

# 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. Head of Information Governance for 'Informing Healthcare' which is a Welsh Assembly Government programme set up to improve health services in Wales by introducing new ways of accessing, using and storing information.

Comments:

The Informing Healthcare programme of work includes implementation of new services and systems in Wales which includes the use and sharing of personal and personal sensitive (health) information. Informing Healthcare also promotes standards for NHS Wales including Information Governance standards.

Examples of collecting, holding and sharing not by Informing Healthcare as an entity itself but in the implementations of specific projects and the programme as a whole include;

- GP Information systems data collected and shared to Out of Hours services for direct patient care.
- Access to existing services and data within hospitals and community through a Welsh Clinical Portal
- Access by patient to their own data through 'My Health Online' and others

Informing Healthcare as a programme will be involved with the testing and integrity of new project implementations and processes information in this respect only.

Purposes for collecting, holding and sharing information (through implementation of new services) primarily consists of improving facilities for clinicians who provide care and treatment to patients or for providing new services to patients.

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

Question 2.

- a) individuals will benefit from improved availability of their health records to health professionals involved with their care.
- b) Society will benefit in enhanced confidence in the health services being provided.

Comments: Examples:

- a) Out of Hours services extend the support available to patients when GP surgeries are closed. Ooh GP's however do not have access to a patients GP record and therefore often work 'blind' to important medical details. This is the same 'purpose' but sharing nevertheless. In Wales, Informing Healthcare has implemented a solution for such sharing agreed by health professionals including GP's as well as patients themselves. This is being rolled out across Wales in incremental steps after engagement with stakeholders. Patients and clinicians alike agree this improves patient safety and care.
- b) In our consultations with patients, directly through patient groups and through patient representation such as Community Health Councils there has been overwhelming support to improve the sharing of patient information for the purposes of direct patient care. In many cases patients have been appalled to learn that obvious sharing of information about them which is needed for their care is often currently not shared.

Question 3.

- a) Individuals may lose 'trust' in services if information is shared beyond their knowledge and beyond their wishes. All too easily information which is held by organisations is 'reused' for purposes other than which they were collected for. A breakdown in trust will lead to a reluctance for sharing of information in general even where the purposes are legitimate and of benefit to individuals.
- b) the main societal perception of risk is one of sharing beyond control. At each breach of confidentiality there is a lessening of confidence. The larger the database, the more national a system becomes the less contact with their own information the general public feel they have. In many respects this apprehension is well founded. Today's technology allows huge amounts of information to be shared very easily. In many respects we are only just now starting to catch up with technology in the issues around 'people' and 'processes'.

Comments:

A real focus of the work accomplished by Informing Healthcare has been thanks to the real engagement and participation not only by healthcare professionals but by patients themselves. This has been critical in building and maintaining 'trust'. The negative responses received by IHC have often been related to perceptions of very large sets of data for UK national systems which they do not see as having local or personal benefit. This negativity creates a knock on effect for local implementations.

Question 4.

Information sharing must be based on a real need and for justifiable purposes. This cannot be a top down approach but rather an incremental one building one purpose on another in an incremental way. The greatest opportunities lay in building information sharing one agreed step at a time. The greatest risk is in assuming a general requirement for information sharing or in attempting to include multiple purposes (or even undefined) all at the same time.

Comments:

There will always be a need to 'ad-hoc' sharing of piece of information. There needs to be informed senior personnel who are able to make decisions on the valid sharing of such information. In the NHS we have Caldicott Guardians and certainly in Wales these are important positions and Informing Healthcare is actively seeking to support the work of the Guardians. For regular sharing of information there needs to be frameworks in place which support the justification of such sharing especially when it is sharing beyond the organisation or the service sector. In Wales Informing Healthcare has supported the work done on the Wales accord for the Sharing of Personal information (WASPI) in conjunction with the Welsh Assembly Government.

Question 5. There may be aspects of this question that are correct in 'holding of too much information' in that sometimes data is collected 'in case'. I would doubt however that too little information is held for a particular present function as that would infer that the public body is not able to carry out its duties. However it could be reasonably argued that new services / improvements for the public could not take place without addition information being held. It is certainly the case that 'joining up services' for better care requires sharing that has not previously taken place.

Comments:

This question highlights the difference between 'holding' information and 'sharing' information. Often the problems of not enough or too much information being held are issues with sharing information and not related to initial collection (though not always)

Question 6.

The difficulty in the case of private organisations holding personal information is that it is so difficult to know. Many collection of information are compiled with a simple tick in a box or mandatory not for the functioning of a contract but because it's just part of the deal. Whether this information is too much is questionable. In most cases the individual would have agreed to the information being held though possibly they may not know the full extent of the information held or exactly who it may be shared with. In a way however this is the responsibility of the individual in this technology rich age.

Comments: I do wonder how much information could be accumulated through disclosure of information by private sector organisations through methods such as '*tick here if you do not wish us to share this information with other interested parties*' ending up being information bureaus and large amounts of personal information being held by organisations that the individual has no knowledge of.

Question 7.

A good example of this is the availability of GP records out of hours. Essentially this is an identical use of information, i.e. the same purpose – the direct care of the patient. However this information is not available to Out of Hours GP's or any other emergency or unscheduled care services. This dismays patients who learn of this and expect essential information about themselves to be available for their direct care. In Wales participation by healthcare professionals has meant that this information is now beginning to be shared. Patients are being informed of the uses (very clear and focused on direct care) and given the opportunity to 'opt out' of this sharing – so far only a tiny percentage have chose to do so.

Barriers encountered have been ethical and perceptual. Oddly the technology was never considered a barrier, just a challenge which would be solved. Legally there was no barrier to the sharing of such information however there were 'perceptions' that there were legal barriers and the 'Data Protection Act' was thrown up and continues to be cited as a reason for not sharing even though many times this is not the case. In the case of the implementations in Wales this has been overcome by participation of the professional who have concerns and treating the issues as an ethical dilemma rather than a legal one. In this way both patient and professional trust has been maintained and the resulting solutions 'more' than just required to meet legal requirements.

Comments:

There are other more obvious barriers in the sharing of information between public sectors for example between Health and Social Care. Here there are legal and perceptual barriers to sharing although not insurmountable they still do require an approach which maintains trust (not easy). The WASPI framework is at least a way forward in Wales as it provides a transparent basis for sharing. There are similar examples of information which would be of immediate benefit to citizens – Health and Fire services, Social Care and Fire etc. In many cases there are no real barriers but because there is a misunderstanding of the factors involved in such sharing and no agreed framework in place it becomes too difficult to take forward.

In addition it should be noted that while there are penalties for inappropriate disclosure there are no penalties for failing to share important information. This means the system support a risk adverse position which is often detrimental to patient care.

Question 8.

As head of Information Governance for the national programme in Wales were I to be aware of any such example I would already have taken action to rectify this issue. Of course, not to be complacent reviews and audits are an important part of the security, information and clinical governance of the NHS and are being 'built in' to new services. The work in supporting the Caldicott Guardians including the provision of a revised Caldicott for NHS Wales also eeks to makes sure that such inappropriate sharing does not take place.

Comments:

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

Question 9. The Data Protection Act works very well although it is a complex piece of legislation and often misunderstood. There is now accumulating a great deal of guidance which is very useful (it means more if from only one or two official sources – the ICO in particular). Changes to the Data Protection Act must be carefully thought through and of vital importance as such changes lead to new misunderstandings and interpretation. The work of the European ARTICLE 29 Data Protection Working Party - Working Document on the processing of personal data relating to health in electronic health records (EHR) is insightful and interesting in the suggestions made. I believe the ideas could be useful in making the sharing of information for appropriate uses easier to accomplish.

Comments: Only comment is that the purposes should be clear and 'purpose creep' not allowed into major projects / large national databases. Again, build bottom up, incrementally.

Question 10.

Second principle is vital otherwise there could be an 'open season' on use. Public bodies may do reasonably well in this respect – the difficulty comes in the very wide scope of some purposes. This may be practical and acceptable in some cases however there needs to be a guard on the uses of information and creep or slipping into another purpose – sometimes difficult for large public bodies. Private organisations may or may not have equal difficulties.

Comments:

Question 11.

Clarity of the use to which information collect can be put to 'in a manner not incompatible with the original purpose' or for purposes which are mandated. The perceptions of the public are that if information is collected in a large central database maintained by the government for purpose 'x'. The general feeling is (maybe media hype) that it will also be used for 'y' and 'z'. Actually of course it may be used for y and z – if so this should be made clear and if this benefits society in the whole be honest about that.

Technology are less of a barrier now than there were – the technology issues are now how to manage the technology and implement in a way that does not ignore the human factor. All the security in the world will not make a system secure on its own – procedures and how people interact with the technology have to be recognised and work in real life.

Institutional barriers actually tend to be people barriers caused by a misunderstanding of issues by those within the organisation or by a perception of risk and reluctance on behalf of the individuals who are the subjects

Comments:

Question 12.

The work of the Article 29 team is valuable and worthwhile incorporating either in the DPA or in other legislation. In terms of other powers the ICO already has a number of powers and if the resources were available to the ICO other powers may not be necessary. As it is the ICO that has to work within the confines of the legislation I would be willing to listen to any further powers they would consider useful.

Comments:

Question 13.

Not negatively – however there are obviously other UK Acts etc which complicate and add to the issues – specific legislation on sensitive data (abortion, venereal diseases, human fertilization, gender reassignment etc). There is also the common law duty of confidence which is very important within the Health sector. European law and developments have an impact in that there are differences some important (article 29) others less so.

Comments:

Question 14. Other than the suggestions by the article29 group no. These should be issues that can be resolved without recourse to further statutory powers. In wales consultation, engagement and participation have proved successful so far. Future work on identification whether that means professionals or citizens can be taken forward in the same way. This maintains trust.

Comments:

Question 15.

The area is a complex one and many problems stem from the lack of people with a good understanding (public and private sectors) not just of the legal issues but the spirit of the law and how it can work practically. Often issues get devolved to lawyers and this does not promote an ease of working through problems.

Comments:

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

Question 16.

Clear whether consent is needed yes (although many would disagree). However whether consent is needed is not always the appropriate question, ethically you ask is consent right – at least in the form of gaining from the individual an affirmation of the use of their information, i.e. respecting their right of self determination.

Comments:

Consent may be required or not. Consent can be implied or explicit. Informing people is necessary where consent is relied on simply in order to meet principle 1. Add in common law and ethics - it's no wonder that this is not understood or used correctly. See article 29 report mentioned earlier for an innovative debate on consent.

Question 17.

What form of consent ? Explicit, implied or self determination?

Explicit consent to sharing or use? To answer the question in a limited way, requiring consent can lead to poorly populated systems and a requirement of citizens to take positive action before being able to take advantage of services. If the majority of citizens believe these uses or sharing of information already should be taking place this is a burden being imposed on them for the few who wish this as an option and do not wish to take the positive step of opting out (opt out's or in are a related issue).

Comments:

Question 18.

The requirements on organisations (especially public bodies) with DPA and FOI are already considerable. Yes, organisations need to be open and transparent on the uses made of personal information. In public bodies this is already happening with FOI and this should be encouraged rather than changed at such an early stage. Existing right need explaining not strengthening.

Comments:

Question 19.

In Wales The WASPI is a good example although it needs appropriate resources allocated. What is not needed are high level policies that impose requirements without resources or the 'how' to do.

Comments:

Again it's a question of engagement and participation of stakeholders that at least tries to ensure transparency.

Yes the framework code of practice is useful as a starting point. On its own it leaves organisations asking how?

## **Section 5: Technology**

Question 20.

Massively so. Even the last 10 years have seen substantial developments which have not been match by procedural and people skills. There needs to be a shift from a focus on technology solutions (and technology driven projects) to more holistic designs which include all the aspects of business requirements, society and individual requirements, the benefits and risks posed (as well as the technology).

Comments:

Question 21.

Does the law need to mandate? In many areas (certainly public sector) good guidance, standards, certification should be enough. In private and public sectors such standards should be promoted and acknowledged in order to build confidence.

Looking at the wider requirements. Not to mandate technology but require in design the following elements : Prevention, detection audit and reactions. No system is 100% secure and to try and build controls that create such a system is bound to fail. Building in a full framework of access controls, detection of misuse and sanctions will work in the real world.

Comments:

There should of course be repercussions should public or private bodies not use accepted standards – ICO should be able to take to task.

Question 22.

If done properly, yes of course and this should be encouraged. In NHS Wales work has been progressing for some time to use pseudonymised or anonymised data exactly in this arena.

Comments:

There is not sufficient knowledge presently although it is growing. Barriers include a lack of understanding of the techniques which lead to a refusal to accept the safeguards.

## **Section 6: International comparisons**

Question 23.

Informing Healthcare has over the last two years requested scrutiny by international peers including Netherlands, New Zealand, Denmark and Finland. Their experience and view have helped shape the programme for Wales and further learning can be made of their good practice. There is also much to be gained from sharing knowledge and learning within the UK.

Comments:

Question 24. See 23.

Comments:

Question 25.

There are certainly examples of countries where the issues are more complicated because of the State boundaries (Canada and USA) for example. We need to make sure that our own boundaries do not prove to be barriers.

Comments:

Question 26.

Not specifically however our international colleagues would be a good starting point to investigate such potential differences of attitude.

Comments:

## **Section 7: Additional questions**

Question 27.

Whatever we do needs to be practical and workable within the services we provide.

Comments:

When considering these issue on data sharing it is vitally important that we introduce the concept of 'balance' ; Sharing vs Confidentiality. Often this can be seen as a choice but it is a judgement of how to share and maintain confidentiality.

**In Health and Social Care settings people do not die from breaches of confidentiality but do die from not sharing important information.**

Question 28.

Comments: