

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 Department of Health and the NHS Information Centre for Health and Social Care (The IC) has an active involvement in collecting and sharing personal information and in promoting appropriate information sharing across the NHS and its business partners. A wide range of information is collected, held and shared:

- (i) Information about NHS patients, including their contact details and the care and treatment provided to them by the NHS is sent to the Department, including the Medicines and Healthcare Regulatory Agency, or input by NHS staff into systems run by the Department and the the IC. Information is collected directly from patients. It is processed to support the provision of care and treatment to patients, to extract finance and management information and to support public health surveillance and medical research.
- (ii) Information about members of the public, political representatives, independent experts and others who write to the Department, make complaints, or have expenses paid for serving on committees etc. This includes MPs and local Councillors.
- (iii) Information about NHS employees is held within an electronic staff register and within a number of other databases which support NHS organisations e.g. knowledge and skills framework database, MTAS and also within the Department's collection of performance and outcomes statistics which reference lead consultants or GPs.
- (iv) Information about stakeholders involved or seeking to be involved in developing policy,

including those acting for voluntary or commercial organisations or on their own behalf.
(v) Information is also processed on employees of the Department for the usual reasons.

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

Question 2.

Comments: Key benefits are improved services, improved planning and better use of resources. Services may benefit an individual directly, such as improved healthcare, or may benefit society or parts of society, such as improving medical or environmental knowledge through research.

Question 3.

Comments: Key risks for individuals relate to the potential for information to be lost, stolen or misused, causing distress, loss of trust between patients and health professionals and/or harm - whether physical, emotional or financial - and that concerns about misuse and loss of privacy may lead to individuals becoming reluctant to access services or support important activities where information is needed. There may also be unwanted media attention in some cases.

For society, inappropriate or even too extensive information sharing may result in a cultural backlash which has the reverse of the desired effect as fewer and fewer individuals agree to provide information, or accurate information, or become reluctant to access services and lack of information makes services less effective, safe and possibly more expensive to provide.

Question 4.

Comments: Technology provides both the greatest opportunities and also the greatest risks where lack of training or education and poor working practices can impact upon many individuals at a time. Security needs to be aligned with the sensitivity and perhaps the business and financial value of information.

Question 5.

Comments: No comment

Question 6.

Comments: No comment

Question 7.

Comments: Better sharing of health information to provide safe care in emergency or urgent care environments would be beneficial. Current NHS IT infrastructure does not support such sharing. This is being addressed by the introduction of the NHS Summary Care Record as part of the NHS National Programme for IT.

Question 8.

Comments: No comment

Section 3: The legal framework

Question 9.

Comments: *DPA Strengths* - provides a comprehensive set of principles to be applied to data processing.

Weaknesses - not so much weaknesses in the Act itself but how it is interpreted and particularly its interaction with the Human Rights Convention and the common law of confidentiality. The act is also unclear in its application where there are many data controllers in common for a dataset and the definitions of personal data, significant harm or distress, disproportionate effort and specified purpose are all problematic at the margins.

Question 10.

Comments: The 2nd principle does not tend to feature as an onerous requirement in health care delivery where the common law of confidentiality will usually require that we process on the basis of consent or make use of anonymised information. However, the definition of a specified purpose is unclear and initiatives sometimes falter on whether or not they are a minor shift in emphasis or represent a new purpose entirely. Similarly, whilst use for research is explicitly recognised as compatible with this principle, other forms of secondary uses of data are not and this can constrain development of improved business processes where the change required is perceived by some as a new purpose.

Question 11.

Comments: DPA has become strongly identified as a barrier to information sharing rather than the means for ensuring that information sharing is legitimate. Also, many organisations do not have a culture that respects personal information sufficiently e.g. staff are poorly trained and there is a lack of management attention. Anecdotally, citizens often see data protection requirements as bureaucratic restraints, rather than as protecting or enabling their vital interests.

Question 12.

Comments: Much tougher sanctions for deliberate misuse of personal data should be introduced. Clarity on the data protection regime needed where databases are shared by a large number of organisations may require new provisions.

Question 13.

Comments: Already mentioned that the common law of confidentiality and Human Rights Convention are key considerations in decisions about sharing/disclosing patient identifiable health information.

Question 14.

Comments: There is a lack of clarity about the standards that should apply in order to satisfy the adequate security principle and mandating appropriate minimum standards would improve matters.

Question 15.

Comments: No comment

Section 4: Consent and transparency

Question 16.

Comments: The Department believes the consent requirements within the health sector are clear. For delivery of healthcare direct to patients implied consent is normally relied upon

on the basis that patients have been informed about and understand how their information will be processed. For other, secondary, uses such as management or research explicit consent is normally required. This is spelt out in the NHS Care Record Guarantee. As part of the NHS National Programme for IT the Department will be writing to all households informing them about how their information will be processed.

For example in 2006 the MHRA established the Independent Scientific Advisory Committee for MHRA database research (ISAC). The ISAC considers whether applications to obtain personal or potentially identifiable Yellow Card data for research that would be exempt under FOIA (Section 40 - personal information) are of scientific merit and should be approved. These are known as type 2 applications. If approved, applicants must also obtain ethical approval from a NHS Research Ethics Committee. Following ethical approval, the MHRA would contact Yellow Card reporters to see if they were prepared to participate in the study. The reporter would then contact the patient to see if they consent to participate in the study. Only once the reporter and patient have given consent would personal Yellow Card data or the contact details of patients or reporters be given to a third party.

Question 17.

Comments: Imposition of a requirement to gain consent for processing would have minimal impact in healthcare as consent is already a major requirement. However any imposition of a requirement for explicit consent would have significant and serious implications for the delivery of personal healthcare which relies largely on implied consent. The DH also exploits personal information collected for patient care for other (secondary) purposes such as planning and research once it has been anonymised. There would be serious consequences for NHS management and medical research if any imposition of a requirement for consent affected the use of anonymised data.

Question 18.

Comments: A standard and straightforward approach to conveying this sort of information would be helpful, particularly if this could be deployed on a website.

Question 19.

Comments: Clearer technical guidance from the ICO will help to improve transparency but is only ever likely to hit a relatively small audience of data protection practitioners who are often not involved in the development of policy. However the introduction of Privacy Impact Assessments would make a significant contribution as this will ensure such considerations are built in at the very earliest stages.

Section 5: Technology

Question 20.

Comments: Technological advances have made the collection and sharing of large amounts of data much easier and consequently considerably increased the risks of damage to individuals and organisations from poor security. However they have also provided stronger security tools for those prepared to use them. Within the National Programme for IT a comprehensive suite of security measures are being introduced which will significantly improve the security of patient data over current arrangements. For the Department of Health, improved security arrangements have made it straightforward to ensure that personal information on departmental laptops and removable storage is routinely encrypted with minimal impact on users, and that access to the Department's network is restricted to those with suitable authorisation. Use of the Government Secure Intranet supports improved sharing between Departments, but we need to be careful to avoid undue reliance on

technological solutions that may fail to deliver if not supported by staff who understand what the technology is doing.

Within the MHRA the ability to transfer data electronically has made it easier to provide reports of suspicions that a medicine might have harmed a patient known as the Yellow Card Scheme. To ensure that personal Yellow Card data are protected the MHRA developed "Guidance on the safe disposal of Yellow Card data by external users." This is available on the MHRA website at http://www.mhra.gov.uk/home/idcplg?IdcService=SS_GET_PAGE&nodeId=928. The guidelines are primarily designed to prevent accidental release of data to others through carelessness or inadequate IT safeguards which enable a third party to "hack" into the researcher's computer. In the past records could be kept under lock and key and it was clear to all how securely this data was held. The constant ability of hackers to find new ways of combating IT security systems means constant vigilance and review of IT security is required.

Question 21.

Comments: This would be welcome across the whole range of security technologies but it would need to be kept up to date. The Department has recently issues guidance to the NHS which states that the use of portable devices must be justified, risk assessed and, if use is deemed acceptable after risk assessment, security procedures equivalent to those described in Section 10.7 of ISO 27002 should be implemented.

Question 22.

Comments: Anonymisation and pseudonymisation will have a significant role in safeguarding personal privacy while at the same time enabling large data collections to be exploited for the public good. The Department is already actively developing such techniques which are expected to make significant contributions to medical research policy development and other secondary uses such as NHS business and financial management.

A major barrier to their use will be the lack of trust that individuals have in the public sector's commitment and ability to ensure that personal information is properly protected from inappropriate uses whether by government or others. A further barrier is also created where data quality is poor and organisations feel they will lose out financially if they don't have complete data to check.

Difficulties may also arise when using anonymised data relating to small groups, where, combined with other data that may be held, it may be possible identify individuals e.g. where rare illnesses or novel drug treatments are under consideration (e.g. the MHRA ask applicants for their yellow card data what other databases they intend using in conjunction with the requested information)

Section 6: International comparisons

Question 23.

Comments: No

Question 24.

Comments: No

Question 25.

Comments: There is evidence from Germany and Canada that the introduction of consent requirements into services which previously did not require consent has a major and detrimental impact on those services.

Question 26.

Comments: Many European countries have greater concern about sharing of personal information than the UK, though there are signs that this is the direction of travel here too.

Section 7: Additional questions

Question 27.

Comments: No comment

Question 28.

Comments: No comment