

# 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:

*Please explain what your interest in information sharing is.*

The BMA's members are interested in information sharing because they are the recipients of sensitive personal information and they have legal, professional and ethical duties to ensure that information is shared appropriately. Patients share information with doctors on the assumption that it will be kept confidential. Failure to keep this information confidential could jeopardise the doctor/patient relationship and make patients cautious about sharing information in the future.

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

Our members hold personal information including demographics, health, lifestyle and social information about their patients. Third party information is also held including details of family history.

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

Our members collect this information in a number of ways. A patient may disclose the information during a doctor/patient consultation. A third party may provide information for example a relative who is concerned about an individual. Doctors also collect information from others involved in a patient's care for example test results, outpatient reports, telephone conversations and letters. This may also include information from other sectors for example social services and education.

At present information is held in the NHS both electronically and in paper files. Where information is held on computers it is backed up and archived and a recent backup is usually held off site. Some organisations choose to hold information remotely on centralised servers. Health records from multiple GP practices may be held on one centralised server with organisational boundaries.

NHS Connecting for Health is delivering the NHS Care Records Service (NHS CRS). One component of the NHS CRS, which has been implemented, is the Personal Demographics Service where all patient demographics are stored centrally. As part of the NHS CRS, patients can choose to have a summary care record which is stored centrally. This is being implemented in six early adopter areas. In the near future, it is expected that detailed local records of patient care will be stored on localised databases and shared between local clinicians providing care to a patient. Data are also stored on the Secondary Uses Service, which is a single repository for patient and care event data. This data will be pseudonymised before being made available to researchers etc unless there is PIAG approval to use identifiable data. In Scotland, Northern Ireland and Wales similar IT programmes are underway.

The majority of identifiable information is currently shared within the NHS on a need to know, implied consent, basis. The information may be shared on paper for example by sending a referral letter. Information is also shared electronically, for example, by email or via electronic systems such as Choose and Book. As outlined above the NHS CRS will mean that healthcare information will increasingly be shared electronically. Those with a legitimate relationship and an appropriate role will be able to access a patient's healthcare information. Information is also shared verbally for example during face to face colleague discussions or on the telephone.

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

The primary purpose for collecting this information is to build a medical history in order to provide quality care to an individual. The main reason for sharing information is during the referral of an individual. There are secondary purposes for sharing information, for research, commissioning, public health reasons etc. With explicit patient consent, the data may also be shared for other reasons for example insurance reports.

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

**Question 2.** *What in your view are the key benefits of sharing personal information to a) individuals and b) society? Please provide examples.*

### **Comments:**

Sharing personal information between healthcare professionals ensures an individual receives the best possible care. Treating an individual without knowledge of a patient's medical history could place that individual at risk of unnecessary treatment, repeated investigation or hospital admission. Sharing healthcare information is of particular benefit to

patients who interact with multiple parts of the health system.

Sharing health information can bring huge benefits to society. Epidemiological research would not be possible without sharing personal information and this has contributed to great benefits in our society for example the identification of the dangers of smoking. Public health surveillance helps protect society by allowing the government to respond immediately to the threat of infectious diseases and environmental threats for example SARS. The effectiveness of interventions can also be measured and this evidence can be used to improve patient care. Sharing healthcare information can also bring benefits to local communities through local audits of clinical practice. Sharing health information can help save public money by enabling improved healthcare planning, commissioning of services, benchmarking and clinical audit. Data used for these purposes should be anonymised unless there is appropriate consent, the law requires disclosure or where there is an overriding public interest.

Question 3. *What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.*

**Comments:**

Sharing healthcare information poses a number of risks to individuals due to the highly sensitive nature of this information. Healthcare information is disclosed by patients on the basis that it will be kept confidential and the more widely it is shared the greater the risks to the security and confidentiality of that information. If information is shared inappropriately this could be very damaging and cause distress. If in the wrong hands, healthcare information could be used for blackmail, fraudulent and other malicious purposes. This could range from professional fraudsters and hackers to a nosy neighbour working in the NHS having a quick look at a record.

Many doctors are concerned about the risks of centrally held electronic records. With paper records, it is necessary to travel to the location of the records to view them and the dispersed nature of paper records would help minimise the potential damage if access was gained. With centrally held electronic records access could be gained remotely and it would be easier to scan large amounts of information. Despite the security and access controls in place, some feel that shared electronic records present a greater security risk. The expansion in mobile devices such as laptops and hand held devices can put data at risk and increase the risk of inappropriate access unless appropriate precautions are taken.

There is a risk with electronic records that those viewing the record will see more than necessary. For example, when a GP makes a referral he/she will include in the referral letter only the information that it is necessary for treatment. With the NHS Care Record Service it will be possible for those with appropriate access rights to view the whole detailed care record and information that is potentially not strictly necessary for treatment.

There is also the danger that once information is shared it may be misinterpreted especially when data are taken out of context, which could have serious repercussions. This is also the case if inaccurate data are held and shared more widely.

There has been much recent media attention about the government losing data and a rising concern in general about the use of our data for example stolen identities and financial blagging. There are concerns about a 'surveillance society', concerns about inappropriate behaviour by systems administrators, fears about government departments sharing information and allowing the police direct access to health databases. Due to recent data

losses, many of our members feel that public agencies are unable to offer an appropriate level of protection. Whilst it is possible for confidentiality breaches to take place without detection, with paper records, there is a risk of a greater security breach with electronic records. The compact nature of electronic information means that larger volumes of confidential information can be leaked as highlighted by recent incidents, for example, the loss of 25 million records by HM Revenue and Customs. Individuals may start to think twice before disclosing information and will exercise rights to withhold information. This may put at risk patient care. It would also have a detrimental impact on research possibilities, affecting society as a whole.

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

**Comments:**

In November 2007, 3000 patient details were lost when a GP's laptop was stolen in Newport. In December it was reported that a PCT had lost 160,000 patient details and in October 2007 it was reported that details of 25 million parents and children had been lost. Whether data are held on one laptop, by a Trust or on a government database, they are never completely secure. The difference, however, is the potential scale of the loss as highlighted by these cases. Concern about the risks of patient data prompted doctors to call for 'the BMA to advise all its members not to cooperate with the proposed centralised storage of all medical records as this seriously endangers patient confidentiality'. There is a growing feeling that there should be a move away from large central databases and information should be shared locally via integrated systems or local servers. This would also support the need for sharing information, on a need to know basis, with others in the community such as education and social services. Paradoxically, large databases of centrally held data will enable greater research and reap the benefits outlined in question 2.

The BMA has repeatedly called for individual explicit consent before healthcare information is held centrally. This will enable patients to evaluate the benefits and risks and control whether their personal information is uploaded.

**Question 5 and 6** *Please provide examples, where in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.*

*Please provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.*

**Comments:**

It is our view that there are times when both public and private sector bodies hold too much personal identifiable data. An example is the data held by PCTs and Trusts for commissioning purposes. Whilst we accept that there are benefits for PCTs and Trusts to access this information, we do not always feel it is necessary for this to be in an identifiable form. We support the recommendation of the Care Records Development Board Secondary Uses Working Group, that the use of data in an anonymised and aggregated format should be publicised and promoted. We feel that the government should put a greater priority on ensuring that anonymised or pseudonymised data are used whenever possible and privacy

enhancing techniques are exploited more fully.

**Question 7.** *Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.*

**Comments:**

UK healthcare IT programmes are facilitating greater sharing of information. We have urged an incremental approach and do not feel any further sharing of healthcare information should be taking place than at present.

**Question 8.** *Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.*

**Comments:**

**Section 3: The legal framework**

**Question 9.** *In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.*

**Comments:**

One of the weaknesses of the DPA is the ambiguity around consent, particularly with regard to Secondary Uses of information. The legal complexities are explored in the Report by the Academy of Medical Sciences - 'Personal data for public good: using health information in medical research': <http://www.acmedsci.ac.uk/images/project/1170326729.pdf>

There has also been some concern about the legality of the NHS Care Record Service and whether, under the DPA, data can be transferred to the spine on an implied consent basis. These ambiguities make doctors concerned about liability issues and result in difficult decisions about whether data should be shared.

**Question 10.** *In your view, how well do public authorities and private organisations adhere to the second principle of the DPA? How valuable do you believe the second principle is? Please provide examples for the reasoning behind your response.*

**Comments:**

The second principle of the DPA is very important in healthcare. Patients take for granted the fact that their identifiable data will be kept confidential and not disclosed for other purposes without their explicit consent. However, most patients would be extremely surprised to learn the extent to which their data are used for purposes other than their direct healthcare.

The BMA has stressed the need for greater education of the public on how their healthcare data are used. We suspect that the second principle of the Data Protection Act is also breached due to lack of training of employees and the absence of appropriate policies being

in place. It is very easy for example to give details out over the phone without thinking through the implications.

*Question 11. What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.*

Comments:

Technology facilitates greater sharing of information and this can become a barrier to the effectiveness of the DPA. At present GPs are data controllers and they can manage this role effectively as they have control over who accesses the data stored in their practice and can respond to subject access requests. With the implementation of the NHS CRS, GPs are concerned that they will no longer be able to effectively carry out this role as the patient data currently held on their systems will be held on centralised databases. It also becomes harder to respond to subject access requests due to multiple contributors to the record.

In NHS institutions there needs to be a shift to ensure that information governance policies are viewed as core business and every individual knows their responsibilities and receives proper training. Unfortunately this is often not the case and is something NHS Connecting for Health is trying to address. Caldicott (information) Guardians need to be given proper training and support to ensure that they can deal with these changes.

The legal complexities surrounding the DPA mean that at times there is uncertainty about whether data should be shared. This results in data being inappropriately stored and shared due to ignorance or misunderstanding but also, at times, makes individuals or organisations overly cautious so the benefits of legitimately sharing information cannot be reaped.

There seems to be a lack of awareness in society of the importance of treating data appropriately. For example there were a number of reports of NHS staff sharing their NHS smart cards to access systems. Whilst the majority of these cases were not with malicious intent these workarounds demonstrate a lack of respect for the data concerned.

*Question 12. What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA.*

Comments:

We believe that penalties should be enforced for those who breach the Data Protection Act. These penalties should apply to both the individuals who breach the Data Protection Act and institutions who fail to implement appropriate policies, safeguards and training.

There should also be measures in place to make sure that these penalties are implemented. Often when there has been inappropriate access to data no action is taken and this sends a message to others that it is not taken very seriously. Any sanctions must be appropriate for the offence.

An example is the Electronic Staff Record (ESR), which is replacing 29 payroll systems and 38 HR systems with a single integrated national system. The BMA worked with the ESR team on drafting a 'staff charter' or agreement on the use of staff data. The BMA asked the ESR team and the government to include a clause that 'disciplinary action would be taken in the event of inappropriate access' with the caveat that local organisations can decide the appropriate disciplinary action in each case. This continues to be declined as it is felt to be completely a local decision. This is an example of how the message is being conveyed that inappropriate access of data is not a serious issue.

A further example is an incident where a PCT employed manager persuaded a district nurse to disclose her username and password. He used these to access patient identifiable information held by a GP practice, whose clinical system was hosted by the PCT, without the knowledge of the data controller (the GP Practice) or the consent of the patients involved. Other PCT employees were also similarly accessing patient data. Members of the local General Practitioners Committee contacted the PCT but to date no action has been taken against the manager or the nurse involved.

There should be a renewed publicity campaign to make the public and organisations of the awareness of their responsibilities under the Data Protection and these penalties. We regularly see TV advertisements to inform the public of what will happen if they do not pay their tax etc but there is little to remind the public of what could happen if they inappropriately disclose information.

*Question 13. Are there any other aspects of UK or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Please provide examples.*

Comments:

It is unclear how the work of the EU Article 29 Data Protection Working Party relates to the Data Protection Act. The 'Working Document on the processing of personal data relating to health in electronic health records (EHR)'<sup>1</sup> states: 'In contrast to the provisions of Article 7 of the Directive, consent in the case of sensitive personal data and therefore the EHR must be explicit. Opt-out solutions will not meet the requirements of being explicit'.

The BMA believes that explicit patient consent should be obtained before healthcare information is uploaded onto the NHS CRS. In England, the government has adopted an implied consent model for sharing drugs and allergies. The BMA has received assurances from Lord Warner that the NHS CRS complies with relevant law. It is not clear how this fits in with this EU development. Doctors continue to express their concern about the legality of the NHS CRS and are concerned that in the future they could be found liable for not complying with this directive.

*Question 14. Are there any statutory powers unavailable that would enable better and more secure sharing of personal information– for example for identity authentication purposes – between a) public authorities and b) public authorities and private organisations? If so, what are they?*

Comments:

There should be an obligation for public bodies or private contractors working with them to share personal information which could assist in the prevention of the serious fraudulent misuse of public services or funds. An example, in the area of public healthcare provision, is the potential sharing of information between NHS Trusts/ Strategic Health Authorities and the NHS Counter Fraud Service or the Department of Work and Pensions.

Such cooperation in sharing patient identifiable information should be allowed with appropriate safeguards to limit the dissemination. It should be the minimum necessary and restricted to investigating officers who would respect the sensitivity of certain information and

---

<sup>1</sup> [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp131\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf)

will be disciplined if they use the information inappropriately.

Question 15. *Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples.*

Comments:

Subject access requests create workload issues for doctors and their staff. Each record must be checked for information which may cause serious damage to the patient and for third party information before it is released. Some medical records are very long and this may take a lot of time. The BMA supports patients having access to their records but the additional workload implications should be recognised.

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

Question 16. *Is it clear whether and when you need individuals' consent to share information about them? Are you clear about the form that consent should take? Please provide examples. Please provide details of any initiative you have been involved in that has been based on consent.*

Comments:

No it is not always clear due to the complexity of the legal position. Doctors have to weigh up both the DPA and the common law requirement for consent before deciding whether to disclose information. This is particularly the case for secondary uses and the BMA has recently produced some guidance focusing on this topic<sup>2</sup>. There have been times when pressure has been placed on doctors to share data on an implied consent basis as it is not strictly in breach of the DPA but by doing so the doctor could be in breach of professional regulations.

Although the DPA and the Human Rights Act have helped improve the situation, the fundamental duty of confidentiality is still in common law and these pieces of legislation have not clarified that. We welcome the government's decision to review this area and feel that consideration should be given to an overarching statute in this area to clarify the situation.

There are also particularly difficulties with regard to consent for parental access to records and this is an area where information may be inappropriately disclosed because of lack of knowledge or understanding.

Question 17. *What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.*

Comments:

There are challenges in obtaining consent, whether it is implied or explicit. Barriers do not however mean that consent should not be obtained. The difficulties in obtaining consent include:

- workload generated by seeking consent

---

<sup>2</sup> BMA guidance on secondary uses of patient information

[http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFSecondaryUses/\\$FILE/secondary+uses+of+patient-identifiable+information.pdf](http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFSecondaryUses/$FILE/secondary+uses+of+patient-identifiable+information.pdf)

- financial implications for example the costs of writing to each individual patient
- time issues – research may be delayed because of the time it takes to seek consent
- Fewer numbers involved if explicit consent is required due to individuals not getting round to sending their response back etc.
- Difficulties ensuring that it is informed consent and patients understand their choices. This is particularly the case when the research is complex and/or the individuals are very ill.

Question 18. *Do you have any suggestions on how to make the sharing of information more transparent?*

*For example, should individuals be given strengthened access rights? And if so, how? Should organisations be expected to do more to explain their use and sharing of personal information to the public? And if so, how?*

Comments:

One of the strengths of electronic information is that it is possible to audit who has viewed and edited information. The BMA supports the development of initiatives such as Healthspace, which will help make the sharing of information more transparent. In England, patients will be able to see who has accessed their Summary Care Records by logging into their advanced Healthspace account. We believe that this should also be extended to detailed records.

We believe that when personal information is held there should always be appropriate audit trails in place and individuals should be able to request a copy of the audit trail and explain the use and sharing of personal information. An example where this is not happening is the Electronic Staff Record, which does not audit when a staff record has been viewed.

There should also be greater transparency with regard to secondary uses of data. In healthcare, there is very little awareness amongst patients about how their data are used. We believe that there should be an area of NHS Choices or Healthspace where patients can view how information has been used for secondary uses and the benefits it brings.

There also needs to be greater transparency with regard to the system staff that have access to systems. This is currently possible in a very limited way with paper records. It is likely that patients are unaware of the non-medical third parties who might view some of their information. Whilst tracking, logging and security systems can be developed to limit this, there are fears that system staff with sufficient seniority may be able to defeat the protections and, due to access privileges, could be subject to bribery or coercion by others.

Question 19. *How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?*

*For example:*

*In your view, how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information ([http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/pinfo-framework.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf))? In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December ([www.ico.gov.uk](http://www.ico.gov.uk))?*

Comments:

The information sharing policy is helpful as we believe it may help encourage organisations

to produce a code of practices and promote good practice. We believe that it should be a legal requirement for organisations that hold personal information to have a code of practice in place.

### **Section 5: Technology**

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

Comments:

Technological advances have had a huge impact on the sharing and protection of personal information in both a positive and a negative way. The impact of technology in healthcare is particularly evident in primary care where GPs have been using electronic records for decades.

Technology has sped up the transfer of data. Integrated systems have enabled teams to access information simultaneously. Information can be shared almost instantaneously with others by email. Mobile devices mean that data can be shared on the move. This is a growing trend in healthcare and has significant benefits for example for community workers or ward rounds. Anonymisation techniques make it easier for data to be used for secondary uses.

In many ways electronic records are more secure than paper records provided that appropriate measures are in place to protect the data. Data can be encrypted, audit trails make it possible to see who has accessed records and it is possible to limit access to parts of information for example a secretary won't necessarily see the whole patient record. The majority of times when data are put at risk are not due to technology failures but human error and not having appropriate procedures in place for example taking appropriate measures to look after mobile devices when they are taken out of a secure setting. As we move towards large central databases of information there is a greater risk of loss of large amounts of information and technology can potentially put data at a greater risk. An example is MTAS where sensitive personal details were not held securely.

Question 21. *Should the law mandate specific technical safeguards for protecting personal information?*

*For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?*

Comments:

We believe that the law should mandate specific technical safeguards for protecting personal information. Those not adhering to the technical safeguards should be held accountable. Although consideration should be given to whether it is realistic to expect the law to lay down technical standards when technology is moving far faster than the speed of legislators.

Question 22. *How, in your view, could 'privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research? Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?*

Comments:

Anonymisation and pseudonymisation do not provide the perfect protection of privacy. Appropriate measures for protecting data, even when it is anonymised, must still be in place as even the most robust systems are liable to inference attacks.

The BMA's view is that when data are anonymised or pseudonymised, it may be used without patient consent. Anonymised data should be used wherever possible, and pseudonymised only where absolutely necessary. The NHS Secondary Uses Service holds data in an identifiable form and there needs to be both technical and appropriate governance processes in place to protect this data. We feel that it is important that patients can opt out. We support the CRDB Working Group on the Secondary Uses of Patient Information proposal that electronic mechanisms are designed to record consent.

We do not feel that there is sufficient advice about the deployment of anonymisation and pseudonymisation techniques. As terms they need to be linked to clearly defined technical standards. Although the NHS had produced guidance on when data should be anonymised, we are not aware of a single authoritative piece of guidance providing technical advice on anonymising information.

### **Section 6: International comparisons**

*Question 23. Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Please provide examples.*

Comments:

*Question 24. Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?*

Comments:

*Question 25. Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?*

Comments:

*Question 26. Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.*

Comments:

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

*Question 27. Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering? Do any of these issues apply specifically to your sector?*

Comments:

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

Comments: