

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: personal information relating to Patient safety incidents including, person name, age, sex and sometimes address sent to the NPSA by NHS trusts. We make every effort to anomalies the data using sophisticated tools.
The NPSA collects the information via XML feeds from Trust risk management systems and via dedicated e-forms on the web. The NPSA filters, screens and cleanses the data before storing it on an operational Oracle database which is used for analytical purposes to identify trends and patient safety issues.

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

Question 2.

Comments: In the NPSA's case we can see potential benefits of sharing personal information to Trusts, Police, Medicines & Healthcare Products Regulatory Authority (MHRA), Coroners, Strategic Health Authority / Welsh Regional Office to protect members of the public in urgent and/pr severe cases

Question 3.

Comments: The general risks I can see are:

Getting the patient information incorrect in the first instance and following up on any actions before the information has been investigated. Identifying and naming a person prematurely opens up the Agency to possible legal action.

Question 4.

Comments: I understand scope to mean within the Agency, wider NHS, Healthcare industry etc and method to mean email, CD, extranet, internet, intranet, database access, ftp etc.

The benefits to us might be that we can share information quicker, without filtering out personal information, which is costly and time consuming thereby reacting to patient safety incidents more effectively. New technologies to share and disseminate information to Trusts, for example, are being looked into

The downside has already been mentioned.

Question 5.

Comments:

Question 6.

Comments: Private organisations hold or share too much information where they use this for unsolicited marketing purposes (spam post, fax, calls!)

Question 7.

Comments: ? Rapid reporting database and NCAS???

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments: In our opinion, DPA has raised significantly the public awareness and organisations' awareness as to be careful with holding and sharing of personal information.

Question 10.

Comments: Reasonably well.

Question 11.

Comments: More user-friendly encryption techniques (e.g. PKI infrastructure for emails)

Question 12.

Comments: Prison for perpetrators

Question 13.

Comments: n/a

Question 14.

Comments: No

Question 15.

Comments: We don't think this is the case.

Section 4: Consent and transparency

Question 16.

Comments: Yes, explicit consent where possible. (e.g tick box on form to be filled in by the reporter/patient.

Question 17.

Comments: Sometimes it is sheer impossible to get consent. E.g. where patient safety incidents have been reported by the NHS staff and reported to a central monitoring organisation.

Question 18.

Comments: individuals making more aware by ICO that they have access rights, and state that organisations should make this much easier for individuals (e.g. online form to be completed)

Question 19.

Comments: Guidance is welcome!

Section 5: Technology

Question 20.

Comments:

Question 21.

Comments: No, technology evolves; law is more static!

Question 22.

Comments: We use anonymisation techniques professionally within NPSA.

Section 6: International comparisons

Question 23.

Comments: no

Question 24.

Comments: Store personal information in local databases, and if needed nationally, than national databases should be able to make a query on these local databases (decentralised model of central data registration, as applied in Dutch health system)

The Dutch government has chosen a form of distributed architecture in which all clinical data is stored at source (i.e. where it was generated) and which can be accessed using a central patient registry that contains links between the patient and their locally stored data. The National Hub, a secure message broker in combination with a registry, coordinates all information exchange (see: <http://albertderoos.nl/?p=105> and http://www.ringholm.de/docs/00980_en.htm)

Question 25.

Comments: no.

Question 26.

Comments: no.

Section 7: Additional questions

Question 27.

Comments: n/a

Question 28.

Comments: n/a
