

Data Sharing Review – Consultation

(Richard Thomas & Dr Mark Walport)

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 Patient Information Advisory Group (PIAG) was established under Section 251 of the NHS Act 2006¹ to advise the Secretary of State for Health about issues related to the processing of patient information in addition to advising on powers under Section 251 of the Act². These powers permit the common law duty of confidentiality to be lifted for activities that fall within defined medical purposes, where anonymised information will not suffice and consent is not practicable. This legislation applies to England and Wales and to the processing of any patient information for secondary uses. It therefore covers data held by both the NHS and independent sector providers and to medical data held in a variety of records and databases. Medical purposes include preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services.

The Patient Information Advisory Group's interest, therefore, is not as a user of personal information but as a regulator of both personal and de-identified information collected in a healthcare context. Consequently, our response will focus on issues related to data-sharing in the healthcare context, and consider, in particular, issues related to confidentiality. Our response will also include reflection on recent events related to inappropriate data-sharing in other contexts and draw on our experience from consideration of such issues over the last six years.

Our response has endeavoured to address your questions as asked. An Executive Summary is also included which draws out what PIAG considers to be the key issues.

¹ Originally under Section 61 of the Health and Social Care Act 2001 but re-enacted under the NHS Act 2006.

² Originally, Section 60 of the Health and Social Care Act and re-enacted under the NHS Act.

Executive Summary:

This Executive Summary is intended to highlight those issues PIAG regards as key and to make some recommendations.

1) Presumption in favour of disclosure or withholding data?

The most fundamental issue is the apparent presumption in this consultation document towards data sharing; whereas, with respect to confidential information, the presumption should be not to share information. Generally, sharing of confidential information should only occur where there is good reason to do so and with the consent of individual(s) to whom the data relates. There are, however, circumstances where data may be shared without consent, for example, where there is a statutory basis or a substantial public interest that favours disclosure over maintaining confidentiality. Use of the substantial public interest justification should be the exception, however, and not the norm. In the health context, breach of confidence can do serious harm to the clinical relationship between patients and clinicians and could lead to patients withholding vital information from clinicians or not seeking treatment with potentially serious consequences for their own and others' health.

2) Factors to consider for data-sharing

The consultation document asks questions about data-sharing in a generic manner. This reflects the nature of data protection legislation but fails to take account of the fact that different issues arise and are relevant to different types of data and in different contexts. There are particular issues in relation to health information because of its confidential nature or because it is sensitive³ information.

Consideration of the appropriateness or otherwise of data-sharing needs to take account of:

- a. the type and nature of information to be shared
- b. the extent to which the information is identifiable or could be linked with other data to render it identifiable
- c. with whom it is proposed that information is shared
- d. the purposes for which it is to be used
- e. whether the individual is aware of such information sharing
- f. whether the individual has consented to the defined information-sharing
- g. the actual and potential benefits and disbenefits both for individuals and society
- h. whether there are appropriate security and confidentiality safeguards in place to ensure that personal information is not then disclosed onwards to

³ We are aware the term 'sensitive' has a particular meaning in DP terms but in this context, we are using it with its usual meaning of information about which individuals are sensitive.

others.

Consideration of the particular circumstances in the light of Beauchamp and Childress's four ethical principles⁴ of autonomy, beneficence, non-maleficence and justice may be helpful in arriving at a decision.

3) Confidentiality

Some have argued for a 'risk-based' approach, we believe that whilst risk analysis may be helpful in informing decision-making but ultimately decisions to disclose personal information should be derived from first principles, particularly with respect to confidential information. Because by its nature the information is confidential and imparted with an expectation of confidentiality, the decision to disclose such information should not be taken lightly. Although not absolute the legal protection afforded to confidentiality is strong, and in fact, it should be easier to make a successful case for breach of confidence than clinical negligence for example. Some disclosures currently made would result in legal censure but few have taken legal action. The most likely reason for this is that people are largely unaware of how their personal and confidential information is used and shared. Additionally, because people are sensitive about the information they may elect not to risk further disclosure or difficulty obtaining services by complaining. It is very important therefore that the law protects people's data to prevent inappropriate or unlawful disclosure rather than simply creating penalties after the fact. That said penalties and fear of litigation have their place in providing an incentive for organisations to take data protection and confidentiality seriously.

4) Barriers or Boundaries?

The consultation asks about barriers to information-sharing. It is important to differentiate between technical barriers and barriers used to safeguard boundaries. Technical barriers such as a lack of interoperability between data and systems, should be addressed to facilitate legitimate data-sharing effectively and securely. Some barriers however are deliberately and appropriately used to maintain the legal and ethical boundaries by preventing unlawful or inappropriate data-sharing. This distinction needs to be understood and considered when identifying whether a barrier is a genuine barrier or is there for the legitimate purpose of safeguarding personal information.

5) Transparency

A key issue as illustrated above is the need for organisations to improve the transparency of the purposes for which information is used and with whom it is shared. The NHS has gone some way to doing this through the development of the Care Record Guarantee and the public information campaign that underpins the roll-out of the Summary Care Record, more however could be done. PIAG has sought to improve the transparency of data use in relation to applications for support under Section 251 of the NHS Act 2006. by placing as a condition of approval on many

⁴ TL Beauchamp and JF Childress, Principles of Biomedical Ethics (5th Edition OUP Oxford 2001)

applicants that patient information materials are developed and disseminated. Greater transparency strengthens the basis for implied consent, where this is appropriate (i.e. for direct care purposes e.g., where independent sector providers are used to deliver NHS care).

6) Organisational culture

The key element to ensuring that data is held securely and confidentially is for organisations to create a culture of protection for personal and confidential information. This needs support from the most senior staff to invest in training and staff awareness and taking account of the additional work and technical resources needed to ensure that appropriate safeguards are taken. Codes of practice and an internal oversight committee can define who may access personal or confidential information, for specified purposes and the rules that should govern its use.

Recommendations:

1. We suggest more training to ensure that clinical staff, researchers and managers understand the law, particularly the common law duty of confidentiality.
2. The development of an organisational culture that supports the protection of personal information from the most senior level down. Codes of practice that define which staff may access and process personal information for specified purposes are useful to underpin this.
3. We recommend that organisations are required to undertake routine information audits to assess what type of personal information is being held and why and to conduct regular reviews to establish whether data needs to be retained in identifiable form.
4. We would also suggest that a description of the data being held and the extent of its identifiability or likely sensitivity should be available to the public.
5. The Information Commissioner, Healthcare Commission, proposed National Information Governance Board and other regulators with a remit that relates to the processing of information should be given stronger powers to investigate, monitor and make recommendations or even place requirements on organisations where failures are suspected or found. These should include a wider range of penalties for systemic failings, negligent or malicious misuse of data both for the responsible organisations and for individual staff working within them.
6. The Information Commissioner could consider how it might create a requirement for organisations holding personal information to record and implement an appropriate range of consents with respect to purposes and data-sharing and that adopts a pragmatic approach with respect to the timing of seeking consent where there are issues of causing distress e.g. immediately after diagnosis of a serious condition is unlikely to be appropriate..
7. Consideration could be given to how to relate the legal requirements related to compliance with the seventh data protection principle more closely to compliance with Information Security standards.
8. Finally we would very much welcome a full and open debate with the public, similar in scale and breath to that generated in relation to opt out for organ donation.

Please answer any of the following questions where you have an opinion.

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.

Information-sharing can provide a range of benefits in the healthcare context such as improved patient safety, better co-ordination between services to provide more effective and streamlined service delivery. Other potential benefits include new knowledge derived from good quality medical research, which in time could lead to improved care and treatment. Patients often assume that their information is being shared, for the purposes of providing them with care, and may be irritated at having to repeat, for example, their demographic details.

It is difficult to assess the benefits, to either individuals or society, without reference to the specific purposes in a given context. Similarly, there is a need to consider whether benefits and disbenefits are actual or potential, and to balance these both in relation to individuals and to society. The question, as framed, is therefore rather unhelpful and consequently difficult to answer in a meaningful way.

Question 3

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

Generally, identifiable information (i.e. personal information) can be shared either:

- with the consent of the subject, or
- under statute, or
- where the balance of public and private interests favours disclosure. In the case of confidential information, there must be a substantial public interest favouring disclosure, which outweighs both the private interests of the individual concerned and the public interest in safeguarding confidentiality.

The main risk associated with sharing personal information is that, once disclosed, the disclosing body has no substantive control over how that information is then used or whether it is disclosed to others. This affects the individual to whom the data pertains in that they would then have no knowledge of any misuse or inappropriate disclosure and would not be able to exercise any control over their personal information. Aside from concerns about any sensitive information, people view

protection from the misuse and exploitation of information about private lives as something that will continue to be important in the UK. ⁵

This has been an issue for UK Biobank with respect to the provision of personal information by the Department of Health and NHS bodies to UK Biobank for the purposes of inviting them to participate in this research project. The disclosure included NHS number but no clinical information. It is the disclosure of name, address and date of birth, which has been of primary concern because of fears of identity theft.

In relation to confidential information, inappropriate data-sharing constitutes a breach of confidentiality. This may have serious consequences for individuals e.g. where confidential information is put into the public domain by the press, but even where the data is not then misused by the recipient, (e.g. medical researchers, on the whole, treat confidential personal information responsibly) the fact their confidentiality has not been protected may be perceived by the individual as a breach of trust. In the healthcare context, this might do serious harm. If patients do not trust the confidentiality safeguards within the system then there is a risk that they may not seek treatment e.g. for Sexually Transmitted Infections with its attendant public health concerns or they may choose to withhold sensitive information from treating clinicians. Such information may be crucially important to their care and treatment or for others.

It has long been custom and practice for the NHS to make confidential patient information available to medical researchers, without seeking consent. It was one of the key reasons for the powers under Section 251 to be established in law, as they provide a means of lifting the common law duty of confidentiality, where there is sufficient public interest. Section 251 powers are only to be used where it can be demonstrated that anonymised data is not fit for purpose and where seeking the consent of the individuals concerned is not practicable, 'having regard to the cost and technology available'.

PIAG was established, in part due to the recognition that that sharing information can bring substantial benefits, but also in part due to the acknowledgement that data-sharing needs to be carefully regulated particularly where consent has not been obtained for the disclosure. It is our experience that the seriousness of these disbenefits and risks can easily be under-estimated by those accessing personal information, generally with good intentions including many in the NHS and the research community. What is apparent is that previous custom and practice did not have a secure legal basis and it is likely the only reason it has persisted is because of the level of public ignorance. This situation is rapidly changing and it is clear that the 'old ways' are no longer tenable. as evidenced by the recent High Court Case of

⁵ 96% of people in the UK polled in the special eurobarometer (225/ Wave 63.1) on 'Social values, Science and Technology' thought protecting information about private lives from misuse and exploitation would be important (77% very important, 19% fairly important) in ten years time (http://ec.europa.eu/public_opinion/archives/ebs/ebs_225_report_en.pdf esp. p65)

a doctor who objected to the use of her confidential medical information for medical research in spite of her actively withholding her consent⁶. There are steps, however, that can be taken to mitigate some of these risks.

As indicated in response to question 2, in determining whether or not to share personal information, an assessment should be undertaken of both the actual and potential benefits and disbenefits. Additionally, a risk assessment should be undertaken with respect to the data security and confidentiality measures put in place by the proposed recipient body, such as those required by PIAG for applicants who have been granted approval to use the powers under Section 251 for specified purposes.

The NHS, similarly, has taken steps to regulate and facilitate legal and ethical information sharing with partner organisations e.g. seeking consent from patients to disclose information to independent sector providers delivering diabetic retinopathy screening services; the contractual arrangements for connection to the N3 NHS network and requiring compliance with the Information Governance toolkit. The NHS still has some way to go to ensure all its uses and disclosures of data have a secure basis in law.

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.

As indicated above, it is important that personal information sharing is considered in context and, therefore, there is a limit on the extent to which it is possible to comment in a generic way. We would also like to reiterate that health related information is sensitive information and the appropriate scope and methods of sharing such information may well differ, therefore, from other types of personal information.

Moreover, it is not simply a case of adopting a benefits / risks based approach. There are some first principles which need to be addressed - specifically that, in the absence of a statutory gateway allowing disclosure or an over-riding substantial public interest justification for disclosure, the only lawful basis for disclosure is with the consent of the individual. This will limit the scope of information that may be shared. Consent does, however, go some way to ensure that fair processing requirements are met and provides an opportunity for longer term retention of data, in some instances, or for consent to be sought for new uses not previously considered when consent was first obtained. It therefore provides opportunities for additional or more extensive legitimate information-sharing.

With the advent of the digitalisation of health information the scope for sharing vast quantities of sensitive information presents both risks and opportunities. Digitalisation

⁶ Whistleblower who was excluded from work for five years wins apology, BMJ January 2008,336 (7635):63.

of health information can:

- allow patient's information to be shared between clinicians in different organisations and locations thus facilitating more effective care and treatment
- facilitate swifter and more accurate clinical audit and better quality medical research
- benefit the security and confidentiality of personal data through access controls, audit trails of who has accessed a record and ensuring data is not lost, all of which represent significant benefits compared to paper records.

These however are reliant on the accompanying business processes being robust e.g. no sharing of smartcards for user authentication which requires that people receive adequate training to ensure they understand what is required and for there to be an organisational culture that supports the protection of personal information. The latter was conspicuous by its absence in the HMRC and led up to the system failures associated with the loss of child benefit data. Whilst to date this does not seem to have resulted in misuse, it could have had disastrous consequences and still might. For some people it has caused significant worry where for example their address is sensitive information.

Following the HMRC data loss, further incidents of data loss by public sector bodies have come to light including nine NHS trusts which admitted losing data. That such incidents have been reported rather than covered up, is in fact a sign of progress, although also an indication of the extent of the learning needed in some organisations.

Whilst the systems being put in place by NHS CFH should help to reduce data loss and prevent inappropriate data disclosure within the NHS, technical systems can only be part of the solution. Smartcards and passwords are only as secure as the way people use them. For example, smartcards have been lost and early on when smartcards were first being introduced, some were issued with the password written on a post it note and attached to the smartcard itself. Such failure further indicates the need for staff awareness and training on what is required and for disciplinary procedures and penalties to be invoked where such failures occur.

The risks associated with digitalisation are that vast quantities of personal information can be shared with ease and, as we saw with HMRC, the DVLA, and the examples above, the robust safeguards that are needed to balance these risks, are reliant on policies and procedures not only being in place but being rigorously followed by staff (cf response to questions 20 & 21 for further consideration of security issues). Managers also need to understand the issues sufficiently to enable them to oversee data usage and extraction processes to ensure they are appropriate. With the greater risks associated with digitalisation, organisations require stronger information governance processes to minimise these risks, utilising the electronic tools available to restrict access, audit access and ensure data extracted is the minimum needed for the purpose.

Many local councils and partnerships have well established data-sharing protocols.

These are a useful way of defining what data may be shared between the partnership bodies and in what circumstances. They are not a substitute, however, for seeking the consent of the individuals to whom the information relates. They can help staff to ensure they do not share information inappropriately. If the protocols are made public they can be used to improve the transparency of data use and sharing.

An example of where data was lost but where there were effective procedures in place was a Welsh NHS trust that lost a disc with information about patients that had received diabetic retinopathy screening and who had needed follow up treatment. Although the data was transferred via a disc i.e. in the same way as the HMRC, there was an audit trail of its journey so that it was known where and when it had been lost and the data had been encrypted, so the risk of inappropriate access had been minimised.

We have rejected a number of applications to PIAG because we were concerned about poor security measures, most commonly the storage of confidential information on laptops or where the applicant wanted to process the data at home.

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.

It is difficult to assess whether any public authority holds too much personal information as one would need to know the reasons why they are holding this information and whether it is being held with the full informed consent of the subject. The extraction of excessive information to be provided by HMRC to the Audit Commission would suggest that this is the case in, at least, some instances.

We would recommend that organisations are required to undertake routine information audits to assess what type of personal information is being held and why. We would also suggest that a description of the data being held and the extent of its identifiability should be available to the public. This would allow data subjects to assess whether organisations are holding too much information or not.

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.

It is difficult to assess whether any private organisation holds too much information as this would need to be assessed in relation to the specified purposes. In relation to Electronic Health Records and access by independent sector providers, delivering care on behalf of the NHS, important questions remain, such as how will their legitimate relationship with patients and access controls be determined? For example, where several independent sector providers are delivering a particular service in an area, are the service providers to be given access to all eligible patients?

data in the area or only to the provider delivering a service to an individual patient? The access control of Legitimate Relationship should restrict access so that a particular provider only accesses records for patients who have accepted referral to their service. Our experience suggests, however, that sometimes the controls are not being used appropriately by PCTs. This stems from a lack of understanding but is primarily because, proper implement of these controls, requires more work and investment and in the competition for resources will generally not be regarded as a priority.

The issues are in essence the same whether public or private sector and therefore we would also like to refer you to our response to question 5.

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).

It is likely that information pertaining to individuals is shared where there is a legitimate reason for such sharing e.g. to provide services to them and in general, could occur either with a statutory basis or consent. The barriers to such information sharing are therefore likely to be technical difficulties e.g. a lack of interoperability between systems or data definitions. It could also be related to difficulties in obtaining consent. In relation to medical purposes, the Section 251 powers were created to provide a statutory gateway for such data sharing. These powers are available as a last resort where it can be justified that identifiers are necessary and where it can be shown that consent is impractical e.g. very historical data, or research on child abuse, where it would be inappropriate to seek consent from parents, as one of them may be the abuser.

In other instances, however, there are boundaries that require negotiation i.e. these are restrictions that have been deliberately created in order to safeguard information and ensure it is not shared inappropriately. There are, therefore, different kinds of barriers. Some are the technical difficulties that inhibit legitimate information-sharing and which rightly should be addressed and overcome. Other barriers, however, are used deliberately and appropriately to maintain the boundaries that prevent inappropriate data-sharing. It is vital that this distinction is understood and maintained to ensure that barriers created to safeguard data are not regarded as a hindrance to be overcome. In our experience, the legal boundaries to information-sharing are often perceived by some in the research community and some staff in the NHS as an unnecessary burden rather than serving the purpose of safeguarding the confidentiality of patient information. It is essential this misunderstanding be addressed.

The overall approval rate for PIAG applications to use Section 251 powers is about 70% although some applicants have to resubmit a revised application showing that they have adequately considered the alternatives of anonymisation or consent and in some instances, this may be for a more limited cohort, where consent is feasible for the remainder. PIAG however is the only body that can lift the common law duty of confidentiality and it is likely that there is a need for a similar mechanism for other types of data and for activities that fall outwith medical purposes. For the 30% that are rejected or referred, applicants are advised how they might undertake the task without recourse to use of Section 251 powers. It is often the case that other avenues are practicable but that the applicant may not have given adequate consideration to issues of confidentiality or consent when designing the study or other activity. This can have cost implications, usually because of delays to starting the activity. It is clear, however, in the framing of the legislation that Section 251 powers are not to be used as a matter of convenience but rather as a means of last resort where the alternatives of anonymised data or consent are genuinely not practicable.

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 taking place, including the risks involved in such information-sharing.

Confidential patient information is being shared by the NHS with independent service providers who either provide data processing services or provide care and the information management services needed to support this. Such data-sharing should occur with contractual obligations of confidentiality and security in place and under data processing agreements. However, our experience in dealing with enquiries from potential applicants for Section 251 approval is that inadequate attention is paid to the first data protection principle that data is processed fairly and lawfully and that sufficient account of the common law duty of confidentiality is not taken. E.g., Many still believe that having an Honorary Contract with an NHS body gives them legitimate access to medical records.

As a minimum, where the NHS is using independent sector providers, the NHS should provide information to patients about how their data is used to support their care and treatment, where it is to be held with a means of opt out for those who object to such data-sharing or processing for a specified purpose. This is in keeping with the Information Commissioner's view with respect to the National Care Records Service Summary Care Record.

PIAG has seen a number of cases where clinicians who have joint or honorary appointments with Universities use confidential patient information (collected for the purposes of providing care) without consent, for research purposes. Some individuals have sought to blur the boundaries of their separate responsibilities and are currently operating outside the law.

We are also aware that it has been custom and practice to allow researchers or

research support staff access to GP or hospital records in order for them to identify patients meeting the inclusion / exclusion criteria for a particular research study with a view to seeking consent to participate in the research study. This involves a disclosure of confidential patient information without consent and is a class of support under Section 251 powers. We believe this class of support is currently much under utilised by the medical research community. Such information sharing without consent or approval under Section 251 is, in our view, unlawful as, in general, research would rarely meet the substantial public interest criterion as described in the NHS Confidentiality Code of Practice.

The risks associated with this relate to the fact that the public is largely unaware of how their confidential patient information is used, and would object to this use of their data without consent. Whilst recent research conducted by Ipsos MORI on behalf of the MRC, and a separate study conducted on behalf of the Wellcome Trust both indicated public support for research⁷. These studies also indicated that people were unaware of the use of their data for research purposes and there was a clear message that people expected their consent to be sought for access to use their personal data. As indicated in our response to question 3, the disbenefits of information sharing without consent are significant and should not be underestimated.

We would like to emphasise that the issue is not with information-sharing per se but with information-sharing taking place without the knowledge or consent of the individuals to whom the information relates. Whilst recognising that there are circumstances in which it is inappropriate or impracticable to seek consent and where there is a statutory basis for disclosure, these should be the exception and not the norm.

Section 3: The legal framework

The Data Protection Act (DPA) regulates the processing of information, including its obtaining, holding, use and disclosure.

The second principle of the DPA is as follows:

“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.”

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.

⁷ Ipsos Mori/ MRC *Consultation on public attitudes toward the secondary use of personal health information for medical research* (June 2007) www.mrc.ac.uk/utilities/Documentrecord/index.htm?d=MRC003810 and the Wellcome Trust *Public attitudes to research governance* (June 2007) www.wellcome.ac.uk/doc_wtx038446.html

Whilst the DPA provides a framework for processing personal information, it cannot be viewed in isolation. Although there are numerous statutes that allow or restrict access to specified data, both the Human Rights Act and the common law are key in contributing to the general legal framework for processing personal information.

In PIAG's experience, whilst organisations will generally have a data protection policy, not all consider the wider context of Human Rights legislation and the common law. This has often meant that few pay adequate attention to the duty of confidentiality or consider whether a disclosure is proportionate in relation to minimising the interference with people's right to privacy.

Additionally, the PIAG application form for use of powers under Section 251 asks applicants to show how they will comply with the eight Data Protection principles. This section of the form is often one of the most poorly completed and least understood. This may be related to the very generic nature of the DPA but it also, in our view, reflects a lack of consideration for confidentiality and data protection issues.

The strengths of the DPA include:

- The protection it provides from unauthorised or inappropriate use of the personal information.
- Although information can be processed without consent under DPA, the Act supports the rights of people to govern the use of their information and upholds the fundamental right of consent to process and to prevent the processing of personal information.
- It confers clear responsibilities on data processors to protect confidentiality
- It establishes important principles about secondary uses, which may be of particular importance in the context of healthcare.
- Data subjects can find out what information organisations hold about them.

Whilst the DPA provides a legal framework for the legitimate processing of personal information, its generic nature means that it would often benefit from adaptation to particular contexts in which information is processed. The NHS Confidentiality Code of Practice goes some way to providing this for the NHS, as data protection, confidentiality and the right to privacy form the core legal framework and need to be considered together.

The main weakness of the DPA, comes from the failure of organisations in interpreting and applying the Act to specific situations and in particular in realising that the first data protection principle embraces the common law duty of confidentiality⁸. This could be addressed through more specific work to consider these issues in particular contexts.

PIAG believes that more robust emphasis should be placed on the need for those holding identifiable information to seek the consent of data subjects and only use information without consent when no practical alternatives exist. The Advisory Group would also recommend greater enforcement powers for the Information

⁸ I Kennedy and A Grubb, 200 Medical Law, (3rd Edition OUP Oxford 2005) pp 1038

Commissioner, the Healthcare Commission and other bodies with regulatory responsibilities in this area. It was apparent from the investigation into the HMRC that the Information Commissioner did not have adequate powers to address the issues properly.

Such bodies should also have at their disposal a wider range of penalties for those found to be either deliberately misusing personal information or that are found to be negligent in failing to safeguard personal data. These should apply both to organisations and to individual staff members.

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.

PIAG recognises the value and importance of the second DP principle although it is important to be clear that this principle does not carry greater weight than the others. This question has however, highlighted a particular issue where data collected legitimately for one purpose by an organisation is then used for other purposes without seeking the consent of the individual. PIAG has had experience of advising NHS and other health providers about this issue and the need to use effectively anonymised data for secondary uses, such as financial audit, clinical audit, service evaluation and health needs assessment. Similarly, private organisations also use personal information for a range of purposes and only 'inform' individuals minimally via 'small print' in contracts etc.

This principle is important as it prevents personal information from being used for purposes from which the individual might withhold consent. Examples would be data provided to a patient organisation for the purposes of being a member of that organisation then being made available to an independent sector body, which uses this information for commercial purposes. The second principle provides protection from such misuses of data.

PIAG is aware that Section 33 of the DPA provides for research to be regarded as a compatible purpose to that for which the data was originally collected. This exemption only exists in UK law and is not included in the EU Directive. It is doubtful, therefore, whether this exemption would be accepted within a European Court particularly as the other purposes listed above are of at least equal value to the NHS in terms of public interest. This would seem to place research in a privileged position compared to other uses. Additionally, it may be a source of confusion for researchers, as consent is still required for the disclosure of personal information under common law, even if the purpose is to be regarded as compatible. It is hoped that the MRC Data and Tissue toolkit, to which PIAG contributed, will go some way to address this⁹.

⁹ www.dt-toolkit.ac.uk

The evidence from the MRC and Wellcome studies¹⁰ would seem to indicate that patients do not generally regard researchers as part of the clinical care team and therefore would not accept that researchers should have access to their sensitive information without their consent. That many in the the research community continue to believe they can legitimately access medical records without explicit patient consent, in spite of six years work by PIAG, would seem to indicate a lack of understanding of the interaction between the DPA and the common law duty of confidentiality.

Question 11

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

Technical barriers to the effectiveness of the DPA include a slowness to implement effective pseudonymisation¹¹ tools so that more data can be used and shared safely without identifying individuals. Similarly, many electronic records do not include a means of recording an individual's consent status i.e. that it has been provided or withheld, that the individual has been asked but has not yet responded, that they have not been asked, that the individual lacks capacity, and now the status of any proxy consent gained through the provisions of the Mental Capacity Act 2005.

Government, and to a lesser extent private sector organisations, have failed to create institutional cultures across public sector bodies that focus on safeguarding personal information and there seems to be a reluctance to seek consent for uses where there is no other secure basis in law.

The DPA carries with it very few sanctions. PIAG would support new sanctions or offences under DPA, to challenge what appears to be a lax culture within government. We would also suggest that any enforcement or penalties should be modelled on health and safety or other relevant legislation such as the penalties attached to the powers given to the Healthcare Commission under the Health and Social Care (Community Standards) Act 2003 and the NHS Counter Fraud and Security Management Services (CFSMS) under the NHS Act 2006.

We need to generate the same culture around data protection as for health and safety. using the sort of model in their 5 steps to success: policy, organisation.

¹⁰ Ipsos Mori/ MRC *Consultation on public attitudes toward the secondary use of personal health information for medical research* (June 2007) and the Wellcome Trust *Public attitudes to research governance* (June 2007)

¹¹ Pseudonymisation is data that includes coded data so that the information should not be identifiable to the recipient but could be traced back to the individual by the original holder of the data. Much data that is labelled as pseudonymised, however, contains identifiers and would be regarded as personal data within the terms of ICO guidance. Work is currently being undertaken by the Digital Health Information Policy team within the Department of Health to attempt to define pseudonymised data. The difficulty with defining it beyond the generic definition that it should not be identifiable to the recipient, is that different types of data will have different degrees of identifiability e.g. rare conditions or ethnicity is likely to increase the identifiability of data significantly.

implementation, audit and measurement; and then reviewing policy to provide assurance of safe practice.

PIAG would also suggest that many organisations outside of healthcare do not have the necessary information governance processes to ensure that sharing personal information is legal, ethical and secure. Information governance processes are fundamental for regulating information sharing, these processes facilitate good practice and can prevent or reduce poor practice. PIAG suggests that the work undertaken by the Digital Health Information Policy team within the Department of Health in developing an Information Governance toolkit and the Code of practice developed by the Healthcare Commission should be disseminated as examples of good practice for other organisations.

Question 12

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

PIAG would welcome a strengthening of powers for the Information Commissioner, Healthcare Commission and proposed National Information Governance Board with respect to providing additional monitoring and enforcement powers for the processing of personal information. Other safeguards could include the requirement for a Code of Practice governing how personal information will be used and safeguarded by particular bodies; an internal oversight committee, which reviews the processing of personal information and ensures that the data protection principles are met. This should include independent membership and should be required to produce an annual report. Requirements should include that only senior staff members can access sensitive personal information and must sanction others' access for specified purposes, which would be recorded.

There should also be a range of penalties and sanctions for inappropriate disclosure, both against the responsible organisation but also against individuals acting inappropriately. The penalties in the 2006 Act for the NHS CFSMS included criminal penalties where disclosure is malicious or negligent.

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.

Reference has been made in several of the responses above to other aspects of UK law, which provide appropriate restrictions on or permissions for confidential information. Reference has also been made to the disjuncture between the EU Data Protection Directive and Section 33 of the DPA in the UK. Please see response to Question 10.

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.

There is already provision in the DPA to ensure that information is processed securely. This would suggest that perhaps the legal requirement needs to be tied more directly with Information Security standards (specifically ISO 27001 & 27002). Robust authentication processes are only one component. Other requirements would be:

- restrictions on which ‘users’ would be able to access what data
- the availability of derived data to replace identifiers e.g. age in place of date of birth
- a range of pseudonyms available to facilitate linkage whilst reducing the identifiability of data.

It is important not to compromise data quality or utility but also to prevent the linkage of datasets where this could render information more identifiable than would be needed for a particular purpose. A clearer requirement to encrypt data for electronic transfer whether via the internet, VPN or portable devices would also be valuable.

In light of the revised guidance from the ICO, giving a wide definition to personal data, additional safeguards are needed for pseudonymised data such as non-disclosure agreements, to ensure data is not disclosed to another party who might misuse the information, and a requirement not to attempt to render the information more identifiable.

The Department of Health has national guidelines for NHS bodies which consider such issues, but there is a need to ensure these guidelines are followed. Policies and procedures are not always followed by NHS Trusts and individual staff, as they require additional work and tend to be regarded as an unnecessary inconvenience rather than as an essential means of safeguarding personal information.

A key issue for PIAG is that whilst robust security arrangements are required of approved applicants, the same degree of scrutiny is not applied to data used for research purposes where consent is in place. Whilst safeguarding information used without consent is a particular concern, nevertheless, the same information security irrespective of whether consent has been obtained.

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.

This begs the question of what is 'unreasonable'. If the DPA protects the public's right to confidentiality or safeguards other personal information, we would ask how this could be seen as unreasonable. Information can be shared without consent where it can be shown that this is in the substantial public interest. Without a substantial public interest to disclose personal information, then obtaining consent cannot be seen as unreasonable.

With respect to the so-called 'regulatory burden' of the PIAG application process, although it may be time-consuming, the application process needs to be robust to ensure that Section 251 powers are not used inappropriately. Moreover, the alternative to the use of these powers is to seek consent or to use data that has been rendered effectively anonymous by clinical staff responsible for delivering care to the patient. The alternative therefore places a greater burden on the NHS and organisations seeking to use confidential patient information than the PIAG application process.

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.

The law on consent is clear: personal information passed to an individual or organisation can only be further disseminated to 3rd parties either

- 1) With consent
- 2) Where there is a statutory basis.
- 3) Where the balance of public interests favours disclosure. Confidential information requires that a higher public interest test is met, specifically that disclosure is in the substantial public interest and balancing this against both the private interests of the individual and the public interest in maintaining public trust in a confidential service.

Consent is the cornerstone that protects confidentiality and failure to seek consent is disrespectful of personal autonomy, undermines confidentiality and intrudes on people's privacy. Whilst there are justifications for not seeking consent, these are not

a matter of convenience but of genuine difficulty or a strong public interest justification.

Researchers and other bodies have argued that obtaining patient consent for research purposes may not always be practical. The fundamental question is what expectations people have with respect to the use of their information. Seeing information only as an asset undermines the autonomy of all patients. Recent research from the Academy of Medical Sciences (Personal data for public good: using health information in medical research 2006) concludes that identifiable data can be used for medical research without consent, provided that such use is necessary and is proportionate with respect to privacy and public interest benefits. Whilst there is some truth in this, the public interest needs to be substantial to warrant disclosure without consent¹² and it is unlikely that most research would meet the standard for this (e.g. serious risk to others). Whilst research, in many instances, is in the public interest, this does not mean that all research is in the public interest and a judgment needs to be reached about each individual research study.

For consent to be valid it must be informed, sufficiently specific in its definition to give the term 'informed' meaning, there must be understanding of what consent is being given and it must be voluntary.

Within the NHS, consent to share information for care and treatment purposes, is often implied within consent to examination or treatment. For secondary uses of data however, consent cannot generally be implied, as most secondary uses cannot be anticipated by patients. The NHS also generally does not take adequate steps to ensure patients are appropriately informed of such secondary uses and consequently any consent implied for secondary uses would be unlikely meet the criteria for validity.

With respect to recording consent, whilst written consent is often the preferred medium, there needs to be the means to record different kinds of consent or the withholding of consent electronically to ensure that people's wishes are implemented and thereby respected. PIAG has encountered difficulties with this, where a GP may know of a patient's wish to dissent from allowing their information to be used for research purposes and have recorded it on the GP system but where this dissent is not recorded on PCT or central databases. Consequently where data is obtained from one of these other sources the individual's dissent will not be known and therefore will not be acted upon.

Question 17

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

This question suggests that consent can only be seen as a negative barrier and that consent is something that needs to be overcome to share information. Consent is an

¹² cf. NHS Confidentiality Code of Practice

appropriate barrier to unreasonable and arbitrary information sharing, furthermore consent requires an engagement with data subjects about what and how personal information is to be shared. Arguments have been made that obtaining consent can introduce study bias in research; PIAG agrees that this may be true for some studies, but that this cannot be seen as a general rule. Moreover, often studies have a range of biases within them, which have nothing to do with consent. Study bias cannot simply be seen as an argument for not seeking consent. PIAG takes issues of study bias seriously when assessing applications to use powers under Section 251 and for example has been a key factor in agreeing to approve surveillance studies undertaken by the British Paediatric Surveillance Unit. This however is only one of several factors considered when PIAG makes its determination about an application.

Applicants to PIAG often claim that it is difficult to seek consent from patients when giving bad news about diagnosis and prognosis. We accept that this can sometimes be the case but would argue that where patients are suffering from long term conditions consent (for example for research purposes or to enter a patient on a disease register) can usually be sought on a subsequent occasion.

Seeking consent requires careful planning and resources but in many instances is feasible. PIAG acknowledges that, in some instances, seeking consent can be problematic but the question that needs to be asked is whether patients expect to be asked for consent. The answer to this question has been shown to be yes in both the MRC and Wellcome Trust studies¹³.

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 simplest way to make information sharing more transparent is for consent to be the basis of information sharing. In addition, organisations could provide clear and accessible information materials explaining the types of data to be processed, the purposes for processing, any benefits and disbenefits to this information being processed, a description of the type of people who will be given access and explaining both the right of opt out and how to access the mechanism to opt out, once consent or Section 251 approval has been obtained.

PIAG would suggest that a full and open public debate on the issues related to the sharing of personal information, with the risks and benefits outlined, would allow public policy to develop in a more constructive manner. If we accept that all

¹³ Ipsos Mori/ MRC *Consultation on public attitudes toward the secondary use of personal health information for medical research* (June 2007) and the Wellcome Trust *Public attitudes to research governance* (June 2007)

individuals have some measure of control over their information then all organisations involved and interested in information sharing should engage with individuals at a general and specific level. Transparency of information sharing will provide assurance to the public that they know how their data is used. It would also provide assurance to those sharing information that they are doing so with the knowledge of the individuals concerned and with public backing for the defined purposes.

Applicants often argue that it is enough to inform patients about the use of their information by putting up posters in GP surgeries. PIAG feels that this is a completely inadequate way of providing information. In contrast, however, we have seen some very good examples of tailored patient information leaflets, which do give clear explanations about how patients' information may be used. A further issue in relation to patient information leaflets is the extent to which NHS bodies utilise them to ensure patients are appropriately informed. PIAG has made it clear that where this is a condition of approval, a failure to take adequate steps to disseminate such information materials would undermine or even negate their approval.

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)?

The simplest way to ensure transparency is to place consent at the heart of all sharing of identifiable information. The guidance produced by the Information Commissioner's "Framework code of practice for sharing personal information" is useful in providing greater clarity on the boundaries of personal information. It neglects to place the DPA in context, alongside the Common Law of Confidentiality and therefore can suggest that compliance only with the DPA is sufficient to justify sharing information. The first DP principle incorporates the common law duty of confidentiality. This omission would seem to have led some to believe that consent may not be necessary for sharing identifiable information. Whilst consent is not always necessary, it is fundamental to the common law which seeks to define the exceptions to consent rather than creating a list of alternative options. Consent should not be seen as something that one should find ways to avoid but should be at the heart of any decision on information sharing.

Scrutiny and accountability can be achieved by:

- requiring confidentiality and security policies to set out clear lines of

accountability with named responsible officer roles (such as PIAG's System Level Security Policy template¹⁴).

- A requirement to use Information Governance toolkits and to meet standards set by the relevant body e.g. the Healthcare Commission.
- Stronger enforcement powers for organisations with a remit in this area, including the Information Commissioner and in relation to health, the Healthcare Commission and the proposed National Information Governance Board (this is being given stronger powers than PIAG had previously, under the legislation currently going through Parliament).

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.

As indicated in response to earlier questions, technological advances present both challenges and opportunities. The challenges are to ensure the scale and speed of information sharing do not lead to inappropriate disclosures and breaches of confidentiality. The opportunities lie in making more, better quality data available for a range of purposes and improving some aspects of information security and confidentiality e.g. through audit trails, access controls, and the use of privacy enhancing technologies etc. More fundamental than the technological advances, however, are the business processes, training and awareness of personnel to ensure that the technological safeguards are used

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?

It is difficult to develop a legal mandate that will apply to all types of personal information and the different scope and methods of processing personal information. As indicated, standards already exist and what would seem to be needed, therefore, is for a stronger linkage between the seventh DP principle and the requisite standards. Part of the difficulty of legislating is that the requirements change as technology advances, both in terms of posing greater risks to information security but also providing new solutions to safeguard data. PIAG would welcome this strengthening to require implementation of security standards. Greater definition

¹⁴ www.advisorybodies.doh.gov.uk/PIAG

could perhaps be provided through a statutory instrument or through greater powers of enforcement.

With respect to the use of portable devices, certainly it has been PIAG's advice that the use of portable devices, particularly laptops which are susceptible to theft, is to be avoided. Where they must be used, industry standard encryption (128 bit) should be used both for portable devices and other electronic transfer. A difficulty with the implementation of encryption is that sometimes encryption software is not compatible with other operational software on systems. There is a need therefore for encryption tools to be thoroughly tested for use with operational systems before being rolled out.

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?

Anonymisation and pseudonymisation are fundamental to ensure information can be used for secondary purposes, where there is no need for direct involvement by individuals. This is particularly relevant for some types of medical research.

Pseudonymisation in particular can be useful in enabling data about the same individual to be linked where data is obtained from different sources or at different times (i.e. longitudinally) without readily identifying the individual.

Progress has been made by the NHS Connecting for Health Secondary Use Service to develop a resource of anonymised and pseudonymised information, which will employ a range of pseudonymisation tools, so that the identifiability of data can be minimised whilst maintaining its usefulness.

Whilst this progress is widely welcomed, researchers and others will continue to need access to identifiable data for some time. In due course, it is hoped that this will meet the needs of most researchers and others using data for secondary purposes. It is likely there will continue to be exceptional circumstances where the available anonymised or pseudonymised data does not meet their requirements. There will therefore be an ongoing need for PIAG or the NIGB to regulate access to identifiable information.

The development of an Honest Broker function has been proposed and is being explored. Access by an honest broker to confidential information will need either a statutory basis or the consent of the individuals whose data is to be processed. The role of the honest broker would be to undertake data cleansing and linkage and then to pseudonymise data, checking the resulting data is not identifiable prior to disclosure. In general, access to identifiable data would not be retained beyond the processing undertaken. PIAG welcomes this proposal as it would reduce the number of places where identifiable data would need to be held. PIAG is concerned however, that any Honest Brokers established have a secure basis in law either through statute or consent. Additionally, PIAG believe that approval for access to data or to

use of the Honest Broker function should be separate from the service function of providing the data. The same principles would also apply to any safe havens that were developed.

PIAG has advised a number of bodies establishing new audits, either within the NHS or professional bodies, that encryption can provide a means of pseudonymising the data so that it is not viewed outside of local trusts in identifiable form. This requires that the same algorithm is used to encrypt data so that the NHS number for example is encrypted in the same way each time, thus enabling longitudinal and cross organisational linkage. As this approach does not require approval under Section 251, these activities have not been considered further by PIAG.

A barrier to the deployment of this type of approach is that such technical solutions require investment. It is only really a solution therefore, for larger scale and long term activities. A period of testing is also needed to ensure data integrity and operational systems are not compromised.

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.

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?

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?

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.

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?

Personal data pertaining to the deceased

The DPA does not apply to the deceased. The recent Epsom and St Helier Information Tribunal determined that confidentiality survives death and is in keeping with the ICO guidance in relation to exemptions under the FOIA relating to confidential patient information. This raises the question of what additional safeguards, such as those in the DPA, should also apply to the deceased. The Department for Constitutional Affairs (DCA), as it was then, recommended that deceased persons should be covered in any information sharing protocols.

The rationale for such safeguards being extended to information about the deceased is to respect the wishes of individuals when they were alive, to protect third party data held in records, to avoid causing distress to bereaved family members and to prevent fraud based on the theft of deceased person's identities.

Family or other shared information

An additional area for consideration would be the issues related to 'shared information' such as genetic information, which would be relevant for family members. This presents particular challenges in relation to consent and the linkage of records of parents and children or siblings for a variety of purposes.

Question 28

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

There would seem to be a fundamental misunderstanding of the interaction between the DPA, the common law duty of confidentiality and Human Rights Act. This has led to some confusion on the part of researchers and others. Key areas of tension are:

- a. That the first DP principle incorporates the common law duty of confidentiality and consequently even where the DPA does not require consent the common law may require it for disclosure rather than to use data for a new purpose.
- b. Where PIAG have permitted the common law duty of confidentiality to be set aside, this only provides relief from one aspect of the first principle and fair processing and the other seven principles must still be met.
- c. Where PIAG has provided relief from the duty of confidentiality, the Advisory Group can place conditions of approval which require a higher standard than that imposed by other parts of the DPA. so for

example, where approval has been given for a medical research project, the Advisory Group can place as a condition of approval that data is not retained in identifiable form indefinitely. This is in line with the fifth data protection principle but is not in keeping with S.33 exemptions for research. The basis for this is that this is as close to compliance with the common law duty of confidentiality as possible and takes account of the need for minimal interference with people's privacy (HRA).

- d. Research purposes under the DPA would appear to have a very broad definition and include activities such as surveys undertaken by organisations such as MORI. There is a degree of tension between this and research as intended under medical purposes in the NHS Act. This needs consideration and may be an example of where a more differentiated approach according to different contexts within the DPA may be appropriate.