

# Data Sharing Review

Richard Thomas and Dr Mark Walport

## Consultation paper on the use and sharing of personal information in the public and private sector

### List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to [contact@datasharingreview.gsi.gov.uk](mailto:contact@datasharingreview.gsi.gov.uk)

Alternatively you can send a hard copy response to:

**Data Sharing Review Secretariat**  
**5.26 Steel House**  
**11 Tothill Street**  
**London**  
**SW1H 9LJ**

Thank you.

### Section 1: Background

Question 1.

Comments:

[Note from the Data Sharing Review Secretariat:

Please note that this submission represents the shared views of the three authors only, Perri 6, Christine Bellamy and Charles Raab and not those of any organisation with which they may be working or have recently worked on this issue. Charles Raab has stated that this submission is undertaken in his academic capacity, and does not necessarily reflect the views of the House of Lords Select Committee on the Constitution, for which he is the Specialist Adviser.]

We have longstanding research interests in data sharing and information policy (e.g., Bellamy and Taylor (1998), *Governing in the Information Age*; 6 et al., (1998), *The Future of Privacy*; Bennett and Raab (2006), *The Governance of Privacy*).

We contributed to the Performance and Innovation Unit's 2002 study, "Privacy and Data-Sharing: The Way Forward for Public Services". 6 collaborated with MORI to

produce a focus group-based appendix on public attitudes; Raab served as a member of the PIU Advisory Group.

In 2004 Raab and 6 (with others) wrote a commissioned report for the (then) Scottish Executive, "Information Sharing for Children at Risk: Impacts on Privacy", which assessed possibilities for applying Privacy Impact Assessment to the eCare Programme.

In 2006, we completed together a major ESRC-funded study on this issue, "Joined-up Public Services: Data-Sharing and Privacy in Multi-Agency Working", RES/000/23/0158), the major part of which consisted of over 200 in-depth interviews with front-line staff working in English and Scottish multi-agency partnerships in public protection, crime reduction, care of the mentally ill and care of the elderly. The interviews provide unique insights into the ways that staff in a wide range of local agencies perceive and handle tensions between data sharing and privacy.

The publication from this project most relevant to the issues discussed in this review is Christine Bellamy, Perri 6, Charles Raab, Adam Warren and Cate Heeney, Information-sharing and confidentiality in social policy: regulating multi-agency working, Public Administration (86:2), forthcoming 2008. See also 6 P, Bellamy CA, Raab CD, Warren A and Heeney C, 2007, Institutional shaping of inter-agency working: managing tensions between collaborative working and client confidentiality, Journal of public administration research and theory, 17, 3, 405-434; 6 P, Bellamy C, Raab C and Warren A, 2006, Partnership and privacy – tension or settlement? The case of adult mental health services, Social policy and society, 5, 2, 237-248; 6 P, Bellamy C and Raab C 2005, Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy, Part I, Public administration, 83, 1, 111-133; Bellamy C, 6 P, and Raab C 2005, Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy, Part II, Public administration, 83, 2, 393-415.

More recently, we have provided advice to civil servants in the Department for Communities and Local Government (CLG) on the development of cross-governmental guidance on data-sharing, in connection with the work of MISC 31, the Cabinet Committee established in 2006 (dissolved in 2007) to develop the Government's policy on data-sharing. A copy of our final report is attached, by kind permission of CLG. This copy of the report is provided to the review in confidence. If any part of this response is published by the present review, this report may not be published, because it has the status of confidential advice to ministers in CLG. We have sought and obtained the permission of CLG to append the report to this submission because we believe, and CLG officers agree, that its contents pertain directly to the questions with which the review is concerned.

Our response to the present consultation draws on a practical approach to the management, regulation and promotion of data-sharing generated from this work, and focuses on helping agencies to understand and better manage risk in

reconciling the competing imperatives necessarily involved in the sharing of personal information.

The Data Protection Act 1998 both allows and requires organisations to exercise professional judgment in relation to the sharing of information, and could never provide algorithms or inflexible rules obviating this use of judgment;

It may therefore be more helpful to organisations to assist them in determining whether or not data-sharing is a justifiable and sensible course of action in a particular set of circumstances, rather than on developing more or better legal guidance that can, in the end, do no more than reveal the problems for which professional judgment must be exercised;

Both sharing and not sharing often entail risks to individuals and to the (often stigmatised) groups or categories into which individuals are administratively sorted in the public services; to the effectiveness and integrity of services, and thus to the health of society and to the perceived legitimacy of data-sharing regimes. The key task is to help organisations to understand and manage such risks;

In conditions of inadequate information that, by definition, hold at the point where decisions to share or not share are made, agencies will sometimes, inevitably, make the wrong call about whether or not to share what they do hold. Frontline agencies in sensitive fields such as child protection, crime reduction, public protection, anti-social behaviour, drug misuse, youth offending or mental health must decide whether, in this uncertainty, they would prefer their staff to risk erring on the side of avoiding false negatives (by not sharing when it might be necessary) or avoiding false positives (by sharing when it might not be necessary). Another key issue is how to manage blame when mistakes occur, especially in hard, sensitive or high-profile cases.

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

### Question 2.

Comments: In analysing the findings from our own ESRC-funded research, we distinguished between three types of benefit (§4, box 2 of the Report which is appended to this submission):

1. promoting the integration of services delivering benefits to individuals or neighbourhoods. That is, (i) sharing of information inputs should enable service providers (ii) to design connections between services' throughputs, in order (iii) to plan and support more efficient, seamless, comprehensive and fully integrated outputs;
2. detecting, preventing or managing risk and harm to third parties, who may be specific individuals or groups (victims or potential victims, for example) in the case of crime, or general groups within the population (e.g. taxpayers) in the case of benefit or tax fraud.

3. avoiding inconsistency and conflict between services, to avoid problems either for service users or for third parties

Agencies should not only be aware of these benefits and disbenefits, but should assess their scale and probability, and also assess the scale and the probability of the risks that they are prepared to accept in their pursuit.

Clearly, these benefits are not achieved by sharing literally any available information agencies possess about individual clients, under any circumstances. Simply enumerating benefits does not obviate the need for agencies to specify the circumstances in which they are likely to be relevant or to decide whether these circumstances apply in a particular case. These tasks are problematic for many agencies, because assessing the probable scale and significance of benefits and disbenefits from sharing personal data is sensitive to small changes in the specification of the "relevance criteria" adopted by agencies. By definition, the most difficult and sensitive cases require the finest judgments, because it is in these cases that the risks are most delicately balanced.

There has been a tendency in recent years toward much greater codification of relevance criteria in many public services, but the research evidence very powerfully supports the view that it is not possible to eliminate professional judgment and discretion by the use of greater codification. Codes are not self-interpreting; and often in the most difficult and sensitive cases, codes do no more than identify areas in which professionals must exercise discretion. Moreover, codification often creates new areas of uncertainty by reducing professionals' confidence in the exercise of judgement based on professional experience and common sense. Indeed, codification in the context of managerial cultures that encourage individual blame can create perverse incentives to engage in defensive decision making, such as "kicking difficult decisions upward", thus causing problems of rising costs, managerial overload and slower decision making.

#### Question 3.

##### Comments:

Several broad kinds of risk to the individual, associated with inappropriate sharing, can be identified. There are risks of

- indignity resulting from the unnecessary exposure of facts or suspicions about a person to people who have no legitimate need to be in possession of them. An example might be the disclosure to an agency not concerned with gynaecological matters of the fact that a woman client may have had a termination.
- injustice, arising from stigmatisation, leading to such wrongs as loss or denial of employment or training; loss of financial creditworthiness; social ostracism, or other forms of discrimination. This issue can arise in adult mental health where disclosure of a diagnostic fact may threaten employment or access to affordable insurance, when in fact the person may in fact be entirely employable or represent only standard insurable risks.

- inappropriate treatment being provided, for example through unwarranted interventions by agencies in individuals' lives or those of their families or households. This can arise in child protection or adult mental health where draconian action may flow from disclosures of information that may be misread as more serious than in fact they are.
- ineffective service delivery, and thus to the public or social interest, as a result of the withdrawal of trust by clients in agencies which are perceived to disclose confidential information too freely or with insufficient care for consent, transparency, accuracy or completeness. This may result in failure of clients to present for service or failure of clients to be sufficiently candid when they do present. These failures may lead to inadequate case management in fields such as substance misuse or mental health. They may also make it more difficult for policy objectives to be achieved (for example, take-up campaigns amongst older people may be undermined by fears of data disclosure, as may compliance with personal tax regimes).

These risks may arising from sharing the correct information in the wrong framing or context leading to misunderstanding, sharing correct but inappropriate or poorly selected information, sharing incorrect information, sharing correct but incomplete information or sharing the appropriate and correct information but in the wrong manner. Among the dangers that may result are inaction, insufficient action, or excessively intrusive intervention; these outcomes may reflect, variously, false-positive or false-negative decision errors. Further elaboration of the risks can be found in our accompanying report to the Department of Communities and Local Government, *Appropriate Information Sharing*, pp. 6-7.

We would emphasise, also, that the improper or erroneous sharing of personal data may not only erode the privacy of the individual (or category of persons) concerned, but, if not prevented or corrected, may contribute to the erosion of the value of privacy as a constitutive property of society itself, which all members of society have an interest in realising beyond the benefit that they each may enjoy from the protection of their individual privacy. One practical effect of this perspective is that there is a collective, societal interest in the quality of the systems, processes and rules by means of which the sharing of personal data contributes to the maintenance of privacy and dignity as important values. This means that the integrity of public-service organisations' information practices and data-sharing decisions is not only important for the quality of the organisations concerned (e.g., health units, schools, police forces, social-service departments) or for the individuals with whom they deal and whose privacy may be immediately affected, but for the interests of the society that sustains and legitimises these organisations.

**Question 4.**

**Comments:**

In the report which is appended to this submission in §3 box 1, we distinguish between the following five types of method for information sharing.

**Box 1: Types of context for information sharing**

(a) Bulk sharing: sharing data routinely (perhaps by secure electronic means) so that agency B can obtain data in defined fields from the records possessed by agency A about specified categories of citizens.

Example: Many police officers have this kind of routine access to the Driver and Vehicle Licensing Authority's database of registered keepers of vehicles.

(b) Bulk sharing and data matching: sharing data routinely, as above in order that agency B can search any field in agency A's databases, compare data in these fields with fields in its own databases, in order to identify citizens who show positive matches according to specified rules. Agency B also retains the information from A's records on these individuals in its own records.

Example: This type of sharing occurs fairly frequently in fraud control in benefit administration.

(c) Targeted cluster sharing: granting access either on a one-off or a recurring basis for agency B to search on particular fields specified in advance in agency A's records, to identify all those individuals with or without a particular characteristic. The purpose here is to examine some additional fields of agency A's records to which B is granted access but without the right either to add its own information to these records, or simply to use its own records to target them for some treatment or other.

Example: This is sometimes done in law enforcement work where the aim is to identify individuals who may be at risk of repeat victimisation.

(d) Structured sharing for individual case management: allowing agency B to access agency A's records for agreed purposes in order to search for information in specified fields about particular pre-defined individuals or about individuals who are known to have particular relationships with a focal individual whose case is being managed by B.

Example: Permission is sometimes granted to a multi-agency public protection arrangement (MAPPA) programme to search the digitised CCTV footage from an area near a school to see whether known sex offenders had been in the vicinity of the school, and perhaps to see whether such a person had been seen near the school with other persons known to the MAPPA.

(e) Unstructured sharing for individual case-by-case sharing: allowing B, either on B's request or on A's proactive offering, access to a particular piece of information about a particular individual. This sharing may be written, electronic or verbal, and may be multi-lateral or bi-lateral.

Example: Unstructured case-by-case sharing is quite common at the point of referral in mental health care, or at a point of crisis in care in the community for frail elderly people.

There are benefits and risks associated with each of these five principal methods. The benefits have been discussed above (see answer to Q2), so here we discuss risks specifically associated with each method.

(a) Bulk sharing risks the provision of information that is excessive for the purposes for which the receiving agency uses the information.

- (b) Matching risks both false positive and false negative errors generated by the algorithm used for matching.
- (c) Targeted cluster sharing risks allowing “fishing expeditions” and unwarranted retention of information accessed, on a “rainy day” justification.
- (d) Structured case- management sharing also risks access to information that is excessive for purpose.
- (d) Unstructured case-by-case sharing is subject to the vagaries of professional judgment.

What is required is the development of practices for each set of related policy fields, (in many instances, cases at local level), by which judgments can be argued out and settlements reached, about the method of sharing that represents, the least unacceptable set of risks and the most acceptable benefits. These practices must of course be, subject to rules for professional practice and audit, which must be agreed at the same time.

In the report appended to this submission, in §8, Table 1, we distinguish between the following four basic types of service context for data sharing, that is, to what is referred to in this question as “scope”.

Table 1: Four pure types of service context, raising different kinds of concern about information sharing dilemmas

A: Universal services, delivered for the benefit of the public

Example: personal direct taxes, social insurance payments, driving licence registration; citizen registration services.

B: Universal services, delivered for the direct benefit of individuals

Example: , education, general health services, social insurance benefits

C: Selective services, delivered for the benefit of the public or third parties

Example: probation, youth offending, MAPPAs, policing, CRB

D: Selective services, delivered for the benefit of individuals

e.g., child protection, services for vulnerable adults, specialist services for older people, specialist health services (such as mental health), social landlord services, drug and alcohol abuse services

In our own research, we found that the most difficult dilemmas for local agencies to deal with tended to be associated with functions of type C, where agencies are required to share unstructured personal data on a case-by-case basis or for the purposes of ad hoc targeted cluster sharing (which are least susceptible to regulation through well understood conventions and rules), in situations where staff are most likely to perceive a conflict between the interests of the individual client and the interests of the wider society.

These tensions are especially difficult to manage in circumstances where:

- (i) sharing takes place (or not) between agencies with different primary functions (i.e., the provision of services to individuals (type D), on the one hand, and services to protect the wider public (type C); For example, we found that most medical and psychiatric practitioners would be in no doubt about their duty to share information in the case of serious crimes or high risk patients, where the connection with their patient was palpable, in order to secure benefits for third parties. However, their professional duties to the patient to protect confidentiality may often prevail in relation to crimes they consider to be less serious, or where patients present less immediate risk, or where the connection to the patient is not clear. This can give rise in some cases to conflicts about the priorities between type 1 and type 2 benefits, which can in some cases only be resolved by ad hoc case discussions at the most senior levels of management, or even by litigation. These are expensive, crude and slow methods of dispute resolution; and where:
- (ii) risks of harm associated with preserving confidentiality are not so immediate or so strong as to overwhelm the risks to effective service delivery associated with breaches of confidentiality; this is sometimes the case, for example, with certain types of sex offenders at MAPPA risk level 2, or with mentally-ill persons who suffer only sporadic episodes of ill-health, or certain types of youth offender whose offending pattern is not yet firmly set; or where
- (iii) where the evidence on which the risk assessment is based is soft or of unknown provenance, as is frequently the case in dealing, for example, with allegations of child abuse or inadequate parenting, or with certain kinds of anti-social behaviour.

As we have already said in response to Q2, the risks to the good governance of data sharing, and thus to the establishment of high public confidence in the processing by public services of personal information, lie in the considerable unpredictability and inconsistency of local practices. This we believe is caused in large part by uncertainty among staff and their managers as to how best to cope with dilemmas between the risks associated with sharing data and the risks associated with breaching confidentiality and privacy.

The key question, then, is how best to give local agencies the confidence and tools to handle these dilemmas with greater consistency, transparency and predictability ( see answers to Q19 and Q27).

Question 5.

Comments:

Framing the issue as simply one of risking the sharing of excessive quantities of information is often not helpful. True, there are cases of simply being told too much. Often, though, the important issue is whether the information that is provided has been furnished at an inappropriately low threshold of risk. This can arise sometimes, for example, where law enforcement agencies may demand

clinical information from adult mental health services about their clients in the absence of clear and sufficient reason to believe the individuals to present a substantial future risk. In other cases, the more important issue is that information may be provided where a receiving agency might over-interpret its significance and overreact. Again, adult mental health services provide some examples, where the provision of information to employers may prejudice an individual's chances of employment, even though it may be provided with the best of intentions about enabling the provision of in-work support. In short, it is more appropriate to think about the risks of inference from information, in the context of its being shared or not, than to focus on quantity.

Question 6.

Comments:

We do not have the empirical evidence to take a considered view on this question

Question 7.

Comments:

Our research found that staff in some settings are much less confident in local arrangements for governing data sharing and protecting client confidentiality, and that they tend to respond to uncertainty in ways that either result in a systematic bias towards the priority of avoiding false negative judgment errors (that is, not sharing in circumstances that may require it) or in practices that appear to be more inconsistent and unpredictable than those in other settings. These findings hold for all types of data sharing identified in Q4, but particularly for type (e), that is for unstructured, case-by-case sharing, which was the main focus of our study. We found:

- with the exception of those in community health teams, staff in primary and secondary health care agencies tend to be reluctant to share with non-medical or para-medical staff outside their own health care teams, and particularly with staff in public protection, law enforcement or crime reduction agencies.
- staff in specialist units within police forces and housing authorities that deal with issues such as sex offending, domestic violence, anti-social behaviour, and child protection/families, tend to be reluctant to share information with mainstream police or social housing services because of the risk of stigmatising their clients and triggering inappropriate interventions. Likewise, primary medical units dealing with substance abuse are often reluctant to share information with mainstream health and social care agencies, let alone with law enforcement agencies, for fear that clients will withdraw their compliance, frankness and trust.
- staff in youth offending teams and community safety/crime reduction partnerships tend to lack confidence in data sharing, and appear to engage in practices that are more inconsistent and unpredictable than those in other types of multi-agency partnerships. We think this is because CRDPs tends to be rather big and diffuse, and also because local authority community safety departments (which often act as lead agencies) tend to lack experience and training in issues to do

with personal information management.

- staff in agencies (such as social landlords, health authorities, schools and colleges) that are only peripherally involved in multi-agency partnerships in fields such as child protection, public protection (MAPPAs) and mental health) tend to lack confidence and understanding of data sharing, compared with core agencies, such as social work agencies, prisons, probation service, specialist police units and community health care teams. They are therefore often reluctant to engage in it, or do so haphazardly. This is because partnerships in these fields tend to be cleaved: that is they tend to be composed of a few core agencies that are closely involved in the field, and understand its demands, but also call on a wide range of other agencies, who may be involved only at very sporadic and infrequent intervals.
- staff across all functions in Scotland tend to express less confidence about arrangements for confidentiality and data sharing than those in England, and consequently appear to engage in less consistent practices.

Our research also demonstrates that the key variable shaping local practices is the institutional setting in which inter-agency working occurs. 'Institutional setting' has two key dimensions, and careful attention is needed to both. Firstly and most obviously, we found a positive relationship between the establishment of positive, formal regulatory and legal frameworks for data sharing and the establishment of more effective data sharing practices. For example, the existence of s. 115 of the Crime and Disorder Act appears to encourage English police officers to share data (perhaps too aggressively so, in some cases), whereas its absence in Scotland appears to inhibit such practices.

However, formal regulation is by no means enough to promote effective and appropriate data sharing. Its value probably lies as much in its existence as in its content (we found few people who knew very precisely the terms of the DPA, or who had actually read any of the many guidance notes or protocols that have appeared in this field), and it is effective only when it is both supported and mediated by an appropriate mix of other institutional attributes. Thus, the second dimension consists in the informal and unregulated practices which affect such important matters as: the degree of organisational cohesion stemming from shared values and purposes; the tolerance of risk, and understanding of risk management, including appropriate strategies for containing blame; space for policy entrepreneurs to negotiate workarounds to cover gaps or inconsistencies in formal regulation or legal frameworks; and political skills in brokering between agencies with different values, priorities and professional codes.

Overall, we found that an over-reliance on formal regulation, unsupported by appropriate informal arrangements, tends to inhibit effective data sharing, by causing staff to lose confidence in the exercise of common-sense judgments based on professional training or experience. In such situations, staff may tend excessively to strive to avoid false negative judgment errors, with the consequences mentioned in Q2 above.

Question 8.

Comments:

It follows from our answer to Q7 that over-reliance on informal or unregulated practices can lead to excessive data sharing and inappropriate breaches of confidentiality, so that there is an excessive risk of false positive judgment errors, with the consequences we spelt out in Q3 above. However, in our sample, we found fewer examples of staff with cavalier attitudes to false positive errors, than of the converse. They tended to work either in law enforcement agencies engaged almost exclusively in data sharing for purposes connected with the management of risk to the public, such as the English police, or in agencies (such as social landlords) that were newly involved in partnership work in such fields. A characteristic of these latter type of agencies was that (in contrast, say, to those in the field of health care) they tended to be insufficiently confident in the values on which their own, less aggressive practices were based to assert them effectively.

However, an important and consistent, if unsurprising, finding is that many staff in a wide range of frontline agencies feared that strong government pressure for more data sharing was pushing their service towards a systematic bias towards risking more false positive judgment errors. They therefore assumed (in the ratio of about 3:1) that blame was in future more likely to attach to false negative than to false positive errors.

In our view, the findings reported in Qs 7 and 8 show that the promulgation of formal regulation, in the shape of legislation, top-down guidance or model inter-agency protocols issued by central government has been salient in increasing the profile of data sharing as an important plank of the government's social policy. However, there are clearly a number of fields of public service where appropriate understandings and practices are insufficiently embedded in the everyday life of agencies for staff to engage in the sharing of data, and even in inter-agency negotiations about data-sharing, with confidence and consistency. This is particularly the case in the growing number of fields (such as child protection, public protection, youth offending services, substance abuse services and mental health) which attempt to reconcile the delivery of benefits to individual clients, whilst also protecting the public more effectively from the risks posed by such clients.

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

Question 9.

Comments:

We restrict our comments to a feature of the Data Protection Act 1998 (DPA) that is relevant to guidance for data-sharing: our comments on Principle 2 can be found in our response to Question 10.

The DPA neither inhibits appropriate data sharing nor promotes inappropriate data sharing. However, for this reason, the DPA necessarily and rightly creates wide areas

for discretionary decision-making that require the exercise of judgment, and this is often perceived to be its major weakness in the eyes of those practitioners who seek certainty and who perceive the DPA as too ambiguous for their needs. Our research uncovered many examples of frontline staff who either called, in effect, for legislation to offer them algorithms that would obviate the need for judgment. We also found many staff who assumed that such algorithms must be immanent in the DPA, and that the root problem was that the available guidance failed to explain them with sufficient clarity.

However, it is probably not worth embarking on yet more exercises in drafting written guidance to the DPA, whether centrally (as was done by the then Department for Constitutional Affairs in publishing its 2003 'toolkits') or locally (as is done in a wide range of local inter-agency protocols). Our evidence suggests that they are hardly ever read or used. In any case, they can never deal with the underlying dilemmas of making judgments where there are competing imperatives as between data-sharing and maintaining confidentiality. Instead, it may be much more useful to help organisations to understand and better manage the risks inevitably associated with exercising judgment, especially in sensitive fields. This task, we think, is a more important and urgent one than amending the DPA, and we explain how it should be undertaken in our response to Question 19.

#### Question 10.

##### Comments:

That the finality principle is sound as a general statement follows from the basic imperatives of confidentiality protection. In the public services, the principle's restriction on obtaining for lawful purposes does not rule out very many things that public authorities in England typically have good service-based reasons to do. However, the principle also restricts obtaining to "specified" purposes. Specification is far from straightforward, either in case law or in professional practice. The impact of many programmes for inter-agency partnerships, joint working arrangements and horizontal coordination, collaboration and integration has been to put significant strain upon the restriction to "specified" purposes. This strain arises because of the addition of purposes to the work of agencies that had previously defined their purposes in handling clients' personal information in terms of the organisation's domain. In children's services and even in education, the addition of child protection goals has been broadly accepted as not straining the finality principle unacceptably. However, the dominance since the early 1990s of risk management in adult mental health has been argued by many professionals in the field to have begun to put real strain on the notion that patient record information is collected and processed principally for purposes of health care. The addition of law enforcement, anti-social behaviour, and even illegal immigration detection functions to a variety of services (e.g., education, social rented housing management, health care) through the use of regulation and statutory duty, and of non-statutory policies and guidance for partnership working, has also led to tensions in some areas. The possibility that some services may be involved in indefinitely many partnerships, each of which may add purposes for

the use of their personal information, certainly strains the idea that the word “specified” implies that the purposes are “defined” or “limited”, or those that most clients would expect when they use a service. Of course, it would generally be accepted that there are situations in which public interest claims must override the expectations of clients. However, the uncertainty created by recent policy developments is problematic in many areas. There may be a case for further work to clarify the concept of “specification” in the finality principle.

Question 11.

Comments: We offer no comment on this question.

Question 12.

Comments: We offer no comment on this question.

Question 13.

Comments: We offer no comment on this question.

Question 14.

Comments: We offer no comment on this question.

Question 15.

Comments: We offer no comment on this question.

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

Question 16.

Comments: In many services, many of the legal and operational risks associated with case-by-case decisions about information sharing can be significantly reduced by securing the consent of the individual concerned, even though consent may not be legally required for information sharing. For example, in most routine contexts in health care, social services, housing management, employment support and even tax and benefits administration, most professional and frontline staff have long known that this is standard practice, and it is often routine. Social workers, for example, often work through consent to any information sharing that can be foreseen in the first substantial interview with a client, and our research found similar practices in many fields, including social housing, youth offending services and specialist medical services such as substance abuse.

However, obtaining informed consent does require staff time, resources and careful recording of the information provided, especially the extent and nature of the consent granted.

Consent is not always a straightforward matter, and it may be unwise to rely on extending consent as a way of obviating risk. Determining whether consent has been granted effectively and relevantly is often difficult. Moreover, even when consent has been granted for sharing, it does not follow that sharing is necessarily wise. The reasons for this are briefly summarised in Box 5 of the accompanying report, as follows:

Box 5: Conditions for valid consent

- (a) Consent must be informed: however, it may not always be obvious just what information the practitioner must convey before someone can be said to be sufficiently informed to make a soundly based judgment about whether they would like one agency to share information about them with another;
- (b) It must also relate to specific instances of information sharing. However, some of the most difficult issues about consent arise where it is believed that a client has given implied consent to certain information being shared with certain other agencies. Just how far implied consent should extend can be difficult to determine, and it may not be clear at what point the individual can be said not to have impliedly consented to the sharing of information where there may be an 'off chance' that it will be needed; and
- (c) Consent must also be voluntarily given. However, there are problems where the giving of consent may have been regarded by the individual as an unavoidable condition of receiving a service, rather than as an unconstrained choice.

There are also many situations when consent cannot, for some reason, be obtained, and there may be others when a client subsequently regrets granting consent and wishes to revoke it. Additional complications arise when clients agree to the sharing of some information but not other information, or with some agencies but not others. Consent that is 'segmented' in this fashion can give rise to some dilemmas for practitioners. This may be particularly true where a client agrees that one piece of information, T, can be given to another agency, but does not agree that they should have access to another piece, S, but where a situation arises in which the other agency either cannot use T, or would be in danger of using T in ways that might be damaging, if they do not know S as well.

Other problems may arise because practices around consent differ significantly from profession to profession and service to service. While medical and surgical professionals are trained in highly structured consent procedures, for instance with regard to medical treatment, most teachers, school administrators, housing managers, voluntary sector staff are not. Conversely, many law enforcement officers tend to assume that there are few occasions on which they would rely principally upon consent, because other grounds would normally be available. With the advent of more joint and partnership working in pursuit of 'joined-up' services, this inconsistency of practice has become a serious issue in securing the support of frontline staff, and probably their clients too, to increased volumes of information sharing in public services.

There are also many situations in which the availability of consent cannot settle the question of whether or not to share - for example, where

- the reasons for sharing or not sharing do not primarily refer to the well-being of the individual, and sharing must therefore be justified on other grounds (such as the public interest, or the overriding interest of third parties, such as children; and where

- the individual is not deemed to be capable of giving consent.

For these reasons, where local negotiators are engaged in agreeing terms for future sharing arrangements, those rules are unlikely to be based on requiring individual consent, at least as the sole condition of sharing data. This means that most inter-agency arrangements will also need to put in place agreements about the conditions for non-consensual data sharing.

People may become cynical about public services if they found they were asked to consent to information sharing that would take place on other grounds in any case even without their consent, leaving their act of consent without moral or even legal force. If there is no risk that the purpose of the service intervention would be thwarted by the data subject's knowing about the disclosure, then the situation should be explained to them, but consent should not be solicited.

Question 17.

Comments: See answer to Q16 above

Question 18.

Comments:

Question 19.

Comments: Q. 19

Referring to our remarks on guidance in response to Question 9, we are mindful of the valuable contribution made by the ICO's 2007 Framework Code of Practice for Sharing Personal Information (FCP), which we believe goes some way towards clarifying many of the issues that are faced by data-sharing decision-makers at several levels. The FCP systematically provides step-by-step guidance, largely in terms of compliance with the data protection principles which are the bedrock of the DPA. We understand that the ICO may be inhibited in departing too much from a compliance approach of that kind, and we believe there is much value in promoting good practice in that way, and by opening the way for specific codes to be tailored to local circumstances in a consistent manner.

On the other hand, we believe that, where the FCP cannot, of necessity, go further than it has done, there is room for the development of additional or alternative decision-making procedures that not only build on a sense of what could (i.e., legally) be done in respect of data-sharing, but go further in assisting decisions about what should be done (i.e., professionally and ethically). For example, in several places (e.g., 1.4; 3.3; 4.2); the FCP rightly puts the onus on practitioners to decide on the relevance of certain pieces of information to the achievement of their objectives. Or it leaves it to their 'experience and professional judgment' or 'expertise' in deciding whether data-sharing is necessary or how to arrive at a 'balanced decision' about how long to retain information.

In such matters that call for judgments – often in urgent situations involving very sensitive data – practitioners at the front line, as well as higher-level managers, may

benefit from gaining expertise in developing strategies and using techniques that help assess the risks and benefits of data-sharing beyond the ascertainment of legal compliance.

In our answer to Q27 below and in the later sections of our report to CLG, we set out an approach designed to assist practitioners with this challenge.

We endorse the ICO's espousal of privacy impact assessment (PIA) as a valuable technique, that could be adapted to the specific circumstances of data-sharing, although the models and templates for PIA were not originally developed for purposes beyond those of single data controllers. We note that the ICO's recent FCP (section 1.2) recommended the use of PIAs where organisations are beginning to think about instituting data-sharing as a regular procedure. Enhanced by the ICO's recent promulgation of a PIA handbook, this is a timely suggestion which could have important practical force. As previously mentioned, the 2004 report by Raab and 6 for the Scottish Executive on a possible PIA for eCare was broadly supportive of the use of this technique, suitably adapted to the specific case. We believe there are substantial benefits to be realised in terms of privacy-friendly project design, better staff awareness of the privacy issues in data-sharing, better understanding of management responsibilities, and improved transparency. PIA is thus an important way of bolstering public trust and confidence in the sharing of personal data, and in the responsible collection, storage and use of these data. It might be for consideration whether PIA should be mandated for certain new systems, as occurs in the USA and Canada.

## **Section 5: Technology**

Question 20.

Comments: We offer no comment on this question.

Question 21.

Comments: We offer no comment on this question.

Question 22.

Comments: We offer no comment on this question.

## **Section 6: International comparisons**

Question 23.

Comments: We offer no comment on this question.

Question 24.

Comments: We offer no comment on this question.

Question 25.

Comments: We offer no comment on this question.

Question 26.

Comments: We offer no comment on this question.

## **Section 7: Additional questions**

### Question 27.

Comments: In our view, the most urgent imperative, in developing a more intelligent approach to the governance of information sharing, both among the public services and between the public services and their private and voluntary sector contractors and providers, is not for more legal guidance, nor for even more codification of professional ethics or local protocols, nor yet for primary legislative change. We believe that the research evidence shows clearly the limits of what can be achieved by the use of such blunt instruments. This is because, as all the current guidance recognises in its call for the exercise of professional judgment, the need for such judgment can never be eliminated.

Policy makers must therefore accept some significant degree of variation and inconsistency in data sharing practices, from locality to locality, from service to service and from team to team, because priority is given to different types of benefit, even in dealing with similar cases in similar fields. Law and codification can but limit the degree of variation. It is also the case, however, that deep-seated conflicts about data sharing priorities have often surfaced in protracted inter-agency negotiations about local data sharing codes and protocols. That is, the process of codification often shifts the site of disputation from the case to the code.

Codes must therefore always be framed in ways that allow people to make judgments in novel, unpredictable or complex situations under general principles.

Rather than more codification, the most urgent policy imperatives are for

- the development of tools with which to cultivate more self-conscious use of professional judgment, in order to enable professionals more confidently to articulate the bases on which it is made, and thus to engage more readily and easily both in local negotiations with other agencies over shared practices and to make case-by-case judgments in their own practice;
- the development of generic approaches to the training of local negotiators and professionals. so as to cultivate the art of thinking about risks and benefits in structured ways, in order to come to more intelligent and confident judgments; and
- the development of cultures and practices of management that give less weight to individual blame for professionals, especially when they make judgment calls about sharing or not sharing client information that turn out badly, but do so conscientiously for reasons that were defensible at the time. Such practices should be aimed at reducing incentives for defensive decision making and for “kicking difficult decisions upstairs”, and for mechanical and literal application of explicit codes. The purpose is to encourage street level professionals to take responsibility for judgment-making. This is especially important where professionals perceive themselves to be at risk of making judgment calls about sharing or not sharing client information that may turn out badly, and need confidence to do so conscientiously for reasons that are rational and defensible

at the time they are made.

In §11 of the appended report, and in its annex, we set out the basic elements that we believe should inform the tools and approaches to such training.

In §41, we discuss the importance of a less blame-oriented management and political culture in sustaining cultures within which apt and astute professional judgment can flourish and be exercised with confidence.

We urge that the challenges of cultivating intelligent and articulate professional judgment, and of creating a managerial culture of learning from errors rather than pursuing individual obloquy, should be seen as important, critical policy imperatives and priorities. These are not merely issues for professional education and management training, even if those are the most useful instruments with which to address the immediate deficit in practice.

Question 28.

Comments: