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.

Please explain what your interest in information sharing is.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

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

The Faculty of Public Health (FPH) is the leading professional body for public health specialists in the UK. It aims to promote and protect the health of the population, and improve health services, by maintaining professional and educational standards, advocating on key public health issues, and providing practical information and guidance for public health professionals.

As a professional body we create and promote international standards of practice and support their development in partnership with other countries.

Other important aspects of our work include forging alliances across all sectors of society with those with an interest in public health (particularly local government), identifying and reducing inequalities and promoting academic research.

The FPH also seeks to promote public health by engaging with the public, particularly through the work of its members in primary care organisations.

The FPH itself holds a limited amount of personal information on members, training and examinations, as well as projects worked on by committees. Our main interest in responding to this consultation is that our members, who work in the NHS (Primary Care Trusts Hospital Trusts, primary care), voluntary and independent sector organisations, government departments, local authorities and universities work extensively with personal information. They collect, hold, use and share information on a regular basis for a wide range of purposes, including service delivery, measuring health status and inequalities, needs assessments, research and evaluation.

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.

A lot of public health work is based on secondary data, usually anonymised / pseudonymised. However, there are some core public health functions that require named personal health data. This includes surveillance and disease registries (e.g. cancer and congenital abnormalities registers)

a) Benefits to individuals

1) The benefits to individuals are wrapped up in the benefits to society (See b below):

- Identifying people at risk of ill-health or disease, identifying possible causal pathways, improving services, risks and benefits at the individual level can be calculated

2) Health services research improves patient care. This requires data sharing between researchers and service providers and is dependent on the collection and sharing of personal data. While data can be anonymised for analysis, personal identifiers need to be collected and shared to avoid double counting and to link different care episodes that belong to the same person.

- For example, three studies illustrate the valuable contribution that health services research has made. One showed that discharging patients from adult intensive care units at night is dangerous, another showed that the quality of care for some conditions improved when payment for performance for general practitioners was introduced, and the third established that the outcome of some surgical operations improves when a surgeon or hospital carries out the procedure more often. None of these would have been possible without the collection of personal information. (Examples from Black N, BMJ 2008; 336: 112-3).

3) The individual also benefits when getting a service or getting a more streamlined service. For example, in multi-agency working, information around family/social support and health needs are shared to enable packages of care to be delivered.

- For example, children can be identified who have repeatedly attended A/E departments (by presenting condition) by analysing GP and Hospital records respectively. This purpose requires patient identifiable data from both sources to be linked so as to identify those individuals most at risk.

b) Benefits to society

Routine data derived from the collection of personal information is used in the following ways:

- To track historical trends
- Conduct operational research e.g. to inform services
- Community diagnosis – identifying health problems and inequalities
- Assessing individual's chances – survival and risk
- Completing the clinical picture (linking information from various sources e.g. primary care, secondary care and community sources)
- Identification of syndromes – through investigating recurring patterns
- Getting clues to as to possible causes of ill-health, diseases and the wider determinants.

(From Morris JN, International Journal of Epidemiology 2007; 36:1165-72)

Data sharing is important to ensure effective use of information for the above purposes:

1) Databases and registers are set up.
2) Data are compiled in a database (adding more subjects to the database from different agencies – completeness of the information)
3) Data are linked from various sources (adding more variables thus enabling research into syndromes, associations and possible causes; understanding patient pathways)
4) Databases and registers are kept up to date in as real-time fashion as is possible (effective data sharing makes this process more efficient)
5) The validity of data are checked by linking / checking that the common/core variables are the same and up to date.

Examples below have benefits to individuals and to society:

- Data from Hospital Episode Statistics (Patient Episode database in Wales) and the Cancer Registries are used to monitor the distribution of and trends in disease, to improve the quality of care and to improve understanding of the causes of disease - without data sharing none of these would be possible.

  HES/PEDW is episode based, whilst cancer registries consolidate a person based record by matching and merging inputs. At present, personal data is essential for that process, as the information for a single person comes from multiple sources. The UKACR booklet demonstrates what UK cancer registries can provide for the ultimate benefit of cancer patients, both to reduce risk and to improve outcomes.

  Reference: UKACR, United Kingdom Association of Cancer Registries. Reducing Risk and Improving Outcome.(Available from http://nycris.org.uk/reports/ukacr.htm

- Investigating inequalities of care (e.g. areas of high mortality rates, high emergency admission rates, high attendance at A/E departments or high abortion rates
- Investigating unequal provision of particular services (e.g. support from medical or social services to patients who are elderly or disabled or those with learning difficulties).
- Environmental and Health Protection require data sharing in dealing with incidents, in planning and emergency responsiveness, and investigating potential causes of threats to health (e.g. a cluster of rare disease)
- Using laboratory data to follow up cases of Salmonella or E Coli 0157 as part of outbreak investigation to find a source to protect public health or to follow up individuals so they can be protected

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

Key risks are the result of inappropriate disclosure:

1) Confidential information is breached, subjects are identified from data. This results in individual harm related to inappropriate disclosure.

2) Loss of public confidence leading to automatic refusal for even holding data or processing it – voluntary withdrawals from registers / withholding consent

3) This leads to incomplete data on registers and databases – non-representative – so threatens the benefits and use of these registers in the first place. Threatens service delivery if the client base selectively withhold consent.

Example:

Very little data would need to be removed from cancer registries to render population cancer survival estimates useless. Not knowing about a single case may have important public health effects.

A published example [Epidemiology Community Health (1994), 48: 232–236] is the investigation of a potential cluster of leukaemia and non-Hodgkin's lymphoma in 0–14 year

old children living in the vicinity of the Dounreay Nuclear Reprocessing Plant between 1968 and 1991. There were 9 cases in this age group. Great care was taken to ascertain and verify all cases. With all 9 cases the increased risk (2.58 times higher than expected) was statistically significant (95% CI 1.18, 4.90). If only one case had not been known to the registry (e.g. after being deleted), the increased risk (2.29 times higher than expected) was NOT statistically significant (95% CI 0.99, 4.13), with potentially different actions resulting.

4) Information becomes viewed as a commodity – bought and sold? This feeds accusations of nanny state, when the purpose is legitimately for the public interest.

Example:

There is always a balance between the interests of the individual versus the interests of society. Subjects do not want their information shared or processed when it is not in their personal interest. It is in the public interest to share this personal data e.g. to prevent transmission of disease or investigate a possible cluster. This conflict has given rise to recent high profile cases around patient confidentiality.

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.

Opportunities:

Scope [what information is shared?]

1) There is a distinction between anonymised data (can never trace origin) and pseudonymised (someone has a key). Anonymised data sharing has the least risks but limited benefits – as secondary linkages and further processing for legitimate purposes are not possible.

2) We would see large benefits and lower risks from pseudonymised sharing (i.e. of the secondary uses kind) as for example proposed in the Secondary Uses Service / NHS Connecting for Health and also by Health Solutions Wales. In non routine sharing transactions, the issuing agency (e.g. a Hospital) should delete all identifying information for individual patients (removing NHS Number, Hospital number, name, Date of Birth, demographic details etc.) and replace these with a single serial link number for each individual patient. A few other data items can also be “converted” if really necessary. For example, date of birth can be converted to “Age” and postcodes be given another serial number.

3) The creation of linked databases for research and for city/neighbourhood planning. For example, regular data sharing is required between PCTs and Local Authorities. The level and detail at which data is shared differs from area to area according to formalisation of local partnership arrangements and interpretations of the need to know.

4) Personal identifiable data is sometimes needed – governed by the need to know. For example, tracing contacts and following up cases for health protection and/or health surveillance.

Spectrum [how shared?]

Electronic data sharing by email is efficient, and paper-free. Electronic transfer of information needs to

take place via secure routes, encrypted and/or password protected.

Electronic transmission also enables subjects to be copied into correspondence or informed electronically of the scope of data shared (where it is necessary to also keep the subject informed).

Data warehouses represent an opportunity for better data sharing. They are efficient and the data can be centrally stored, secured and validated.

Risks:

1) Security breaches - unauthorised or unnecessary access to personal data. Good encryption software is needed. For example, the data sharing that takes place between pathology laboratories and cancer registries in USA is done in real time via secure internet links.

2) Inadvertent disclosure. Example - disclosure by subtraction (patients become identifiable when linking two data sets)

3) Occasionally the public health need to know is overridden by too stringent data sharing controls. This need to know is not automatically catered for, as it comes under one of a number of exemptions (Sections 30 -33 of the Data Protection Act). For example, Exemption 33 enables data processing for statistical, research and historical trend purposes, and the further processing of data originally collected for another/related purpose. Being an exemption, there is the onus to prove that the purpose of data sharing is not incompatible with the original purpose for which the data were collected.

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

Too much data

1) Duplicate data sets (particularly if not good quality or not up to date). This gives conflicting messages and not a true reflection of the subject. Duplicate systems are inefficient – the need for data cleaning and updating, storage and security are also duplicated.

2) Various sources are not linked. There is a need to plan services jointly and also need to understand the association between the wider determinants and health. For example, a lot of time is now spent in Local Area Agreement planning and in Joint Strategic Needs Assessments in compiling data from various sources.

A key principle set out in the National Statistics Code of Practice (Protocol on Data Matching) (http://www.statistics.gov.uk/about/national_statistics/cop/downloads/NSCoPDatamatching.pdf) is that "In order to reduce the burden on data providers and to fully exploit the value of existing statistical sources, data matching should be used in preference to creating new statistical sources, wherever possible, and where the results are likely to be of comparable quality. The range of attributes used to establish a common identity will be the minimum necessary for the matching operation to succeed." In other words, data matching (linkage) requires personal identifiers (which can subsequently be deleted or stored separately). Without data matching new and duplicate data collection may be necessary, increasing the risk of inadvertent disclosure.

Too few data

1) In relation to many areas of the health service we have poor or incomplete national data - e.g. in relation to primary care there are no national databases equivalent to Hospital Episode Statistics for secondary care.

2) Routine data sets do not cover all variables of interest e.g. information on lifestyles. Members of the public assume that their GP holds complete and up to date information on their lifestyles and health risks. For example, respondents to a lifestyle survey have commented in their response that as their GP already holds this information, the cost of running this survey was not justified. In reality, some patients would have that information recorded but it would not be up to date and the coverage would be incomplete for all patients registered with the GP.

3) Another deficiency in most medical records is the lack of indication as to whether the patient's condition improved or not, or when any change occurred. Sometimes changes in clinical data is recorded (such as haemoglobin levels in an anaemic patient) but not problems or symptoms experienced by the patient such as tiredness or pain. If the latter are recorded it is mainly in "Free text" rather than in a coded form which can be analysed statistically.

4) Up-to-date telephone numbers/contact details for clients/ patients/ population in an area are not available to public sector organisations. For example, running a telephone (lifestyle) survey is expensive as you would need to buy-in the telephone numbers via a marketing company. Telephone sample surveys are used extensively in the US. Postal surveys have had such a poor response.

Question 6. 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.

With respect to data sharing – Private and voluntary organisations are contracted by public sector organisations for specific purposes. Sometimes, they are viewed by the public with suspicion. This limits the scope of what they can do with the data that is in the public interest e.g. private research companies/consultancies.

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.

Please explain as fully as possible why information is not being shared, detailing what the barriers to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.

1) In Scotland, the sharing of information between the population census and hospital discharge data has been beneficial (an anonymised data linkage project) but this is not happening in England. There would be considerable benefits in terms of understanding the social determinants of health.

2) There are problems in linking details of care provided in private institutions to medical records

relating to care provided in the NHS.

3) There is a new focus on social marketing for public health – using the tools and expertise developed in the private marketing sector for public health improvement and campaigns. We need to get the market profile of patients/clients, and reach or access them with appropriate health promoting messages. This is a new area, and needs to be developed – not least of which this requires data sharing agreements to be put in place public and private sector organisations that are robust and monitored.

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.

Please describe the information-sharing concerned and why you believe it should not be talking place, including the risks involved in such information-sharing.

Perhaps security breaches? This can be due to genuine mistakes, e.g. attachments to emails (not removed or not encrypted). Or lack of understanding of security procedures – e.g. insecure transfer of information especially electronic means (email, CD, memory sticks)

Illegitimate access to records? E.g. where staff in an institution (Hospital, GP Practice etc) obtain access to the personal records of other members in the same (or related) institution. If a consultant goes "off sick", for example, then many staff are likely to wonder what the problem is, and they often find out!

Interpreting the duty of care versus patient consent? E.g. where hospital consultants informed GPs of the diagnosis of individual patients, and these patients have objected strongly to this happening without their consent.

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.

Strengths

1) The emphasis on need to know, and fair processing requirements

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Is access to personal information limited to those with a strict need to know?

2) The requirement for subject consent

- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?

3) The onus on the data -controller for security

- Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?

4) Exemptions to safeguard the public interest.

Weaknesses (are mainly in the implementation)

1) Consent to share

- If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?

Many agencies are now reluctant to share data because of “confidentiality concerns” even when to do so would obviously be in the patient’s interests. Good practice guidance on consent is needed (perhaps expanded from what is in the Framework Code of Practice and interpreted locally by organisations/businesses in their local codes of practice)

2) Storage duration

- Do I delete or destroy personal information as soon as I have no more need for it?

How long to keep records? What kind of backup constitutes good practice e.g. destroy paper but keep electronic? What about photographs and consent forms?

One may need the records for other purposes not the original purpose. The Act provides that personal data processed only for historical, statistical or research purposes in compliance with the conditions set out in section 33, may be kept indefinitely. (Section 33(3)).

3) Quality of data

- Am I sure the personal information is accurate and up to date?

The fourth principle (data will be accurate and up to date) doesn't always work well - e.g. we do not do enough to validate the quality of routine data:

4) Staff training.

- Have I trained my staff in their duties and responsibilities under the Data Protection Act, and are they putting them into practice?

For example, staff on induction are asked to sign a Confidentiality and IT use policy, but are not trained on, or not supplied with hardware /software for remote working or secure transfer of information (e.g. encryption)

Other issues:

1) One problem with the DPA 1998 is that it is open to interpretation. How exactly are "fair" and "lawful" processing to be defined? On the one hand it seems quite liberal and on the other hand restrictive.

2) There is a distinction between individual level pseudonymised data (which is personal but not personal identifiable). It is important to differentiate between patient/person-identifiable information and pseudonymised (but person-specific) information (such as HES). The requirements, in terms of confidentiality and security, are very different. Public health needs the capability to link person-specific data (either through an anonymised identifier or through fuzzy matching of other variables).

3) There needs to be a review of the DPA 1998, the Common Law duty of confidence, the Human Rights Act 2000 and the FOI Act 2000 with a view to simplifying and clarifying the situation for health data.

For example, the Scottish judgement ruled that barnardised data was not personal data.

"I have come to the view that a table setting out the census ward data for 1990-2001 for the Dumfries and Galloway postal area, barnardised in the manner described, would not constitute personal data of any of the children resident in Dumfries and Galloway who had in a relevant year been diagnosed with leukaemia," said the judgment. The case involved the seemingly competing demands of freedom of information legislation and data protection laws. It is thought that a major proportion of cases going to the Scottish Information Commissioner relate to the interaction between FOI and data protection legislation.

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 and the reasoning behind your response.

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

With respect to data held only for specified lawful purposes – Generally, public bodies adhere well to this principle, with systems and processes in place. In practice it is valuable in identifying information needs and processing requirements.

With respect to further processing – it is very difficult to know in advance exactly how data can be used to benefit individuals or society. Novel ways of using patient data are being discovered all the time e.g. testing new hypotheses or using new methods of analysis. In this context the exemption in Section 33 is valuable, as it provides for further processing (not incompatible with the original purpose).

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

No specific comments

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

Some form of audit/inspection? This is partly delivered by the role of the Information Commissioner

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.

This European Directive does not seem to have caused much trouble in Europe apart from Germany where cancer registration failed. It is superfluous. It seemed to trigger the problems with GMC guidance in UK.

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? Please provide examples and any steps you believe could be taken to improve matters.
A clear distinction is to be made between those with a need to know identity of subjects and those who do not need to know (where anonymised / pseudonymised data are sufficient) a) **Need to know**: e.g. preparing multi-agency care packages – here there is a need to share identifying data between agencies. Different agencies hold different identifiers e.g. Child Health NHS number and social care Child Reference Number. Medical records – details relating to one patient may come to be stored in the records of another with a similar name or address etc. Use of Barcodes etc. to identify patients rather than typing in 10-digit NHS numbers or identifiers could help here b) **Do not need to know**. Removing personal identifiers and holding them separately is an important measure for research, service planning and other secondary uses.

Question 15. Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples. Please outline your proposals for streamlining the legislation to ensure that such burdens are minimised.
Private organisations need to make a profit, and arrangements for data sharing need to be included in any contract placed with them as regards patient care. ONS disclosure guidance was very useful for PCTs and others – similarly good practice guidance is needed for data sharing agreements between public and private sector organisations

<u>Section 4: Consent and transparency</u>

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.
It is not at all clear - there are constant discussions about implicit and explicit consent. For example sharing of hospital discharge data happens with implicit consent and it is difficult to see how we could feasibly collect this kind of information or complete cancer registration data if explicit consent was required:: It is also not clear if patients would consent to further processing that is within the Data Protection Act under Section 33 exemption for statistical or research purposes. Although this is legitimate under the

Act, ethical clearance committees might sometimes rule against it as specific consent was not sought.

For example, lifestyle data was obtained by survey to identify lifestyle habits in a population. The consent form covered this original purpose. Could the data then be linked to a PCT held database on primary care or a separate research database or cancer registry or shared with patient's GPs to update their records? For each of these linkages, the case could be made for the public/societal benefit – but subjects' consent was not sought originally.

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

This would almost certainly undermine the usefulness of cancer registries and other routine data sources in the UK - the lack of completeness and the selected sample taking part would make them useless for monitoring changes in cancer epidemiology and management and in supporting quality improvement.

There are real problems with patients who do not have English as their first language, and with those who do not fully understand the possible adverse consequences of giving consent.

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?

The Freedom of Information Act has been well publicised and used (e.g. by members of the public and lobby groups).

The public register of data controllers is sufficient via notification to the Information Commissioner; as this includes a statement of the types of data and their purpose.

There may be a need to have a detailed declaration available locally, for example, a Board level register.

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)?

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December (www.ico.gov.uk)?

Most professionals are unaware of the existence of this code of practice (published in Oct 07 or even the preceding consultation).

It is useful that the code has been highlighted in this consultation – as it gives guidance in general terms as when and how to share data fairly and securely. However, this does need to be interpreted locally with examples for each organisation as to what information is shared and how it is shared. These local codes of practice become meaningful to staff and patients.

To facilitate this, information governance leads in organisations need to ensure these developments are publicised, and that local codes of practice are developed. For example in PCTs, local codes should be explicit about the framework within which further processing could take place and data sharing without explicit consent under the Section 33 exemptions.

With regard to privacy impact assessments, these mirror the health impact assessment methodology that public health professionals are used to. However, the duty and the methodology have not been widely shared or publicised within the public health community. Privacy strategies could be embedded as a requirement for organisations, with the depth and scope left to individual organisations (according to breadth and scope of its functions).

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.

1) Information Technology provides far greater opportunities for information sharing and illegitimate access to personal details than paper records ever did. Obtaining access to paper medical records for anyone apart from local professional staff caring for patients was always quite difficult. No-one could just walk into a medical records department and find the case notes they wanted, for example.

Computer records can be accessed by secretaries, nurses, paramedical staff, laboratory and X-ray staff etc. (without individuals being able to be named because they all work on shift rotas).

2) Computer databases can in principle be trawled for identifiable information through search queries(e.g. for any details of people living at particular addresses or with particular diseases etc).

3) Any identification number based on biometric details of individuals (fingerprints, Iris scans. DNA etc) would be dangerous in that unlike a bank PIN number, it could never be changed even if it became widely known (e.g. to the Press, etc.)

4) On the other hand, technological advances have made information sharing more efficient, and linkages between various sources of data have become automated.

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?

Password protection and encryption render the data useless without the access rights/code. However, the public are suspicious of any “technical” means of data protection, believing that all “codes” or “encrypted records” can be “cracked”.

More emphasis should instead be placed on anonymisation and use of serial number codes to replace identifiable fields.

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?

This is an important measure that we strongly support. This enables personal data to be shared and used without identifying subjects.

Example:

Connecting for Health Secondary Uses Service will deliver this function for the NHS (Health Solutions Wales) – but there is a need to grant access rights for researchers who need identifying data for linkages or to be able to contact subjects.

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.

More extensive use of linkage methods in Western Australia has reduced the need to use identifiable data - see the graph at http://www.datalinkage-wa.org.au/go/data-linkage/privacy-protection

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?

No specific 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?

A previously introduced requirement for informed consent in parts of the former East and West Germany led to the effective collapse of cancer registration.[1] A similar situation developed in Hungary. Ascertainment fell to an estimated 70% or less, partly because patients withheld their

consent but partly because doctors did not ask for consent, either because they forgot or because they did not feel it was appropriate to seek consent from a person already weighed down with the implications of a diagnosis of cancer. Research indicates that people exercising their right to withhold their data would differ systematically from the rest of the population leading to unquantifiable selection bias and reducing greatly the reliability and value of the data. In fact, some of the most seriously ill patients with the poorest prognoses would not be able to give their informed consent, leading to apparent but spurious improvements in national cancer survival statistics. We have not been able to find a single example anywhere in the world of a population-based cancer registry or clinical audit operating successfully on the basis of informed consent. By successfully, we mean having data of adequate quality to be included in international comparisons, and producing local and national output which is likely to have some real impact on morbidity and mortality from cancer.

Although we have read a description of an elaborate system designed to deal with privacy, security and confidentiality concerns in Germany,[2] people should not accept this solution uncritically. Only a small proportion of German cancer registry data is included in international comparisons of incidence and survival implying deficiencies in data quality and, to our knowledge, any useful output from the German registries is extremely limited. Writing about the German anonymisation solution in the journal The Lancet Oncology, and based on his own experience, Joachim Dudeck concluded that "This model cannot be recommended".[3] In fact, apart from a specialist childhood cancer registry, the only German data included in recent European comparisons of cancer survival[4] was from the Saarland Cancer Registry, which covers a population of just over one million and represents a small fraction of the total population of Germany. Until recently, cancer registration in Saarland operated under a state law which allowed physicians to notify new cases of cancer to the registry without the consent of patients. Dr Hartwig Zeigler, from Saarland Cancer Registry, has told us that "This is the main reason why the Saarland Cancer Registry is still the only one in Germany which can present reliable, valid and complete incidence data of the area covered".

References:

1. Becker N. Cancer epidemiology and privacy laws: recent trends in Germany. Eur J Cancer 1993; 29A: 661-3.

2. Blobel B. Requirements and solutions for security and privacy in medical registries. Br J Healthcare Comput Info Manage 2001; 18: 28-30.

3. Dudeck J. Informed consent for cancer registration. Lancet Oncology 2001; 2: 8-

4. The EUROCARE Study

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.

No specific 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?

No specific comments

Question 28. Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.
There should be more emphasis on the benefits of sharing data and on the risks of not sharing data: There should be more emphasis on pseudonymisation and anonymisation techniques to enable more secure data sharing

Full name	
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)	Information & Intelligence Committee (c/o Lindsey Stewart)
Date	14/2/08
Company name/organisation (if applicable):	Faculty of Public Health
Address	4 St Andrew's Place, London
Postcode	NW1 4LB
Address to which the acknowledgement should be sent, if different from above	
We work on the assumption that we will publish the responses we receive. Please state explicitly if you want all or parts of your submission to be treated as confidential, explaining why. Please note, that this does not in itself guarantee confidentiality (see 'Publication of summary of responses' section below).	

We intend to hold more in-depth interviews with certain respondents. Please indicate if you would be happy for us to contact you.	Yes, I would be happy to be contacted ☒ No, please do not contact me ☐

Publication of summary of responses

Following the end of the consultation we will publish a paper summarising the responses. The response paper will also be available on-line.

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004). Although information held by the Review Team is not covered by the Freedom of Information Act we intend to operate a voluntary access scheme in keeping with the FOIA, and please be aware that the majority of the Review's information will be handed over to the Ministry of Justice for long-term preservation at the close of the Review, and the Ministry is covered by the FOIA.

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Ministry.

The Ministry and the Review will process your personal data in accordance with the DPA.