

Data Sharing Review

Section 1: Background

Question 1

Please explain what your interest in information sharing is.

BCS is the chartered professional body and learned society for IT and computing in the UK. BCS is tasked with advancing the knowledge, study and practice of IT/Computing in the UK for the benefit of the public. BCS has a large and growing membership of around 63,000. Members are drawn from the public and private sector, academia, and a vast array of specialist areas. Members work together in the form of focused specialist groups, and forums covering areas such as security, ethics, health and education.

The issues around information sharing are of great importance to individual members across this community and to the BCS collectively. The BCS has been looking in particular at the use of personal data in the public sector over the last two years. The basic premise is that increased data collection, use and sharing across the public sector is not only inevitable, but when done well, beneficial. However, there are many concerns about current practice.

This response incorporates input from a number of groups and individuals inside the BCS, including the BCS Information Privacy Expert Panel (BCS-IPEP) and BCS Health Informatics Forum (BCSHIF). Due to the level of interest shown in this review from the BCS Health Informatics Forum, BCS has decided to include the HIF response as a complete document in Appendix 2. This, we hope, will give a valuable insight in to experiences of data-sharing within the health sector.

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.

There are many benefits that are or could be realised by personal information sharing, usually specific to the circumstances where it takes place. In general terms, individuals can benefit from services that revolve around their needs rather than those of a specific department or sub-group within an organisation. Where there are important statutory or ethical obligations to individuals it may be that sharing personal information is a pre-requisite to meeting those obligations, particularly for vulnerable groups.

An example would be appropriate sharing of data between different agencies that deal with children, such as schools, social services, health care providers and police.

At a societal level, many of the goals around citizen-centric public services are widely-recognized as beneficial, and are only possible with data sharing. It is also important to recognize the potential economic benefit, not only in terms of efficiency and cost reduction, but in enabling new services or markets.

Sharing personal information within law enforcement or security services is also recognized as necessary for public safety and criminal justice.

A good example of appropriate and useful information sharing has been around vehicle taxation. Putting insurance and MOT information together, and an online process, has been broadly beneficial to individuals by making the process simpler and more easily accessed. It has potential societal benefits in terms of reducing criminal behavior, and more efficient, cost-effective and paper-free service delivery.

Question 3

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

Collecting, using and sharing personal information at a national level brings with it new and emerging risks, and these risks are almost by definition un-quantified, and perhaps even unknown. Widening access to stores of personal data or increasing the size of those stores increases risk and introduces new ones. An element of risk exists for any use or storage of personal information – paper or electronic – but use of IT and Internet technologies brings a range of positive and negative consequences.

Some of the important risks around information sharing arise from loss (or even use) of meta-data and contextual or procedural knowledge embedded in the original context of collection and use. This may be as simple as losing track of the consented purpose of information, or as complex as mistaking intelligence based on hearsay for hard evidence. A lack of information about sourcing or confidence can lead to misinterpretation. Data quality such as errors, duplication and mis-filing that would have been dealt with simply in a local context can be catastrophic for processes in a shared context.

For individuals, the risks ultimately stretch from personal inconvenience through to invasion of their privacy, financial and reputational damage or even collapse. Loss, exposure or corruption of an individual's personal data can ultimately contribute to poor mental health or even suicide in extreme cases.

At a societal level, some of the most important risks are around public confidence in government and commerce. If public confidence is weakened by incautious or inappropriate sharing of data, then society's ability to pursue wider goals will be threatened.

In balancing these risks, it is important to recognize that the benefits of sharing are sometimes clear and immediate, while the risks may be more abstract, diffuse, longer term or hard to recognize. Recent public and private sector data losses have provided examples of not only the risks and potential risks, but also of the way decisions can be made without a full picture of the consequences. In that sense, a fundamental lack of education and culture of data protection in a data-sharing context lead to some of the gravest risks.

It is vital also that the requirements of informed consent are taken seriously, and not an afterthought, otherwise trust will be undermined. Individuals need to feel that their information is being treated with respect; when consent is properly obtained it reinforces a positive view. In the public sector, cases where information use is (inappropriately) not

consented to can undermine broader perceptions of personal information use in government.

Finally, sharing of personal data can also lead to larger and more visible targets for attack. Large, multi-departmental databases, for example, could emerge as de facto national critical infrastructure. While it may be convenient to pool and share personal data in the public sector, financial and personal security is often built on the assumption this data is not available to any one individual other than the subject. As well as increasing the temptation for public sector workers, large or more detailed systems can become a highly attractive target for fraudsters, and hence at greater risk.

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.

The greatest opportunities tend to arise where the evaluation and treatment of risks and benefits revolves around the needs of the individual. For example, personal information sharing within healthcare can clearly and directly lead to better outcomes for individual patients. Effective interaction across different service providers in the context of child protection does require information sharing, but again where the individual's needs are at the heart of policy, the outcomes can be highly beneficial.

The best way to achieve that benefit is through a mature process of engagement and information governance. The balance of risks in a personal information context needs to be discussed and evaluated with stakeholders and subjects of that personal information. It may well be that 'trust' in those sharing personal data is not about an evaluation of capability and ethics, but about perceived incentives and restitution. In a situation where the practice of information governance is to a high standard, individuals can easily identify, communicate with and seek action from those who have authority and control over their data. By contrast, it is often the case that unclear responsibility for personal data can in effect mean an abdication of responsibility across an entire organisation that is more accurately perceived as such externally by the public than within the organisation itself.

Much of these issues are of course pertinent without wider sharing of personal information taking place. However, in a sharing environment the risks are greatly heightened as the context in which issues arise may be even further disconnected from the one where data is entered or maintained. When information is corrected in one context, there needs to be a process to propagate and audit changes wherever else that information has been passed or made use of. In practice, this usually requires systems that are designed with that requirement from the start, rather than as an add-on.

Some of the most worrying trends in the public sector are where personal information is shared across different data protection cultures and contexts, and where re-use is for starkly different purposes (from the individual's point of view). For example, detailed, personal and highly-sensitive information may be passed to healthcare workers in the context of a professional relationship without any consent for making it available to a wider group of people or government officials in another field. Taking a view that consent

was implied, or that exigencies of a situation override the need for consent could ultimately damage professional relationships and willingness to provide information in future.

Poor communication also generates risks, particularly around consent and where data collection has mandatory/statutory components alongside voluntary. When combined with areas where withdrawal of consent is either difficult or impossible this can create a great deal of ill will.

Finally, where there is a pressing need for sharing of personal information but no well-designed technical mechanism, this tends to lead to work-around solutions that can present unacceptable risks that are not immediately obvious to auditors.

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.

Examples of public authorities holding too much personal information include:

- Education information derived through the Key Stage (SATS) process where there is no mechanism for giving consent or opting out, and the data is shared very broadly.
- The National DNA Database holding personal information on individuals without consent and without conviction. Where samples are stored, the information contained within may in effect be extensive and highly sensitive.
- Sensitive health data relating to vulnerable adults, persons under public protection and children at risk may present risks that cannot be mitigated by current protections.

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.

Private sector organisations holding too much information:

This is not such a problem in private sector organisations but it does occur:

- Within the hospitality industry, where hotels demand identifying information from guests at check-in.
- By larger retailers. For example, shops that demand name and address information before they will issue a VAT receipt.

In both cases, consumers are not informed about what data is being collected, by whom, or for what purpose.

Private sector organisations holding too little information:

- Data shared between the NHS and private care homes. Sometimes care homes struggle to obtain sufficient care information about residents to adequately care

- for them. Sometimes they receive information which is not necessary for the service they provide.

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.

There are numerous cases where information is not being shared, but could usefully be. Across the many branches of healthcare there is a great deal of work taking place to appropriately join up, for example, primary and secondary healthcare. Quick and efficient transfer of records between GP surgeries to follow patients is also clearly beneficial, but not yet taking place outside pilot schemes. There are also clear cases in the criminal justice systems where data is not being effectively shared between police, courts and prison systems with a range of resultant issues.

In all these cases the barriers are complex, and usually combine financial, structural, technical, cultural and legal issues in a way that is hard to unpick. Some of the themes seem to be around underestimation of the criticality and complexity of information governance, and of how much organisational (rather than technological) change needs to take place alongside information sharing.

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.

An example where the BCS has repeatedly expressed concern has been over intentions to widely share general medical records (as distinct from summary care records). The benefits for patients and for research were records to be centralized (or virtually centralized) are unclear. The risks to such large scale storage and wide access, however, are very large. This is in contrast to the clear patient benefit and lower risks of transferring medical imaging, test results and appointments between primary and secondary care systems.

The risks include:

- the target such systems represent, particularly as so much valuable information is concentrated
- the difficulties in effectively auditing and policing access on this scale

- Inflexibility of systems leading to a lack of granular permission control, or local work-around solutions that compromise security – e.g. sharing passwords or access keys

These risks may well be worth a trade-off for large and widespread benefit to individuals, but much of the cited benefits do not require centralization of systems.

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.

The principles of the DPA are clear, concise, widely accepted and have broadly ‘stood the test of time’. The act has also led to mature, sustained and productive debate on the issues. However, the act is weak in two specific areas. The first comes from the new challenges of dealing with personal information protection when it is collected, used and shared on a large scale. Definitions of the ‘data controller’ become unwieldy, as the organisations and use are so large that responsibilities have become organisational and abstract rather than personal and specific.

The BCS has been working on this specific issue, and has produced a position statement that outlines proposals that could lead to changes in the Data Protection Act. This statement is included as an Appendix 1 to this submission.

The second area where the DPA is weak is enforcement and audit. Where breaches occur, the actions and penalties are not sufficient to act as a deterrent. Audit, particularly on a large scale, appears to be insufficient.

Enforcement, however, needs to be proportionate and act on those with authority, responsibility and capability. Authority, responsibility and capability in many cases will be spread across different parts of an organisation. In the public sector, a Minister may have responsibility, a senior official may have authority, but the person with capability and sight of the issues may have access to neither.

In other compliance areas, there are regulations and professional responsibilities that have, if not the force of law, a positive impact on behavior. This is one of the reasons why the BCS has been working towards professional status for information technology practitioners. It may be that exploring solutions in this area could have a wide and positive effect without requiring large scale and direct legal action.

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.

Re-purposing and re-processing of data inside the public sector has become routine. Through secondary legislation officials are able to bypass the second principle. While the reasons for this may be logical, they may amount to convenience for the department rather than benefit for the individual. Without necessarily any intention to do so, this has resulted in an erosion of the second principle.

The second principle could be described as a codified expression of part of the wider government-citizen social contract. In that context it protects the citizen against excessive concentration of power in the hands of government officials. If public servants can access or change records through sharing systems on tax, criminal justice, health or education without a) a clear purpose for which that data was collected and b) clear communication of that purpose and consent received, that puts a great deal of power in their hands. It is very rare that such power is necessary, and where it is needed there are already routes for access with audit and even judicial oversight. Without the second principle, there would be no realistic barriers to curtail an unnecessary and potentially dangerous level of sharing.

Question 11

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

Technical

The enforcement mechanisms for the DPA are insufficient: breaches that may cause considerable suffering for individuals, such as damaged credit reference histories, rarely result in any meaningful penalty for data controllers.

Institutional

Even when enforcement (or reputational damage) occurs within the public sector, it may not directly affect those who have failed in their duty of care.

Societal

The public may have become unresponsive over data protection problems because of a lack of accountability. Despite great efforts by the ICO, complaints are often ignored or require a great deal of perseverance to see through. The balance of power between individuals who may have suffered because of breaches and the organisations responsible is such that the individuals may be safely ignored.

In the end, this may lead to a situation where individuals refuse or withdraw consent en masse because of negative experiences. This could also result in the DPA being ineffective, as part of the reason for its existence is to provide an environment where individuals can safely and confidently share their personal information with the public and private sector.

Question 12

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

In addition to the position statement attached to this submission, there are a number of measures that need to take place around audit and enforcement. There is also clear scope for increasing use of minimum standards and best practice, and the BCS would be interested to explore how chartered status (for example) could be combined with recognized standards and practice to develop more meaningful safeguards.

BCS believes that the following provisions should also be considered:

- All government information sharing should be notified to, and audited by, the Information Commissioners Office (this is already the case in New Zealand, where it is mandated by the Information Privacy Act 1993);
- The Information Commissioners Office should be provided with powers to initiate inspections, investigate offences and bring criminal prosecutions against deliberate or repeat offenders.
- Penalties for offending need to be reviewed and increased to match the impacts of breaches on citizens. For example, convicted offenders should be disbarred from acting as company directors. They can also be stripped of professional status, although this is rarely used.
- Failure to have proper risk assessments and regular audits available on file could be de facto evidence of non compliance. In some circumstances, risk assessments and audits may even need to be published to increase confidence.
- The ICO should be resourced to provide better guidance, audit and support to facilitate compliance for those who need it.

For these measures to be effective, the Information Commissioners Office will require greater resources and a shift from its primary stated purpose of encouraging good practice towards more active measures such as enforcement.

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.

There is a certain amount of confusion arising from legislation such as the Housing Act, Children's Act and others as they appear to conflict with the DPA. More generally, secondary legislation in a wide range of areas has eroded the principles of the DPA as they apply to the public sector. There is also some confusion around the relationship between the DPA and FOIA that may require further clarification (if only through explanatory notes).

On a more positive note, the Financial Services Authority has been able to use banking regulations to encourage and enforce good data protection in that sector.

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.

BCS believes there is a need to shift the focus of statutory powers from permitting sharing, giving further weight to securing information and enforcing the DPA. Both public authorities and private organisations should incorporate traceability mechanisms and a greater right to audit data management processes so that their sharing is made more transparent to the citizen – who cannot, after all, submit a Subject Access Request to an organisation if they are unaware that processing of relevant personal information is taking place.

Star ratings awarded to public authorities should also take into account DPA compliance.

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.

Responding to DPA ‘subject access requests’ can be time-consuming and costly, however, this tends to be concentrated on specific sectors (such as health trusts). There may be scope for supporting the streamlining of processes where there is undue burden.

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 ICO and other bodies (including the BCS) provide very clear, concise and practical guidance on these issues, and best practice seems to be generally well understood in the private sector.

Question 17

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

Such a requirement already exists, and a lack of consent (or proof of consent) on existing data sets presents a clear barrier to sharing beyond what has been consented to. It may be that obtaining consent is costly or otherwise difficult in such a situation. This is not, however a reason to ignore the issue of consent.

It is important to recognize that there will be occasions where a need to gain consent in order to share is overridden by clear and immediate benefit to the individual. For example, in situations where emergency care is required, clinical decision making may require un-consented access to clinical history to prevent injury or loss of life. The Health and Social Care Act states that it is not necessary to obtain consent if it would not be practicable to do so. What is 'practicable' is debatable, and has been misused. Further clarity would be useful in this case.

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?

Under current law it is not possible to consent to sharing without having been provided with a 'plain English' complete and compliant Fair Processing Notice, and this should continue to remain the case.

Information sharing would be made more transparent through greater respect for obtaining consent. Furthermore, individuals need strengthened access rights not only to the data but to metadata/derived data and audit trails so that data subjects can see what information has been created, and how their information has been used.

Specifically for the public sector, there are a number of suggestions for strengthened access rights in the position statement in the appendix.

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 Framework Code of Practice and Privacy Impact Assessment approaches are well thought out in themselves. However, they are only really used by those already complying with the DPA. It is unlikely to have any effect on organisations that are failing to comply either willfully or through ignorance. Furthermore, the Code of Practice is based on the assumption that the Information Commissioner's first statutory duty is to promote good practice, and hopefully that will expand.

Policy set out by the ICO on information sharing is developing well in a way that engenders confidence, but is of little use unless that policy is enforced and adhered to widely.

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.

Technological advances have and will continue to enable larger, wider and more sophisticated collection, storage, use and sharing of personal information. For example, an optical disc such as CD or DVD, or a flash device, can store significant personal details on the entire population of the UK. The ability to copy, store and analyze on this scale has radically altered the risks, challenges and methodologies around sharing and protection of personal information.

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?

The law simply cannot keep up with technical changes. Instead, the law should focus on infrastructure and requirements that refer to minimum standards and best practice that is set, updated, maintained and disseminated elsewhere.

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?

The DPA already caters for protecting privacy whilst facilitating activities such as performing medical research, and should not be treated as a barrier to those activities. The statistical community has long been able to effectively anonymise data for research purposes, and procedures are well understood. What is less well understood are the technologies that can support privacy protecting techniques, and it is in this area that research could assist.

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.

The New Zealand Information Privacy Act 1993 is seen as a successful legal framework for sharing and protecting personal information, and could be useful in a UK context.

Question 24

Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

No comment

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?

No comment.

Question 26

Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

No comment.

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?

As outlined in the position statement in Appendix 1, information governance is both vital and poorly understood. Alongside a great deal of legal, regulatory, technical and technological work to develop that, there is an important role for training standards and awareness work.

Question 28

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

The view that citizen-centric services and good data protection are somehow in conflict is one not shared by the BCS. This view is to some extent propagated by the different levels of acceptance and understanding of the data protection agenda across government. This is largely cultural, and immensely challenging. There are in different parts of government good examples of governance, security and awareness that need to be shared. There are also some mechanisms for doing so, but there could and should be more.

What seems to often stand in the way is the way data protection and sharing issues are regarded as technical, or the purview of technologists. Instead, policy and implementation need to both take the issues seriously, and have good data protection at heart.

In that sense, the recent government data losses have raised the profile of these issues, but the current climate of interest needs to be turned into action. This review is an important part of that process.

BUILDING TRUST IN eGOVERNMENT

BCS POSITION STATEMENT ON DATA GUARDIANSHIP

The BCS supports the increased use of technology to hold information needed to deliver services, since there are myriad potential benefits to be had from information and data sharing. The BCS also recognises the corresponding risks that attach to an increase in data/information sharing and the ubiquitous nature of the wired world in government, commerce and society. The BCS therefore advocates a sensible and cautious approach to information sharing that seeks to optimise the benefits, whilst being aware of and guarding against the risks. This is particularly important in the government arena where the potential threat posed for civil liberties and personal privacy should be acknowledged. The BCS therefore welcomes eGovernment initiatives, but urges the development and application of information governance and common sense guidelines that are needed to underpin the guardianship and use of citizen data held on public systems.

Those holding personal data should recognise that the risks to data held in electronic form are greater than those for the same data on paper. So the technical and procedural measures to protect them need to be stronger to reflect the greater risks associated with holding large collections of personal data electronically. Such collections may, therefore, need to be assigned 'Impact Levels' (for confidentiality, availability and integrity) and be treated accordingly by following an extension of the current established security accreditation processes into the area of information assurance.

As a starting point the BCS is proposing that the information governance and data guardianship principles for personal data should include the following (outside the arena of legal obligations and the prevention and detection of serious crime):

Accountability

1. All government departments should follow sound, publicly accessible, information governance principles (clear responsibility, accountability, authority and processes for: collection, retention, identity matching and sharing, dissemination, disposal, risk assessment and audit of personal information) in order to foster public trust in their data guardianship.

Visibility

2. Citizens should have the right to be informed of and to have free access to all the data that is held by the government about them.
3. Citizens should have the right to correct data about themselves if it is wrong.

Consent

4. Citizens should be asked for their informed consent in respect of private data to be held about them for a specific purpose.

5. When it is suggested that such personal information might be used for a purpose other than that for which it was originally collected, the consent of individuals should be explicitly obtained.

Access

6. Citizens should have a right to know which officials or groups of officials (e.g. the police, all staff in DWP and HMRC, doctors) will have access to the personal data (that they have consented to have held) and who has actually accessed data about them.
7. For elements of specific types of private data, e.g. personal healthcare information, the citizen should have the right to limit who has access to the data without his or her explicit informed consent.

Stewardship

8. The original collector of personal data should have a duty of care with respect to that data. They must ensure any organisation sharing it understands both the risk assessment associated with that data holding and any caveat associated with its integrity and appropriateness for use for purposes other than that for which it was originally collected (e.g. has it been verified or is it interpretation and hearsay, when was it collected and does it have a finite useful life, has it been cleansed).

The Data Protection Act 1998 was written in an age of 'data silos'. While it covers several of these points (see Annex A), it does not cover all aspects of data guardianship in the 'data sharing' age adequately, nor does it cover information governance.

A legal requirement to undertake a formal risk assessment of any system holding personal data should also be considered, with the results subject to independent approval. Such assessments are already legal requirements in other IT realms (e.g. safety critical and secure systems). The risk assessment should be required to take account not only of the government's interests, but also of the citizen's, both collectively and individually (see Annex B).

ANNEX A – Data Protection Act 1998, Schedule 1 - The Data Protection Principles, Part I - The Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
 - a. At least one of the conditions in Schedule 2 is met, and
 - b. In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. 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.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

ANNEX B – Possible Impact Levels for the Provision of Public Services

Risk is commonly defined as impact x likelihood. The measures required to protect IT systems are therefore dictated, in part, by the likely impact should the security of a system be compromised. Each possible impact is typically assessed according to its impact level, which may range from those that are negligible to those that have major consequences for the UK.

The following is an example range of impacts on citizens' privacy or the security of their personal data that would be likely to result should the security of a system or media holding such data be compromised. The list is intended to generate discussion, leading to an agreed approach to quantifying possible impacts, thereby enabling a methodological approach to defining appropriately robust measures for protecting personal data.

1. Loss of control of a citizen's personal data beyond those authorised by the citizen.
2. Loss of control of many citizens' personal data beyond those authorised by each citizen.
3. Loss of control of a citizen's sensitive or financially significant personal data beyond those authorised by the citizen.
A compromise to the identity or financial status of an individual citizen.
4. Loss of control of many citizens' sensitive or financially significant personal data beyond those authorised by each citizen.
A compromise to the identity or financial status of many citizens.
5. Widespread compromise of identity management systems or personal financial systems across the UK.
6. The collapse of identity management systems or personal financial systems across the UK.

**BCS Health Informatics Forum – Collective Response to Data Sharing
Review (Richard Thomas & Dr Mark Walport)**

Consultation : 12 December 2007 to 15 February 2008

Context

This collective response reflects the perspectives of members of the British Computer Society Health Informatics Forum (BCSHIF), which encompasses all the home countries and professions. These include (clinical and management) academics, system designers and developers, implementers and super-users of the full spectrum of health systems, processes and solutions. This response includes views of individual members working in Information Governance, commercial application suppliers, academia, the clinical professions and management consultancy.

The differences in the scale and scope of concerns relating to emergency care are real and significant. These need to be expanded upon once this high level consultation has concluded.

There are questions raised about the exact definition of some terms in this questionnaire – for example what constitutes ‘sensitive’ data. Even basic demographic data can create risks during data sharing.

Section 1: Background**Question 1: Please explain what your interest in information sharing is.**

Members of the BCSHIF are actively engaged in:

- all aspects of capture, handling and processing of health data
- developing and deploying processes to access, amend, share and use sensitive data in a high profile sector which affects all members of the public
- end-user clinician roles in direct contact with data collection and sharing among multi-professional teams responsible for patient care, and still in some cases using non-electronic sources

As an example one respondent works in ‘Information Governance (IG) within the NHS. This role involves promotion of best practice within the IG agenda by the local health community; a community made up of acute, specialist, mental health and primary care trusts. In addition, links exist to local authorities to facilitate best practice particularly in data sharing with social care partners. Most personal information collected and shared is, of course, patient or client information including basic demographics, clinical information, i.e. diagnoses, treatments and administrative information relating to appointments and

attendances. Information is collected directly from service users or via data sharing arrangements, i.e. care pathways - GP to secondary care. Information is shared by fax, email (NHSmail), electronically and via the physical movement of paper records, i.e. casenotes. Predominantly, the purpose for holding and sharing personal information is for the provision of health care. In addition, data is used for public accountability, including Government returns, audit, capacity and financial planning and other related matters. With explicit consent, information is often used for research purposes'.

Other responses indicated that the range of personal information collected, held and shared includes:

- Electronic patient / client and staff records
- Personally identifiable data for many purposes including research; additionally e-records of students in many disciplines.
- Controlled access to real data for assisting customers with system problems. Note - testing of applications is carried out with realistic not real data.

Personal information is collected, held and shared:

- Under European Directives in local, corporate and national databases; following local policies and national NHS Information Governance rules.

Personal information is collected, held and shared for purposes such as:

- Individual patient care, clinical decision making, facility management purposes; audit, monitoring and assessment.
- Corporately to assist user organisations to effectively use our software to collect, store, manage, process, audit and report on confidential patient data.

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.

Providing clinical care within the NHS is fundamentally based on the availability of complete, accurate and up to date personally identifiable information.

Benefits (a) to individuals

- Safer and best practice health care, wherever the individual patient interacts with healthcare staff
- Creation of a potential for personal ownership of your own entire health data & an enhances an individual's ability to check accuracy of the data held, whichever professional is using it

- Provision of care/treatment using seamless care pathways relating to the holistic clinical history of an individual which can then be utilized across organisationally boundaries
- Reduction in invasive data capture, reduction in duplication of (potentially inconsistent) data, creation of a consistency of context and a more complete history on which to base clinical decisions
- Improvement in individual care by an individual not having to correct or restate information at each clinical attendance. This requires that to be of benefit, the information stored must be accurate and up to date. For example, for the older person who cannot remember their medication, the benefits of shared personal information are self evident.

Sharing information between staff, sites and organisations is core to the delivery of high quality, patient-centred care.

Benefits (b) to society

- In identification of disease outbreaks, trends and patterns in illness, monitoring of performance and health research leading to earlier and more effective tackling of health issues
- When areas of risk are highlighted, shared records facilitate professional management of that risk to individuals from themselves and to the public; e.g. in cases of child or elder abuse and outbreaks of infectious diseases.
- Improved clarity of the detailed descriptive profile of a community, makes it possible to appropriately assess the needs and demands of a geographic area and to track the outcomes from planned health strategies and interventions more effectively
- When the risks and effort of duplicate data collection are removed by appropriately managed sharing – reducing the occurrence of inconsistent data and subsequent ill-informed decision making
- In research, record sharing contributes to greater understanding of trends in medical care and the efficacy of treatments.
- From better resource use and improved budgeting, based on accurate profiles of need, demand and usage – making resources go further
- Improvement in the provision of healthcare via data sharing benefits society with an improving level of health which impacts on children, workforce and longevity.
- In reduction of the cost and burden on the public of collecting information
- Complete consistent personal staff records of work activities, personal development, sickness / absence, training needs and professional registration help both the organisation and the individual staff member

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

Risks (a) to individuals

- Invasion of privacy and loss of autonomy, potential loss of control / oversight by the data subject.
- Personal information shared by accident or by design against the wishes of the patient or treating clinician can be exacerbated by mass data storage which increases the risk of exposure due to the large numbers of staff able to access it, due to lack of security measures or mishandling. For example - demographic details of abused spouses that reach the wrong hands could have tragic effects.
- Uncontrolled/uncoordinated amendment, within a shared system, of data elements of an individual's own record (even by authenticated, authorized professionals from different disciplines, sectors or domains) may result in data being mis-interpreted and consequent damaging actions being taken.
- Shared data, located in different stores may be updated without reference back to the originating (or other sharing) locations; thereby producing inconsistent records purporting to describe the same individual, with inconsistent consequential actions. For example, where health information is shared with social services to update their records and information that could have a bearing on the health of the individual is identified by a social worker and not passed back.
- Versions of data on non co-located databases relating to the same individual may not all be maintained as contemporaneous, resulting in jeopardy to decisions made on any of the sources.
- Many bodies, (for example, the Census, Small Area Statistics) routinely round figures to prevent even inadvertent release of personal information. If applied to health data, this can result in risks to the identification of low prevalence clinical conditions if alternative analytic procedures are not used.
- Data collected by one profession (using one set of data standards and definitions) being misinterpreted by another profession using a different set of data standards and definitions.
- Inappropriate unplanned use of personal information potentially resulting from theft/loss of personal information, e.g. HMRC, the armed forces, some health trusts.

Risks (b) to society

- The loss of trust by the general public in the competence of any public sector body, government department or other organisation to safeguard personal data may prompt the public to be reluctant to volunteer information and be cautious regarding 'databases' generally.

- Not sharing necessary information can incur significant clinical risks, when strategic clinical decisions have to be taken on the basis of incomplete information. For example, deductions and decisions made on incomplete, inconsistent data may result in incomplete planning data for epidemiological monitoring, locating of new health facilities, managing of demands made on health facilities
- Inappropriate (wrong or untimely) alerting of professionals to potential health risks from an individual may result in increased risk to (sections of) the public, harassment of individuals or collective panic which could spark detrimental actions

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.

Greatest opportunities

- Sharing of health records with (explicit) informed consent for specified actions amongst authenticated, authorized professionals who have a legitimate relationship with the individual on a need to know basis can result in enhanced clinical interventions and patient outcomes
- Through a single sign on, it will be possible to only 'inform once' and have information shared between necessary parties; for example when someone dies their relatives can inform a shared service which contacts public bodies, e.g. NHS locations, about releasing outstanding clinic appointments that will be no longer used. This benefits NHS efficiency, people who use the released appointments for investigations earlier than planned, and relatives who no longer get distressing calls for appointments for the departed individuals.
- The ongoing activity around record subjects opting in/out of having their records uploaded and made available provides lessons for future consideration. For example the NHS National Programme for IT pilot in Bolton which is creating Summary Care Records widely accessible to a range of authorized professionals has been accompanied by a considerable communications campaign; the Scottish Emergency Care Record project is similar. Evaluation of the lessons and outcomes from initiatives like these should be utilized in determining a satisfactory way to progress.
- Techniques such as encryption, anonymisation & pseudonymisation, as already deployed in some NHS projects, have a definite role to play. Formal assessment and evaluation of their use should be disseminated widely for consideration across all sectors. However, care needs to be taken with so called pseudonymisation, which can in fact lead to identifying the subject by using it in conjunction with a secondary data set.

- Concern is raised regarding the limited use of algorithmic techniques in sharing data, (particularly aspects of complexity theory, rule induction, neural nets, genetic algorithms and other forms of machine learning) which it is felt should be more widely taught and professionally required.
- Organisations that need to access patient information within the NHS Care Records Service (NHSCRS) and other National Programmes set up Registration Authorities (RA) to manage processes to verifying the identity of health care professionals and workers who wish to register to use these services. Once authorised, individuals are issued an NHSCRS smartcard by an RA. Individual professionals use their NHS CRS smartcard and their smartcard pass code each time they log on. However Universities are not able to become RAs to verify the identities of nursing students who carry out block work-placements in a variety of NHS locations. This requires considerable duplication of effort, particularly if the students go to multiple Trusts for their work experience sessions.
- For example, buying car road fund licenses 'on line and 24/7' are recognized as a huge step forward from visits to a post office. However, this is facilitated by large databases held in linked insurance companies, DVLA, MoT test centres.

Greatest risks

- Data must only be shared for the length of time that it is necessary for the declared purpose, such as treatment or investigation. With medical records, this means that once a clinician is no longer responsible for treating a patient, access to that patient's records should be prevented. There may sometimes be a case for opening access again, for example to prepare evidence for a court, but wherever possible the patient or a relative's consent should be sought first.
- Data aggregation e.g. health data being shared between government departments & outside with (life) insurance companies etc – which becomes more important as genetic data indicating predispositions that may not emerge in addition to actual circumstances etc is included in health record.
- Information sharing of any identifiable data must always have the consent of the data subject, and there is a risk if consent is assumed this without having made every effort to contact the data subject and obtain that consent. Those who may wish to withhold consent must be made aware of the proposed sharing and the mechanism to refuse consent. This must be protected by law.
- The failure routinely to encrypt person-identifiable/sensitive data and to send such data by email, post or courier in an unencrypted form.
- When storage and transmission is insecure, risk applies to both paper records and electronic ones. The paper ones can be accessed and read by anyone with a secondary school education. Properly encrypted

- electronic data, by contrast, can be accessed only by someone with special skills and access rights. The risk is getting the balance between protection and usability wrong.
- Uncontrolled cascading of personal information that cannot be backtracked, does not contain a rigorous audit trail, may deploy inconsistent coding of content and has the facility to become inconsistent.
- Aggregated data 'pre-digested, by researchers, managers, or civil servants' may not produce such a rich analysis as re-analysis of primary data. In certain circumstances consideration of such access may be considered subject to appropriate consent being given.
- There are different issues with non-identifiable information, which can be released for research and budgetary purposes, but care needs to be taken with so called pseudonymisation, which can in fact lead to identifying the subject with a secondary data set to hand.
- Large databases that centralise huge volumes of data may be seen as a way forward to streamline and simplify processes but are at threat from normal risk, e.g. flood, fire etc but also from 'hacking' and, internally, poorly trained or controlled staff. The technological and other controls on access, usage, content, staff training and disaster recovery on large centralized databases which contain personally identifiable data are generally the most resilient but the consequences of failure are greater. The issue is in getting the balance right. Relying almost entirely on technological barriers to misuse is a risk in itself: these should be reinforced by stronger financial and judicial penalties and personal and professional deterrents.

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.

Examples of where public authorities hold too much data

- Where sensitive, particularly health data relates to vulnerable adults, persons under public protection and children at risk. Until secure robust practices around individual privacy are in place and trusted by the public and professionals, skepticism and reluctance to share sensitive data will remain.
- Recent lapses in public sector bodies, including the NHS, have demonstrated systemic problems in information security, which have undermined public and professionals' confidence in the bodies' ability to protect the rights of the individual. It appears that the needs of the organisation are being rated more highly than the "rights" of the individual. These problems have existed for a long time but have only recently caught the public (and media) attention.

- Government actions to collect more and more personal, sensitive data on its subjects appears insatiable, and equally worrying is the attempt to join up different government databases so that all of its employees can gain access to all data.
- It is felt totally unreasonable, and a complete breach (of trust and the DPA Principle 5) for DNA and fingerprints obtained from innocent witnesses and those acquitted of a crime to be retained in order to build up a database of the entire population.
- Concerns, such as those outlined above and a perception of the cavalier attitude of government departments to the importance of the need for security of personal data, may explain public lack of trust in the reasoning behind a national ID card scheme. No citizen should feel they cannot leave the house without an ID card in their possession, or that the ID card has to be produced first before they can open a bank account, register a birth or death, or take out a mortgage.
- Joining up databases with a single identifier, e.g. replacing the national insurance number with the NHS number in the Northern Ireland database makes the loss of such records catastrophic in the hands of extremists, and the greater the number of people having access, the greater the chance of extremist infiltration.

Examples of where public authorities hold not enough personal information

- A northern Local Authority (LA) wants to share its own data about residents with the local Fire Service. This is to promote home safety checks and the availability of free smoke alarms to vulnerable residents. It would appear however that DPA insists on explicit consent from each household for such sharing to take place. This is an example of where data could be used for a beneficial albeit peripheral purpose but isn't.

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.

Examples of where private sector organisations hold too much personal information

- Retail buying patterns, based on data captured from store purchases may result in lifestyle and health deductions that are inappropriate relative to an individual (doing the purchasing rather than personally consuming the product).
- In commercial companies where data is covertly cached when end users believe it to be deleted and where personal information (for example on social networking sites) is easily uploaded but challenging to remove.

Examples of where private sector organisations hold too little personal information

- Data shared between the NHS and private care homes can vary. Sometimes care homes struggle to obtain sufficient care information about residents to adequately care for them. Sometimes they receive information which is not necessary for the service they provide. The NHS for some time has followed the recommendations of the Caldicott Report that encourages limiting data access and sharing to a 'need to know' basis.

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.

Sharing is not taking place as extensively as may be beneficial in:

- Care processes where both health and social care agencies are involved, for example in chronic disease management, for an individual. The concerns raised above (around data quality, audit and transaction monitoring, maintaining the integrity of the shared data and formal permission of authorized/ authenticated professionals with a legitimate need to know) will all need more careful consideration, policy development and deployment in this shared scenario.
- Without question, sharing for child protection purposes should never have any barriers. Often interpreting the Data Protection Act is very difficult, because of the absence of clear guidelines and a tendency to rely on legal precedent. Stakeholders are thus reluctant to do otherwise sensible things for fear of breaching the Act (the Soham murders are a tragic example). Steps must be taken to facilitate but control sharing not prevent it, in order to avoid the Data Protection Act becoming a Data Prevention Act.
- Conditions when increased population mobility and the frequent movement of an individual means that change of access to data about an individual must be rapid, robust and comprehensive. The welfare of an individual may be jeopardized if their health record is not available as and when necessary, especially in emergency and potentially critical situations.
- Situations where the individual holds their own health record and makes it available for explicit purposes to professionals involved in their care management. More consideration is required into :
 - how individuals choose to share and expose their own information held in myHealthSpace, Microsoft HealthVault or more open social networking sites or even on their own home devices

- the duty of the relationship between organisations that host or provide the means of hosting data that individuals are accumulating about themselves (i.e. health records copied to them or downloaded off myHealthSpace or provided by the individuals themselves from monitoring devices and of course the socio-demographic linked information). 'Facebook-type concerns' about the amount of personal data individuals are exposing might just be a trend showing how individuals are taking custody of their own information and making their own decisions on the utility of exposing it more widely to selected viewers and tools.
- Circumstances where there is a potential for commercial organisations to begin offering methods for people to extract their records from a GP system and load them onto HealthVault or myHealthSpace. Policies and procedures must be in place to ensure that this type of data sharing is robust and secure.
- Situations where a new breed of (commercial) organisations will be suggesting to consumers/patients that they create their own longitudinal 'life' record and that they then expose it in a controlled way to chosen tools/providers. The agent for sharing will be the individual directly. Exploration is required regarding how to provide the right standards and advice to allow individuals to make informed decisions about what they share and the risk/benefit trade-off involved. As sharing increases then the better the predictive power of the analytical tools that run on top of that information may become; but the risk escalates if such solutions are not moderated / regulated / managed effectively.

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.

- Managers and clinicians may not be aware of the power of data to answer many of the questions which they need to pose, and may not have appropriate competencies in appropriate statistical or mathematical training to carry out potential additional analysis. Additional training within traditional curriculums or additional courses may be indicated.
- Sharing of an individual's personally identifiable data requires trust and demonstrably robust procedures which are not perceived to be in place currently. This trust must be re-gained by significant investment in risk assessment and reduction strategy implementation, extensive system testing, transparent communication with interested parties (including the

- public at large) whereby truthful responsiveness to external questions are gained.
- Patients sometimes believe that an out of hours service or an A and E department can just switch on access and refer to their primary care GP record. This does not currently happen, except in one or two pilot sites, because historically there have been differences in clinical coding structures. There would indeed be benefits such cross-referrals, but with the caveat that the patient must give permission on each occasion, as happens in Scotland. To make this process work robustly there is no need to continually extract data onto one huge (centralized) database with all the associated risks. Technology is now perfectly capable of ensuring that different systems interoperate with each other on a just-in-time basis. Using a 'portal' model it may be possible to gather the information needed, at the time it is needed, and drop the connections when the patient contact is over.
 - Public trust in the security of shareable systems is being destroyed, for example : by media-portrayed suggestions that medical information on the 'Spine' (centralized database) can be given without audit to the Security Services, leaving no trace; Government data sharing projects are awarded to consultancy firms with little or no prior knowledge of the culture of the UK health service; and apparent watering down of the current DPA in order to give in to the Governments demands for ever more personal and private data on its citizens.

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.

- In principle, our concerns cover where personal information is being shared :
 - Between organisations for purposes that were not explicitly agreed by the subject of that data, for example where data are shared with the police or tax authorities with the specific aim of identifying an individual.
 - Where data is not only being used for the purpose for which it was collected, or for which sharing was agreed
 - Where shared data is being misused
 - The sharing process puts the information quality in jeopardy; for example, mis-interpretation of common codes
 - Sharing processes are not being operated appropriately and consistently, by recognized (accredited) professionals
- Some Primary Care Trusts (PCT) are of the opinion that they have a right to access any patient-identifiable data they wish, and send their employees round to GP practices to extract it. This is completely against

- NHS Caldicott Guidelines, and has resulted in the trust which used to exist between practices and PCTs has now broken down.
- The Department of Health, for the National Programme for IT, is putting great pressure on practices and PCTs to make identifiable patient data on the entire population of England available on one vast (centralized) data base 'the Spine'. This will contain medication, allergies and adverse reactions to start with, with patients only written to once to ask if they wish to opt out. The details of all children under 16 will be up there anyway, regardless of the parents' wishes or their status as vulnerable, under witness protection or of celebrity status. It is possible that from within two million employees in the health service, anyone with a smartcard can gain access to any demographic data on the spine that they wish, and then merely put in the audit trail that they accessed the wrong record 'by mistake'. Medications can sometimes be enough to identify a patient. The 'sealed envelope' to protect data that it is the patient's wish to keep secret is promising but has not been developed yet; the first summary care record pilot sites have gone ahead without it. Postal invitations in England to take up an 'opt-out' status were found to have not been delivered in many cases.
- Opportunities exist for NHS patient data to be used within clinician's own domains for investigations about certain conditions or treatments that could be considered 'research', and about which the patients are quite unaware. Even legitimate transfers of patient data to national recognised initiatives, such as the Cancer Registry, often do not adequately inform patients or offer any form of choice or opt out. The NHS Patient Information Advisory Group (PIAG) was intended to be an interim proxy measure but movements to capture explicit consents appear to be extremely slow in coming.

Section 3: The legal framework

Question 9: In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

- The DPA is clear, concise, widely accepted and has broadly 'stood the test of time'. The main strength of the Act is that it exists and has done so since 1984. In that time discussion, debate and consultation have all contributed to raise awareness that organisations and the government simply cannot do what they like with personal data. In the 21st century that must be a good thing. The weakness is in interpretation and application.
- The Information Commission does not have enough staff to effectively 'police' the requirements of the Act; appearing to rely on deterrent

- operations and the impact on others from high profile cases put under scrutiny.
- The DPA as it is written, does what it says, it provides a directive to protect personal data. It would work better if each government employee had to undertake training in its meaning before being allowed to work on any personal data.
- Any dilution of the conditions, such as allowing data to be processed for a purpose for which it wasn't collected, or keeping data for longer than was necessary for the original collection purpose would break the meaning and intention of the Act.
- The processes for responses by organisations to requests under the DPA can be protracted and used to obfuscate legitimate questions.
- Often NHS data protection officers at the 'sharp end' have difficulties in providing clear advice to local staff because of the lack of clarity available interpreting what the Act says. Greater clarity around schedules 2 and 3 would be useful along with more guidance with regards to sharing; in a similar manner to that available within 'Every Child Matters'.

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.

- Organisations rarely carry out a rigorous and replicable process to undertake the “specification” of “purposes”, resulting in ‘analysis by stealth’ in some cases; for example ‘data no longer being used for the purpose it was collected’ must be terminally destroyed, not used to populate vast, unconsented databases as may (anecdotally) be happening.
- The wording (of the second principle), if adhered to, would offer the correct amount of protection. In a health context if you obtain consented data to treat a patient, you are not then entitled to share that patient's records with Public Health, the PCT, Social Services, or any other body, without going back to the patient for further consent. The problem is that this clause is not being followed as it should, and there is room for better training in what it means, and better policing of the principle to ensure it is followed.
- Within health, the biggest threat to Principle 2 is the inappropriate use of patient data for research. A compelling argument that such use is for the 'greater good' abounds and often clinicians do not recognise the emerging 'patients rights' argument; perhaps this is a legacy of 'paternalism' within the health domain. The confusion between purposes of 'audit' and 'research', and how implied consent works for one under 'provision of healthcare' and not the other requires resolution.

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

Technical

- Technically it is largely possible to protect data in individual databases, with interoperability functionality to share when necessary and only when required for the benefit of the data subject or the original purpose. Government needs revisit the pressure it exerts on organisations to collect and process more and more personal data without consent, just because it would make the life of the security services easier.
- Technology appears to break down when attempts are made to scale up the solution, and to start promising security that cannot be delivered, such as sealed envelopes (currently a concept not a tried and tested deliverable product). The issue of hundreds of thousands of smartcards has already led to the reported loss of thousands of these; without stringent monitoring of every smartcard issued, and its withdrawal (or not) when people leave; the system continues to jeopardize the effectiveness of the DPA.

Institutional

- DPA principle 5 is that data should only be held as long as necessary for the purpose for which it is collected. In practice, data collected and held on computer is rarely deleted when no longer needed for its original purpose. In practice, with clinical records, this can mean that once a clinician is no longer responsible for treating a patient, access to that patient's records by that clinician should be prevented. There may sometimes be a case for opening access again, for example to prepare evidence for a court, but wherever possible the patient or relative's consent should be sought first.
- When a very well known media personality was critically injured and rushed into intensive care at an NHS hospital, over 500 members of staff accessed his record, many out of curiosity. The institution's practices were able to determine that only a small number actually had any legitimate reason so to do, and rapidly put disciplinary and re-education processes in place to minimize future similar incidents.

Societal

- The future of the NHS is linked to the development of the National Programme for Information Technology (NPfIT). In summary, this is the upgrade and linking together of IT systems that will facilitate greater access and sharing of patient identifiable information. The intention is to improve the delivery of care to patients, however, the DPA may find its own intent at odds with this 'brave new world'. Institutions may continue to

- 'hide behind' the DPA when reluctant to share information. The general public may withdraw consent if is fearful of large government databases planning to share data seemingly without control.

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

- Sufficient resources to maintain and explain judgments and responses to requests for information under the DPA within a reasonable time frame, and at an acceptable level of detail.
- Currently there is no real process for redress for those whose right to privacy has been breached, or sufficient deterrent or sanction to government departments to seek to collect data without consent. Stiffer penalties for breaches, loss of data subjects' personal information, and any proposed government legislation to gain greater access to be subject to the constraints of the DPA as non-negotiable.
- The powers of the Commissioner to prosecute, fine and imprison should be reviewed and increased to respond to recent high profile incidents.
- Equally, the ICO should be developed so it can provide staff to visit organisations to provide guidance, audit and support to promote greater local understanding and compliance.

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.

- Article 7e weakens the DPA, giving an override to the rights of the individual to give consent first to any data collection or processing. 'In the public interest or in the exercise of official authority' is too wide ranging, and exactly the sort of terminology which gives rise to the fears about the current legislation.
- Clause 8:3 of the DPA which states '*Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.*' could be taken to mean that anyone working in the NHS could process data claiming they were 'involved in the management of healthcare services', whilst in principle breaching the DPA.
- Article 25:2 states that '*The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations,*

- *the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country*’ is unclear about who should carry out the assessment. It also says it is acceptable ‘*to protect the vital interests of the subject*’, however, in practice a GP practice transferring confidential patient letters for transcribing to India is in no position to carry out any assessment of the security operations in India.
- Sometimes local IG staff who also administer Freedom of Information requests struggle to reconcile the links and relationship between DPA and FOI. Once more greater guidance would be beneficial.
- The Police and Criminal Evidence Act, 1984 (PACE) can abreact with the principles of keeping track of legitimate access to person-identifiable records, as it states that it is not allowable to log that a specific record has been viewed by the police in the pursuance of investigating, say, a shotgun incident, even if that patient information has no relevance to the incident being investigated and is subsequently made public.

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.

Between public authorities

- Local authorities should be obligated to develop local structures and processes with the local health community to provide effective mechanisms for communication, protocol development and improved data sharing.

And additionally between public authorities and private organisations

- Use of regularly changed and personally encrypted personal IDs. The problem of implementing such solutions lies in human factors not in the identification itself, but in the transmission of the identification. That is usually most safely done by using multiple routes. For example, some IDs are sent by post, confirmed by return email, and verified by telephone.
- Introducing obligations relating to creating and accessing audit trails on all copying / extracting processes in addition to those existing for enquiry / input / modification / deletion.
- Statutory power should include unannounced inspections – but there would be need for a massive staff to make it a reality. However, with any changes to statutory powers there will be a need for greater

- awareness/education about principles & practices of law etc for all staff, with additional emphasis in work contracts & professional codes of conduct and the like.

Question 15: Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples.

- Responding to DPA (and FOI) requests can often be a time consuming and costly exercise. In the same way, subject access request (SAR) administration whilst clearly well established is a growing burden on health trusts. Effective communication with patients is a 'two-edged sword' and the growth of the 'expert' patient, often courtesy of the Internet, offers the prospect of increasing SARs in the future. In the very long term, within health, the replacement of paper-based records with electronic records only will vastly improve the administration of SARs.
- For all organisations (potentially) holding relevant information, processes to secure access by the subject to all information about a clinical condition or outcome for an individual create a considerable workload, where content may currently be fragmented and distributed over many sources in both paper and electronic form. This currently may currently require many requests to be made to many organisations.

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.

- NHS protocols exist for both primary and secondary care organisations, and specialist registers, such as of cancer patients, and occurrences of notifiable diseases. For example – the 'Care records guarantee' is good in principle but has weaknesses. The related 'sealed envelope' technology is, as mentioned above, not yet available and its capability is as yet unclear.
- Academic institutions and the NHS have Ethical Committee regulations to ensure 'research' is only carried out within agreed areas under explicit consent agreements. There is less clarity about access, data management and handling once the research has concluded but data has to be retained for defense or any challenges to resultant publications.
- Section 60 of the Health and Social Care Act 2000 set up the Patient Information Advisory Group (PIAG) to judge whether researchers should be allowed access to identifiable health records without patient consent (or knowledge) when obtaining consent would be unduly onerous, or more

- rarely, when it may cause unusual distress to subjects – or in the case of minors, to their families. In these situations researchers currently forward their research proposal for PIAG to deliberate whether researchers' access to identifiable records without patient consent might be accepted. This process is totally lacking in transparency or respect for the patient's rights with regard to access to their record. It signally fails to acknowledge the role of a patient as a partner in research

Please provide details of any initiative you have been involved in that has been based on consent. Collected examples from BCSHIF members follow.

- From experiences in NHS NPfIT initiatives to date, issues of consent to share data with the summary care record are complex, such as :
 - Assuming no opt out is invoked if there is no response to letters is not facing up to the responsibility to ensure all patients in practice have really consented for their data to be shared.
 - The identification of roles for role based access is fraught with difficulty and has not yet been resolved. For example, receptionists working on GP practice reception desks have to share terminals, and there is no way that they could log in and out for each transaction, so they end up using terminals with other staff's smartcards in. The same problem will arise in pharmacies when e-prescriptions service rolls out (and already has in hospital A&E Units). Instant fingerprint identification might get round this, but it will always be down to the staff to follow procedure, and human behaviour will often take the easiest, if not the most secure, route.
- Within a health environment the requirement for a schedule 3 condition (regarding: processing of sensitive data) is often easily satisfied. However, there is a legacy of reliance on implied consent and it is not clear when and in what form consent should be sought within health. The situation is further complicated when linked to social care because of what appears to be fundamentally different approaches; for example the previous Fire Service example given in response to question 5.

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

- Situations where emergency care is required. Clinical decision making may require to be based on clinical history, if not accessible the outcome may be life-threatening.

Any perceived 'barriers' are there for the protection of the individual.

- Section 60 of the Health and Social Care Act states that it is not necessary to obtain consent if it would not be practicable to do so. What is 'practicable' is debatable, and has been misused. For example it was judged that the names, addresses, DOB, NHS number and medical conditions of persons with diabetic conditions could all be extracted from GP records without the patient's consent, (for retinal screening purposes) because it was not deemed 'practicable'. In fact, contacting the patients to ask for consent could easily have been achieved by a mail merge letter from GP clinical systems. In fact, some practices were so upset by the proposal to go ahead without consent that they contacted their diabetic patients anyway, at the practice's own expense.
- It would depend on the nature of the sharing and, most importantly, the nature of the data subject. If the data subject is being visited, treated or counselled anyway then an opportunity exists to offer explanations and seek consent. Seeking consent via 'mail shot' may in some circumstances be less successful, for example: to those with no fixed abode, newly moved home or with reading-related or other difficulties in interpreting such a request.

Question 18: Do you have any suggestions on how to make the sharing of information more transparent?

- In general, individuals should be able to access data held about them, in part merely to ensure that that data is accurate. There may be exceptions on grounds of national security, but each exception should be argued before a specialist body.
- In the light of current concerns with data security, exploration of the implications, risks and opportunities arising from patient-held clinical records should be funded and the findings immediately considered as a potential way to demonstrate explicit consent to use of the contents.
- Explore the feasibility of making it possible to make blanket requests under the DPA relating to 'all data held by public sector bodies relating to a named individual', including the established linkages and access routes for each public sector organisation.

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?

- Individuals should certainly have a right to know what is being held about them, and who this is being shared with. A portal website listing all organisations having the right of access to listed sensitive information should be widely publicised and kept up to date. That website should also give details on how to check this data, how to correct errors, and how the subject of that data could remove data if this is desired. Obviously there will be exceptions such as child abuse

- registers; but even there, the parents should have a right to know exactly what information has been collected on them, from whom, and the right of a response to this. Currently the whole process is clothed in secrecy, causing needless anxiety and speculation.
- There are clear and important exceptions to the parents' rights to know information, which could potentially put the child in danger and/or ruin the collection of evidence in some police investigations, such as in the case of rings of abusers.
- Greater communication with the public should take place so they better understand what is happening routinely with their data. Greater use should have to be made of organisational websites to inform the public about their data. The ICO should have a more high level profile to encourage the public to ask questions of organisations that hold their data. It is suggested that a DPA version of an FOI publication scheme should exist to structure what organisations need to be telling the public.

Question 19

How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?

- As this consultation is the first time it has been drawn to the attention of many BCSHIF members, publicity must have been limited. Early comments indicate that it seems to make a good stab at providing advice on sharing, but is a bit too general. For example just what does 'actively communicate' really mean when talking about consent? No real guidance has yet been identified on when information can be shared for research or public health policies, and when it should necessarily be anonymised.
- The recently produced materials are sensible – especially the guidance to small businesses. However, more examples in natural language not jargon would emphasise the meaning.
- The documentation referred to was difficult to track down, and the instructions on how to implement it were not easy to understand.
- General guidance, whilst useful, remains general and is often of limited value when organisations are dealing with specific intentions to share. The ICO should offer a bespoke service whereby organisations (or sectoral representatives) could obtain advice regarding specific intentions to share with 'templates' developed that could be 'tweaked' to suit the unique aspects of the proposal.

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.

- Recent technological advances have made it possible to store and analyse much greater amounts of data than it was previously possible so to do. The Web 2.0 movement is also leading to an emergence of changed attitudes towards data sharing, where many people are happy to openly share a lot more information about themselves with a wide range of people, many of whom they may not know. There are obvious dangers in this if people are unaware of the risks involved (e.g. identity theft). The development of identity management systems (e.g. Open ID) will have an impact on access to data and so on sharing, but it may be too early to say exactly what the impacts will be.
- Technology has enabled the collection and storage of vast amounts of data in one place, rather than individually held paper files which can only be read by one person at a time. Any number of people, with the right access, can access any number of files simultaneously. Whilst this can benefit the data subject by not having to continually ask them for the same data on a care pathway, it has increased the risk of improper access and data leaks. The ability to load the data of millions onto one CD means that the leak can be catastrophic if that data is lost, and worse, gets into the wrong hands.
- There needs to be information governance training drummed into every employee who has access to sensitive or personal data, and risk assessments performed on every data transfer procedure to ensure safe transit and only appropriate access. There should not be vast data storage put in place before the ability to protect the most sensitive items has been developed (see lack of 'sealed envelopes' mentioned above).
- With many users feeding the same data store, the manner in which ownership of each entry has still not been settled, and this constitutes a risk to patient safety which needs to be addressed.
- As stated, NPfIT within the NHS will radically change the availability of personally identifiable sensitive patient data, albeit with controlled access. The adoption of the use of smartcards to an e-gif level 3 standard reflects what is now to be expected of organisations which are embracing technology. In this world greater access will be available but more tightly controlled for those who need it. Role based access and the concept of 'legitimate relationships' are further electronic solutions to be adopted by the national programmes to ensure that control exists within systems.

Question 21: Should the law mandate specific technical safeguards for protecting personal information?

- The law should mandate that there be protection, but the technical details should be determined by specialists, not by lawyers or politicians.
- There should be an explicit requirement that all personal information held on portable devices be encrypted to a standard – but the designated standard will change over time and should be delegated to specialists to

- determine. Technologies are going to change too fast for them to be cast in the stone of legislation.
- Issues relating to 'portable devices' should also be extended to on-line data storage facilities – but it is recognized that complexity increases when many of such facilities are located in other countries.
 - The knee jerk reaction of 'let's encrypt everything' requires more detailed analysis of what the relevant procedures and data transfer paths are. For example, GPs transfer their medical records on CDs tucked into the paper envelopes with the residual historical paper record. The transfer path is by secure NHS courier. If the paper path is secure, then the CD doesn't need to be encrypted, and indeed it would not be practicable to do so. The sending practice doesn't know the 'demographic configuration' of the receiving practice, because patient notes are shared through a secure forwarding service process. It is therefore not possible to send an encryption key. If paper is secure, then the CD is also. Transferring all records electronically is being implemented on a phased basis but there is still the requirement to either print out or make available on CD the record being transferred even if the record has been sent electronically. This dual process is likely to continue for the next couple of years, demonstrating that the whole GP patient registration process depends on physical transfer of records.
 - Laptops and Personal Data Assistants containing personal data must have a high level of encryption, as must any networks used for transfer. There is also the need for improved training, currently Government (public sector) staff and contractors do not seem to recognize their accountability and responsibility to do everything they can to protect individuals' data.
 - A law to mandate statutory standards of security would be very difficult to keep pace with technological change. However :
 - Industry standards and recommendations should be commonplace, de facto standards, embedded in organisational policy.
 - Controls assurance mechanisms should focus more on outcomes and less on process
 - It must be recognized that existence of policies (a common assurance litmus test) is not the same as compliance. The NHS provides a good example, in that for some time, NHS bodies have been required to complete an "Information Governance Toolkit". Following the data losses at HMRC, a new set of Department of Health emergency information demands was mandated, a primary purpose of which seemed to be establishing unequivocal local chief executive responsibility for any and all failures.

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 is appropriate if genuinely carried out but, for example, a rare clinical condition and the first half of a postcode might be enough to identify a patient. Medical research should use only use anonymised data. If actual patient details are truly needed, then there is no alternative, the patient must give informed consent or be given the right to refuse to take part.
- The Department of Health Patient Information Advisory Group (PIAG) is responsible for deciding which data sets can be extracted under Section 60 exemption, but their impartiality can be questioned since there are no actual patient representatives on the Group.
- Pseudonymisation is not true protection of data, and enables someone wanting to identify a patient to do so relatively easily with the possession of a second data set. It should only be used as a compromise if an element of identification is essential, and it is not practicable to gain consent from the patient.

Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

- There is little awareness of detailed advice on how to truly anonymise data, what pseudonymisation means, and when they should be used. This guidance should be made more readily publicly available.
- Barriers to using anonymising and pseudonymising techniques may result in pressure from bodies such as the Faculty of Public Health, who assert that they have a right to any person identifiable data they are interested in, and put pressure on lower employees to collect and give them this data.
- The NHS has clearly embraced technology within NPfIT, has recognised the need to include privacy enhancing technologies (PETs), the deployment of such functionality, if done properly, would improve information security. Such techniques remove the user responsibility, and reduce the staff angst over what they could do compared with what they should do.

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.

No response

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?

- Giving patients access to their own records, to share with clinicians treating them in other parts of the country is being piloted in the United States, and is beginning to be available here. Handing control to the patient, with the records stored locally but linked for necessary details, is widely considered a much safer way of dealing with emergency need for access to records, and is always up to date.

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?

- The permissive approach to sharing personal information has been of particular danger in countries such as Russia, and early to mid-20th century Germany, where the individuals' rights have generally been curtailed, and a surveillance state is the norm. The USA is now following this path with the compulsory gathering of fingerprints and the like, and demands for personal demographic and financial bank details from European residents wishing to enter the USA. This causes mistrust of the state and creates a 'them and us' culture.

Question 26: Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

No response

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?

- Linkage techniques related to complexity theory and their contribution to robust data sharing should be researched further and the findings disseminated widely, in order to more fully understand and identify ways to minimize the risks from data sharing processes.

- Efforts should be made to address the fact that so many, particularly politicians and journalists, still believe in the efficacy of unaided human judgment. Decisions should be made on the basis of the most appropriate and comprehensive material that the decision maker has authorization to use; those not using such opportunities should be classed as negligent and the public should see them as such.

Do any of these issues apply specifically to your sector?

- Clinical education should include training in how to evaluate risks and opportunities stemming from making decisions, with or without reference to an evidence base or based solely on personal knowledge.
- Healthcare computing is a very sensitive subject, and grave concerns exist that some of the implications of (centralized) enterprise-wide systems and (collective) summary care records have not been appropriately considered, or discussed with the public at large, who also have not been made aware of developments, options or issues.

Question 28: Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

- Some contributors felt that the whole NHS NPfIT programme needed to be examined more thoroughly than it has been from the point of view of security and protection of the data relating to individuals and controlled access thereto.

End – response from BCS HI Forum.