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:
The National Information Governance Board for Health and Social Care provides advice to health and social care on all information governance matters, including sharing information. It reports to and advises the Secretary of State for Health.

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

Question 2.

Comments:
To an individual sharing health and social care information facilitates the delivery of services which are joined up, safer, more responsive and can be personalised to meet patients' needs more effectively. It enables key information, such as demographics, to be given once and used many times and facilitates maintaining the accuracy of information. In certain circumstances timely sharing of clinical information, for example allergies, drugs being taken etc, can be vital in choosing the most appropriate treatment in an emergency. Sharing information between clinicians and patients has clear potential benefits in self care and self management.

Sharing information can also prevent risk or harm. Several reports into child abuse (most extensively in Herbert Laming's report on Victoria Climbie) have pointed out the importance of sharing information between health, social care and other professionals. The report into the case of Fred and Rosemary West also highlighted the dangers of not sharing information.

From a societal perspective sharing information facilitates planning and funding the delivery of health and social care based on needs and allows a coordinated approach across services to be taken. It also allows statistics to be collated and research to be conducted in a variety of areas ranging from service planning, through disease prevention, to the delivery of care and treatment and the monitoring of their effectiveness. Sharing information improves the efficiency of services by providing the correct information to frontline workers when they need it.

Question 3.

Comments:

The key risk is that confidentiality is either breached or is perceived to have been breached. The consequence of this is that individuals might then refuse to share their information and depending on the situation either the individual, society or possibly both will be impacted.

There is a risk to individuals that if information is shared in a way which does not allow it to be kept up to date it can potentially become inaccurate and users may not be aware of this. In health and social care inaccurate information can lead to wrong decision making which can put the patient/client at risk.

There is also a risk that data is shared without consent or is used for purposes which were not envisaged when consent was given. This can undermine trust and confidence in the person to whom the information was given and also in the information governance practices and management in the organisation holding the information. This may extend beyond the service directly involved.

In health care situations have arisen where individuals have been so concerned about confidentiality and data sharing that they only use A&E departments or drop in centres or use a false name. Also those with infectious diseases which are, or are perceived to be, notifiable may try to protect their identity by not seeking treatment. The consequence of this is not only to the individual and their family as it can have a direct and potentially costly impact on public health.

Fear of inappropriate information sharing has an impact on the individual and also on society on both an ethical perspective and also on a practical basis which can range from incorrectly resourced services to the impact on research of incomplete data sets.

The delivery of many public services, including elements of health and social care, depend on the use of independent contractors. This means that information will cross back and forward between public and independent sector organisations, posing particular challenges in ensuring that information governance standards are both consistent and consistently applied.

The creation of electronic records allows an increased number of contributors to each record. Whilst there are benefits to this it needs to be well managed to ensure that the

accuracy of the record is not compromised.

Question 4.

Comments:

Properly controlled, governed and resourced the use of IT provides the greatest opportunity for improved information sharing. Conversely, incorrectly controlled, governed or resourced, it poses the greatest risk.

Used appropriately IT allows information to be shared in a controlled way. It is more responsive than paper or portable media can be. Examples would include the community nurse who can access information on surgery IT systems using wireless functions or the patient seeking emergency treatment far away from home.

The consequences of using IT which is neither controlled nor resourced have received significant media attention recently. Losses and inappropriate use have probably always occurred with paper records, the point being that IT can facilitate this taking place in bulk and at a speed which can make recovery difficult. Electronic databases also allow data to be “trawled” to identify specific characteristics with far greater ease and effectiveness than is afforded by paper records.

The main risks associated with the use of paper to share information are that it is slow, it often lacks standards or consistency, it can easily get lost or for other reasons may not be immediately accessible. Also the value and the safety of the sharing element depend on legibility.

Question 5.

Comments:

Possibly not an issue of too much data but the linking of databases can make information available or allow inferences to be drawn which were not expected or anticipated when the information was provided, and for which consent was not given.

Question 6.

Comments:

Question 7.

Comments:

Service users have a perception that standards of confidentiality are not uniform in health and social care. They might also believe (in some cases correctly) that sharing information with social care agencies might prompt an intervention. Consequently some service users will share information with those delivering health care which they would not share with those providing social care. This can result in incomplete information sharing.

Difficulties can exist even within the same service. Many patients are prepared to share very intimate details of their life with their doctor which may be relevant to a medical problem but they may be very unhappy if that information can be accessed by a person in a different healthcare sector. The important issue about information sharing is not only whether the

information is secure with those who access it but also whether they have a clinical or care need to access it.

Reference has already been made in answer to Q2 that several reports into child abuse (most extensively in Herbert Laming's report on Victoria Climbie) have pointed out deficiencies in sharing information between health, social care and other professionals.

Public confidence in information sharing can be improved by the development of clear and uniform information governance standards between organisations sharing information, where the highest standard amongst them is adopted, maintained and governed rather than the lowest. Governance standards need to be backed up by firm disciplinary and if relevant legal action.

Question 8.

Comments:

Our response relates not to information sharing which is taking place but to constant attempts to erode the confidential nature of health and social care information. There are several situations where it is clearly appropriate that information should be disclosed without consent and these include reporting gunshot wounds where it is in the public interest to do so and notifiable communicable diseases. However, as health databases are believed to hold the most accurate and up to date details they become targets for those who wish to locate individuals or groups of individuals, for example failed asylum seekers.

The impact of this type of activity can be very significant. It reduces confidence in services which rely on trust and it increases concern about the use of electronic systems which when used appropriately can deliver major benefits to service users. It can also potentially impinge on issues of human rights and/or civil liberties. There is a tension between, for example, the need to disclose notifiable diseases and the risk to public health from those who prevent disclosure of their details by not seeking treatment.

In forensic psychiatry, the need for absolute confidentiality between patient and clinician in order that disclosure can take place could be fundamentally impacted by concerns, real or imagined, that data was being shared.

We have expanded on our position on the confidential nature of health and social care information further in answer to question 28 but suffice it to say here that the National Information Governance Board for Health and Social Care believes that the special sensitivity of health and social care information should be reflected in statute.

Section 3: The legal framework

Question 9.

Comments:

It could be argued that a weakness for the DPA is the context in which it operates, in that it has to be interpreted alongside European directives and common law.

Section 7 (subject access) of the DPA is a strength. It provides fairly straightforward rights

and also logical ways of balancing the rights of third parties.
The section 55 offence sets a high bar for culpability. It is uncertain what "without the consent of the data controller" means. An individual, data subject or data controller may find it difficult to ascertain what type of conduct is prohibited, and this is a weakness.

The concept of data "controllers in common" is being used to share the responsibilities of data control and it has the potential to cause confusion and inappropriate sharing.

The act does not expressly deal with the issue of informed consent in a way that can be understood by service users. Schedule 3 introduces the concept of explicit consent, but the act does not supply usable definitions or guidance as to how this concept should be understood and applied. This affects the issue of re-use of information, especially in the area of research over a period of time, when new purposes present themselves that were not anticipated at the start of data gathering and purpose setting. This is a weakness.

The DPA requires that data is not further processed in any manner incompatible with the purpose for which it was given. People give data for health and social care and may not always be aware that it could be used for other related purposes.

We are aware that the crime and taxation exemptions under section 29 of the DPA are regularly presented to clinicians by the authorities when seeking information as conferring a right to access rather than providing them with protection if they can justify the exemption. Again we feel that clarification is needed here.

The act does have a weakness in its definition of a health record. In Part VI, as defined in section 68(2), a health record is defined as one which relates to the physical or mental health of an individual which 'has been made by or on behalf of a health professional in connection with the care of that individual'. With the current trend towards self management and expert patients, entries made by patients should be considered part of the record.

Question 10.

Comments:

In general terms, the reasons or purposes for processing data is a widely understood concept among public bodies and private organisations. The second principle is very valuable and is one of the key concepts in the Act. It acts as a check on the overuse of personal data.
For example, many social care assessments gather a wide range of data that could allow professionals to conduct broad investigations in an attempt to fix all or most of a person's perceived problems. The second principle encourages professionals to concentrate on their core purposes, the reasons for their involvement and the scope of the service user's consent.

Question 11.

Comments:

Whilst the public seek privacy and rightly expect the appropriate handling of their personal information, they may not be aware how the information that they are willing to provide in completing, for example, shopping surveys will be used.

We believe it should be made clear to those providing information, what their information will be used for and how long it will be kept.

Question 12.

Comments:

The Information Commissioner's Office's (ICO) power to inspect data controllers without consent should have a statutory basis but also have adequate provision for the protection of confidential information. The ICO should also have power to impose a summary fine, with reasons and recommendations, on data controllers on a similar basis as the Financial Services Authority. The section 55 offence should be simplified and split into a series of offences covering individual and corporate offences. The revised section (or sections) should also clearly delineate civil and criminal offences and penalties. The consent of the Director of Public Prosecutions in section 60 should also be reconsidered.
We can broadly endorse the powers being sought by the ICO to increase the penalty for the mis-use of information which have been laid out generally in November and December 2007 as well as January 2008. To avoid too onerous a scheme, any reporting or regulatory function could be risk related.

Further, we note that the Act has not generated any or any significant private law actions for damages and we suspect that this may be due to the drafting of the section 55 offence and the general discretion given to courts to make orders under sections 10 to 14.

Question 13.

Comments:

In general if it could be drafted to be easier to understand that would be a bonus. The interaction between common law and statute in the UK perhaps adds to some confusion.

A key issue is whether the public are able to understand the various pieces of legislation that have been put in place to protect them. It is difficult to implement effective information governance if the rules are not understood. The Department of Health has published the NHS Care Record Guarantee for England and the Information Commissioner has gone to great lengths to put information on his website to explain the Data Protection Act. The Information Commissioner should provide information on all aspects of confidentiality/security legislation including clear definitions of key concepts such as consent and explicit consent, anonymised and identifiable data.

Question 14.

Comments:

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.
Comments: Health and social care is delivered by multiple organisations which need to share information in order to deliver services efficiently and effectively. The underlying principle is that people should be aware of how their information is being used and consent to this. If it is to be used for other purposes then additional consent should be sought. Problems can occur where boundaries overlap or blur and perceived "common sense" is applied rather than clear principles. An example is a clinician treating a patient for a condition which that clinician is also carrying out research into. The patient has openly provided information to the clinician for the purpose of receiving care, but that clinician cannot then use that information for research. There is a further point which can be made under this question, which is that effective governance can only be fully implemented if consent requirements are clear not only to those who are seeking to use information but also to those who provide it. An interesting question to pose in the context of consent is whether individuals should be allowed to consent prospectively to their personal data being used for future research projects, including those not yet defined.

Question 17.
Comments: The National Information Governance Board strongly supports the adoption of a system which requires consent. However, in health and social care there are circumstances in which obtaining consent is not possible, for example unconscious patients requiring emergency treatment. There are processes to deal with these situations but best practice is not always observed and health and social care professionals need to be adequately trained.

Question 18.
Comments: Consent makes information sharing transparent. The National Information Governance Board agrees that information sharing should be transparent and that individuals access rights are currently, in principle, appropriate. We do, however, have concerns about how errors or disputes over the content of clinical records are dealt with. Whilst there is existing legislation and professional guidelines for dealing with this situation we feel that this is an area where the implementation of legislation needs to be enforced. We are aware of some individuals who find resolution difficult to achieve and we feel that information should be regarded as "co-produced" by the service user and the professional. The Department of Health has acted to make the use of information transparent by publishing the NHS Care Record Guarantee for England in 2005. This is a document aimed at patients which explains how their information is used in healthcare and what their rights are. The guarantee is reviewed annually and approved by the Plain English Campaign. To date no other government department has published a similar document although we are

aware that the Department for Children, Schools and Families is working on a similar document and also that a Social Care Guarantee is being prepared.

The Department of Health has also established the National Information Governance Board for Health and Social Care to provide oversight and advice on information governance matters. It has ensured that the remit of the board covers the bodies that most frequently share information so that common policies and practices can be established across care. The Health and Social Care Bill, currently before Parliament, will make the Board a statutory body.

Question 19.

Comments:

Data Controllers should take responsibility for information sharing and be working to common, replicable, standards as outlined in the Framework Code.
Within health and social care Caldicott Guardians from the organisations sharing information, could provide oversight of information sharing frameworks, especially those which crossed organisational boundaries.

Privacy Impact Assessments would bring clarity. However, they raise the question of who would conduct them. For example a patient with concerns about information sharing and a medical researcher would be likely to produce a completely different impact assessment on the same information.

Lay involvement in all these processes should be increased to maximise transparency and public confidence.

All organisations should have an equivalent document to the NHS Care Record Guarantee for England.

Section 5: Technology

Question 20.

Comments:

Technology offers many benefits to health and social care which has traditionally operated paper based systems. The use of IT provides major benefits over paper in the storage, retrieval and, if properly applied, the security of records. It also supports improved speed of communication, for example getting test results from hospitals to GPs and potentially increases the volume of data which can be transferred and handled.

Many health and social care services are delivered remotely in either service user's homes or, for example, nursing homes. IT can provide significant benefits in the delivery of these services by facilitating remote access to central information systems and removing administrative burdens allowing the professional to focus more on service delivery.

We do not support the criticisms about the concept of central databases of health and social care information. Where central databases are properly administered and protected these can allow secure access to information which otherwise may have to be distributed using

portable media or paper. The ability to provide an audit trail of every access to an electronic record is an important advance in confidentiality which is not available with paper records.

Many million paper records are still in use in the NHS and social care, and are often kept in vast storage areas. Keeping these records in electronic form affords a degree of protection against physical damage e.g. fire or flood which cannot be cost effectively achieved with paper records.

The ability to access information using IT also brings tensions. This can occur between professionals caring for patients and those in the same profession who wish to carry out research. It can also occur between those who are known to have access to information provided for the delivery of care and those who wish to use this information to enforce legislation – security services, immigration services etc.

Question 21.

Comments:

In principle the National Information Governance Board would support mandating technical safeguards for the protection of personal information, but would point out that:

a) This would need to be appropriately resourced, in terms of funding and manpower.

b) The safeguards would need to be regularly reviewed to ensure they remained at the necessary high standard.

c) Mandated standards would require a mechanism of audit and a framework of sanctions for non compliance.

We are already pursuing this line and have asked the Patient Information Advisory Group, a statutory body which can, in specific circumstances, approve access to patient information without the consent of the patient, and the Information Standards Board for Health and Social Care to advise us on the practicality of implementing a standard for pseudonymisation.

Technical safeguards can, and do, protect personal information particularly where portable media is used or in the prevention of bulk downloads. However, there is a residual risk from those who have legitimate access to information and choose to behave improperly. For this reason we support the Information Commissioners proposal to increase the penalties for misuse of information.

Question 22.

Comments:

The Care Record Development Board established an expert group in 2006/7 to consider the secondary uses of patient information. They made several recommendations related to the use of anonymised and pseudonymised information and we have attached a copy of their report with our submission.

Clearly access to a large amount of clinical information which is either anonymised or pseudonymised will be beneficial to researchers and the benefits of properly planned and managed medical research are easily demonstrated. However, this raises two points – firstly that it cannot be assumed that all research is good research and secondly that where

there is the possibility of identifying the patient from the information then either their consent should be sought or approval from the Patient Information Advisory Group via section 251 of the NHS Act 2006.

The medical research community has issues around the exclusive use of anonymised and pseudonymised information and believes that some research mandates the need for identifiable information. The National Information Governance Board firmly believes that if this is the case then consent or a legal alternative e.g. the approval of the Patient Information Advisory Group should always be sought.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:

The Information Commissioner has repeatedly expressed an opinion that due to the particularly confidential and sensitive nature of health information it should be regarded as different from other personal information. The National Information Governance Board fully supports this position and considers it appropriate that this should be extended to include social care information.

We believe that all information provided for, or during, the provision of health or social care, including demographic details, was provided solely for the purpose of receiving care or treatment and should not be used for other purposes. It is often argued that demographic details provided during the delivery of care are not confidential as demographic details can be obtained from several other sources. Our position is that if this is the case then one of the other sources should be used.