The key risk from an individual perspective is that those charged with the protection of data (lets say in compliance with the Data Protection Act) fail to do so. The outcome of this is that the information handed over in trust falls into the hands of a person or organisations that the individual has not consented to receive it. The consequences can range from embarrassment, damaged reputation, and identity theft, variable degree of personal or business financial loss to total national or international discrimination. The mass storage, collation, aggregation or integration of data across a wide range of transactional systems spanning organisational boundaries makes the likelihood of these risks being realised more frequently as has recently been witnessed.

b) The current increase in volume loss of compromising data involving large swathes of our society (25 million in the case of child benefit) could create more risks than legal information sharing was intended to address. A major risk is that this volume of 'lost data' could be used at some point in the future to exploit the information sharing culture advocated in the name of reducing national fraud, improving public services and protecting society against national security and global terrorism.

The routine mass storage of or access to individualised data by central government is extremely difficult to justify given the complete breakdown in their ability to comply with the most basic data security safeguards let alone the Data Protection Act principles.

Trust would need to be restored to provide unequivocal assurances that data captured, stored or processed would only be used for the purpose it was intended for and not used to routinely discriminate an individual or group of individuals. Even in the 'not so new electronic world' there should be complete transparency around the capture, storage and processing of personalised data.

Without adequate controls or safeguards around the protection and use of personalised data

there can be little doubt that society will find a 'work round' any national or intrusive information sharing strategy..

#### Question 4.

Comments: Information sharing at a local level in support of direct care or service provision must deliver optimum value to the citizen involved. The sharing of information between delivery partners and their staff for a specific event or episode provide the greatest opportunity to improve efficiency and effectiveness of service delivery direct to the citizen. Much has been said about the introduction of back-office shared services with variable thoughts expressed about the degree of financial savings (and reinvestment in front line services) achieved. The generalised sharing of information between front-office staff across health, social care, private, voluntary and third sectors would improve both outcomes and value for money of social Strategic Delivery Partnerships. Such information sharing can be done through secure electronic messaging based on citizen consent rather than rely on volume data transfer or paper between agencies.

The greatest risk must be the growing perception of unaccountable, uncontrolled and undisciplined sharing of information at national level under the pretext of protecting society against global terrorism or at least national security or fraud. The almost weekly loss of large quantities of sensitive citizen-centric data is undermining the trust and confidence in Government to protect our data in the knowledge that it could then be 'recycled' at some point in the future to attack the fabric of our society. There can be little justification for large national data repositories with an increasing depth of person identifiable information be this in health, benefits or other centralised agency.

#### Question 5.

Comments: As stated above it is suggested that the perception (often much worse than reality) is that Central Government has access to too much information on each individual through the increasing tendency to create a national integrated data management infrastructure.

These national systems have been designed to capture information to feed the centralised performance monitoring function rather than support direct service delivery through the front office. The controlled sharing of data at a local level (where most citizens interact with government services) would enhance the citizen experience, reduce transactional costs and significantly contribute to improved outcomes.

An increased focus on community based (localised) information sharing would also start to demonstrate that citizens are at the heart of service reforms - information sharing supporting integrated service delivery returning improved outcomes to both the citizen and society.

#### Question 6.

Comments: No direct first hand experience - we must also bear in mind that there have also been a number of high profile data losses from the private sector in recent

times.

We must be careful not to compare public and private sectors too closely in respect of the sharing of information (use of data). The public sector is being credibly driven down the route of integrating services horizontally; collaboration across departments in central government and through multi-agency working locally. This shift from the previous vertical business models will mandate the sharing of information horizontally - that is across different cultures, management structures, ways of working, performance targets. This differs from the better examples of data use in the private sector where the data including business intelligence is limited to a singular private sector organisation (vertical). Could we really see the day that Tesco will share 'their' data' with ASDA for example to help improve the shoppers experience - they both use the data to improve the financial bottom line?

The use however should not get mixed up with data management and controls. We would suggest that there may be good practice that can be shared between private and public sectors and vice versa.

#### Question 7.

Comments: To avoid repetition please refer to the example above (Q4) where improved information sharing across and within strategic delivery partners at a local level would improve citizen centric service delivery.

There are many reasons for not sharing data or information at local community level and this ranges from 'not allowed under the Data Protection Act' through cultural differences in delivery approach to 'more than my jobs worth'. There has generally been a vertical (organisation or department) focus to service delivery and data management. The data, for example, is owned by the organisation and not the citizen and that the sharing of data involves giving access to the whole record rather than restricted based on the 'need to know'. In health environments there is the added problem of sharing information across conventional boundaries where clinical context must be maintained.

With the shift to Local Strategic Partnerships involving public, private, voluntary and third sectors some of the political and policy hurdles are being eroded. This is gradually being converted into local drivers for change and the development of integrated service delivery. This multi-agency (horizontal) planning will hopefully lead to improved data sharing without the creation of additional community based data repositories. It is important that existing barriers are overcome and that the vision of integrated services is fully supported by appropriate and integrated information.

There must be a shift to enable information sharing to put the citizen at the heart of authorisation and approval processes even if this is stratified (demographic, clinical, relational (legitimate relationships)) and discipline specific where appropriate.

Question 8.

Comments: We are not aware of any such instances.

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

Question 9.

Comments: The key principles of the Data Protection Act are fine and have stood the test of time. The real issues are not with the Data Protection Act but with data management controls including IT security procedures. The main weakness of the DPA is that it is perceived as a 'tick in the box' process and that many organisations fail to link it seriously with Information Governance and Assurance. The protection and management of personalised information should be a key area within corporate internal control processes with a board level executive director nominated as the accountable officer. Personalised data should be afforded the same controls that are applied to financial systems. Compliance should be monitored in line with corporate Audit requirements and not left to the IT function.

There needs to be further alignment with ISO standards on data security and management or other industry standards (ITIL, CoBIT etc).

Question 10.

Comments: Again it is more perception than reality but with the Government's agenda including increased use of horizontal aggregated or consolidated information covering sensitive areas like ID Cards and Children's Services. The definition of processing in the context of data and information sharing across multi-organisations where accountability and ownership is blurred needs further clarification. It will be difficult to overcome the consent issues in such a complex and free flow environment.

We would suggest that the second principle is valid and protects the individual from the inappropriate processing of data. However it needs to be strengthened to address the systematic and seamless transfer of data across organisational boundaries where compliance with the individuals' 'purpose' becomes almost impossible. It is suggested that the ownership of the data remains with the individual and not the 'Government' as a whole. The individual approves access to data on an event by event basis and retains the right to withhold access without compromise or penalty.

Question 11.

Comments: The key societal barrier is the same as with any other mutual transaction...trust, confidence, respect, benefits, accountability and responsibility. It is suggested that in respect of an information transaction with 'Government' in particular these values would score very low indeed.

The barriers that stand in the way stem from having clear ownership or accountability for personal information. It would be rare that it is exposed to the same executive scrutiny as any other corporate asset and we refer you to industry standards on

Strategic Asset Management. This is not a technical but rather an institutional issue. Technical issues are addressed through IT security policies and procedures but this must be derived from the corporate direction on risk based information governance and assurance.

As stated earlier, Board ownership combined with robust internal controls are required rather than rely on IT processing functions to singularly protect the data. We have included Corporate Social Responsibility in Annual Accounts why not Data or Information Governance?

Question 12.

Comments: It is felt that the DPA is 'fit for purpose' but additional teeth need to be given to the array of functions that enforce compliance including the Information Commissioners Office. We must clearly put the citizen at the heart of Information Governance and Assurance.

Ownership must be clearly defined, accountability must be transparent and purposes must be clear and understood by the citizen. There must be a right to withhold personal information or to revoke authorisation in reasonable cases without fear of discrimination.

Question 13.

Comments: We are not aware of any directly but reinforce the argument that the issues will not be addressed by additional legislation. The underlying Information Governance and Assurance controls need to be more robust with local 'Information Supremos' being empowered to monitor and enforce compliance.

Question 14.

Comments: Not that I can see - again this would not be legislation but more robust business and technical direction that focuses on the their 'duty of care' in the protection of the citizens personal data.

Question 15.

Comments: Not that we are aware of - we would suggest that planning adequate control mechanisms up front would be far less burdensome than 'clearing' up after the loss of part of the organisations data asset. Add to this the reputational and financial loss then the 'burden' is a sound investment.

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

Question 16.

Comments: Having had extensive experience of the NHS in both centralised programmes and in acute Trusts we feel that the guidance was clear be this explicit or implied consent. There was also the supporting legislation around Access to Medical Records as well as legal guidance (Gillick Principle) in the case of young people.

The consent associated with a direct intervention can be understood or grasped but the area of consent in respect of information sharing between, say, local and central

government are more difficult. Many at local level do not understand the purposes for sharing information with central government let alone know how this data looks in the 'bigger picture' of the Governments Information Sharing Agenda!

We found a report by the Children's Rights Alliance for England titled 'Children and young people talk about information sharing - Children's and young people's views and comments on the Cross Government Guidance on Sharing Information on Children and Young People' an extremely interesting view of the citizen expectations in the next generation.

#### Question 17.

Comments: We are not sure that gaining consent is a barrier - we would suggest that it is a citizen's right to give a third party approval to share information based on understandable 'terms and conditions'.

It is reinforced that for localised interventions consent can be obtained, event by event, and the 'terms and conditions' can be explained. The credible move towards local integrated services supported by agreed care pathways could also be manageable. How do you secure a single individual's consent for the national aggregation of data when you know that they may subsequently be the subject of electronic discrimination.

#### Question 18.

Comments: Putting the citizen at the heart of Information Sharing as is the undertaking in the case of service delivery. Make custodians of data truly accountable, think whole-system and ensure that the difference between legislations, executive direction, management control and systems controls are fully understood by those providing information assurance. Information Assurance should be a key 'item' in every corporate report.

#### Question 19.

Comments: It must be remembered that the recent loss of data was not about agencies not complying with the Data Protection Act or breaching the citizen's consent 'terms and conditions' aligned to purpose.

The data appears to have been a sub-set of a much larger 'national system' where data was extracted and 'sent' to external agencies by what could be described as 'poor security arrangements'. In other cases it was about employed individuals breaching their own internal controls by storing large amounts of personal data on a portable device. Why was so much data sent in CD format or held on a laptop given the investment in creating secure IT environments including mobile?

We support both the framework agreement and the Privacy Impact Assessment in principle but would stress that much is to do with lack of ownership at senior levels. Regulatory Impact Assessments on centralised policy should clearly incorporate the impact on data management including the increased use of

aggregated data across many departments. This does not, however, address how the impact is communicated to the ultimate owner of the data (the citizen) and how they may suffer as another part of the 'bigger picture' is approved or implemented.

We would suggest that the Data Management impact assessments are conducted by a cross-party agency with objective assessors. There is an urgent need to detach personal data from the manipulation of remote government departments and put accountability with locally elected establishments. Yes this may create an 'Information Divide' but it restores faith in the governance and assurance processes.

## **Section 5: Technology**

### **Question 20.**

Comments: The national aggregation of data, powerful linking and analytical tools, and the growth of 'scrutiny' forums have certainly created some challenges to the legal sharing of personalised information.

Technological advances on the other hand have also delivered increased protection and security functionality be this encryption, access based controls, single sign-on, disaster recovery or the ability to track individual law infringements on a global basis.

Yes - technology and the citizen's expectations have both moved fast particularly in the area of social networking where sharing personalised data is accepted. The difference is that the citizen is in control of what they release and with whom they share it which is far from the position in respect of service transactional data.

As with service transformation technology is an enabler - the recent losses of data were not technological issues but corporate failure to keep internal controls abreast of the shifts in technology and changing business models in respect of data processing. Centralised data processing for instance creates more corporate risks that need to be visible and managed than if the organisation was directly responsible for all data management functions.

Technology will continue to advance and we need to ensure that where these latest solutions get implemented they are supported by an appropriate investment in data protection and security at all levels.

### **Question 21.**

Comments: No. Each and every organisation, both public and private, must be able to prioritise investment to return optimum value to their shareholders or stakeholders. Integrating Information Governance and Assurance with corporate internal controls will ensure that data loss risks are on and owned by the executive agenda.

No law can mandate to this level of detail and still encourage innovation and freedom to shape their solutions based on returning optimum value to their community stakeholders.

Question 22.

Comments: This is one area where we have significant expertise and experience and there are already moves ahead in the NHS to use this approach in research and commissioning through the deployment of the National Spine's Secondary User Service (SUS). This is an area certainly worth investigating. Locally the use of personalised data in research must be approved by an ethical committee.

Having recently been involved in looking at the use of synthetically created data for use in a national training systems it was clear that the alternative options (anonymisation and pseudonymisation) being considered were not understood by key decision makers. It was equally difficult for those understanding the different techniques to respectfully engage with their superiors to discuss the inherent risks associated with these approaches. The exact same decision makers approved the use of synthetic data once confronted with external expert advice stressing that the use of personalised data, even in anonymised or pseudonymised state, would have breached the 2nd Principle of the DPA.

There is a need to fully understand the technical differences between the various techniques used to 'de-personalise' data. For example pseudonymisation removes person identifiable data but there needs to be a link stored that maps the output record with the input data. For research this is considered acceptable so that if there are any 'time bombs' discovered within the data the link information can be passed back to the data owner for action including tracking down the affected citizen.

The issue comes back to ensuring all parties fully understand what the purpose of capturing, storing and processing personal information is. The sharing of data must be fully justified, preferably locally, and again against a clear and accountable 'purpose'. Part of this process must include taking and respecting expert advice on which, if any, of the de-personalisation techniques need to be deployed. There is little doubt that a mix of these techniques would have minimised the consequences of the some or all of the recent personal data losses.

**Section 6: International comparisons**

Question 23.

Comments: Nil of note

Question 24.

Comments: Nil of note

Question 25.

Comments: Nil of note

Question 26.

Comments: We understand that some of the Scandanavian countries have a liberal approach to information sharing although we have not researched this in any depth.

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

Question 27.

Comments: The need to look beyond the DPA is to be stressed - corporate responsibility, director liability and accountability, compliance with industry standards on data management and empowerment to act locally.

The regulatory impact assessments need to explicitly address information assurance and there needs to be a governance forum, including experts in this area that can test policy and strategy assumptions. The observations and recommendations should be published through an independent agency.

Question 28.

Comments: Nil of note