INFORMATION
to share or
not to share

The Information Governance Review

Information: To share or not to share?

The Information Governance Review

March 2013

Contents

Chairman's foreword

Every citizen should feel confident that information about their health is securely safeguarded and shared appropriately when that is in their interest. Everyone working in the health and social care system should see information governance as part of their responsibility.

Unfortunately that is not currently the case, as the Future Forum so clearly described in its report in January 2012. This strongly recommended to Government that a review of information governance should be commissioned, to include the current rules and their application. The Secretary of State for Health in England accepted the recommendation and asked me to conduct such a review independently.

I had gained some familiarity with the issues when I chaired a Review in 1996—97 on the use of patient-identifiable data. We recommended six principles for the protection of people's confidentiality, which became known as the 'Caldicott principles'. They included a recommendation that organisations should appoint someone to take responsibility for ensuring the appropriate security of confidential information. The people undertaking these responsibilities became known as 'Caldicott Guardians'.

My association with the subject developed in June 2011 when I became chairman of the National Information Governance Board during the final period of its existence before disestablishment in March 2013. There I heard first hand about concerns relating to information governance that arose during the passage through Parliament of the Health and Social Care Bill.

The opportunity to undertake a further useful piece of work, affecting the delivery of the best care possible to our population and reassuring citizens that their information is in safe hands, was for me irresistible.

In accepting the invitation, and having learned in 1996—97 how best to approach such a task to achieve a useful outcome, I decided to ask key organisations to suggest suitable individuals who would constitute a small panel of relatively expert members, individually independent too.

Our overarching aim has been to ensure that there is an appropriate balance between the protection of the patient or user's information, and the use and sharing of such information to improve care.

I hope that the reader of this report will think that we have achieved some success to that end.

It has been gratifying to learn, in the course of the Review, that the Caldicott principles continue to be valuable, but would benefit from minor amendments. The original report was written in 1997 when the service was more paternalistic and much less patient centred. Now citizens are a lot more concerned about what happens to their information; who has access to it, for what purposes is it used, and why isn't it shared more frequently when common sense tells them that it should be.

The Future Forum's key recommendation relating to information governance stated that data sharing is vital for patient safety, quality and integrated care. We endorse this wholeheartedly and have been struck by the loss of confidence of many clinicians with whom we spoke, about when it is safe to share information and the safeguards that are required for sharing.

It won't come as a surprise that, writing within a few weeks of the publication of the second Francis report on Mid Staffordshire NHS Foundation Trust, we were struck by the need for cultural change in the NHS. A re-balancing of sharing and protecting information is urgently needed in the patients' and service users' interests, which is supported by those citizens with whom we discussed these issues.

There is clearly an urgent and ongoing need for education and training in this area for staff, and also for patients and service users. Given the imperative to meet the needs of an ageing population, particularly at the boundary between health and social care, it is crucial that systems for principled sharing of information are well understood. As the Health and Social Care Act 2012 takes effect public health, within its new managerial structure, must also be involved.

There is imbalance in other parts of the system too. While the research community has protested in the past at perceived impediments to their endeavours deriving from information governance, they have worked hard to resolve these. Patients are generally keen to contribute to research but do want their consent obtained appropriately.

The new commissioning arrangements have highlighted concerns about identifiable information being sought excessively and used inappropriately.

In all these situations the Panel has attempted to clarify, simplify where possible, and remind the reader of the law and the rules pertaining to confidential information and its uses.

It has been a privilege to work with members of the Panel and the officers supporting our work. We all hope that this report will prove useful and the Secretary of State for Health will ensure that it is considered carefully, that our recommendations are implemented and monitored for the wellbeing of the population, and for the benefits in care that will be derived from research, appropriate commissioning of services, and policies in relation to the public's health.

While we were asked to consider the issues in England, there is much in our report which should prove useful in all the jurisdictions of the United Kingdom.

Fiona Caldicott
March 2013

Executive summary

Chapter 1: Introduction

People using health and social care services are entitled to expect that their personal information will remain confidential. They must feel able to discuss sensitive matters with a doctor, nurse or social worker without fear that the information may be improperly disclosed. These services cannot work effectively without trust and trust depends on confidentiality.

However, people also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service. So good sharing of information, when sharing is appropriate, is as important as maintaining confidentiality. All organisations providing health or social care services must succeed in both respects if they are not to fail the people that they exist to serve.

The term used to describe how organisations and individuals manage the way information is handled within the health and social care system in England is 'information governance'. In 1997 the *Review of the Uses of Patient-Identifiable Information*, chaired by Dame Fiona Caldicott, devised six general principles of information governance that could be used by all NHS organisations with access to patient information. The chapter sets out those principles, which have stood the test of time. It explains why the 1997 review gave priority to discouraging the uploading of personal information on to information technology systems outside clinical control. The issue of whether professionals shared information effectively and safely was not regarded as a problem at the time.

NHS organisations responded by appointing 'Caldicott Guardians' to ensure that information governance was effective. The practice spread to other public bodies, including local authorities and social care services, and the remit of the guardians was extended to provide oversight of information sharing among clinicians.

Over recent years, there has been a growing perception that information governance was being cited as an impediment to sharing information, even when sharing would have been in the patient's best interests. In January 2012 the *NHS Future Forum* work stream on information identified this as an issue and recommended a review *"to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care"*. The Government accepted this recommendation and asked Dame Fiona to lead the work, which became known as the Caldicott2 review.

The introduction sets out how the review has been conducted and puts it in the context of the Government's Information Strategy, the Health and Social Care Act 2012, the Open Data White Paper, the review of the NHS Constitution and other relevant initiatives.

Chapter 2: People's right to access information about themselves

The Review Panel heard evidence that people's lack of access to their own records causes great frustration. We were told that patients who attempt to become involved in decisions about their care are often thwarted by 'information governance rules' that ignore their express wishes. Examples included patients being charged a fee for access and patients being denied the opportunity to receive information in a form that suits them, such as by email, or in an audio format that can be accessed by blind people.

Problems mainly originated from local information governance policies, which vary between organisations. The chapter gives examples of good practice. It recommends that all communications between different health and social care teams should be copied to the patient or service user. There should be 'no surprises' for the patient about who has had access.

Chapter 2 notes that the *The Power of Information*, the Department of Health's Information Strategy, said people's access to their care records should be improved, with individuals gaining electronic access to their own care records where they request it, starting with GP records by 2015 and social care records as soon as IT systems allow.

The Review Panel thinks this right of access should cover hospital records, community records and personal confidential data held by all organisations within the health and social care system. It believes that access should become available within the next decade. This will not automatically happen unless there is a clear plan for implementation.

The chapter further recommends that an audit trail of everyone who has accessed a patient's personal confidential data should be made available in a suitable form to patients via their health and social care records.

Chapter 3: Direct care of individuals

When it comes to sharing information, a culture of anxiety permeates the health and social care sector. Managers, who are fearful that their organisations may be fined for breaching data protection laws, are inclined to set unduly restrictive rules for information governance. Front-line professionals, who are fearful of breaking those rules, do not co-operate with each other as much as they would like by sharing information in the interests of patients and service users. There is also a lack of trust between the NHS and local authorities and between public and private providers due to perceived and actual differences in information governance practice. This state of affairs is profoundly unsatisfactory and needs to change.

The Review Panel found a strong consensus of support among professionals and the public that safe and appropriate sharing in the interests of the individual's direct care should be the rule, not the exception.

Direct care is provided by health and social care staff working in 'care teams', which may include doctors, nurses and a wide range of staff on regulated professional registers, including social workers. Relevant information should be shared with them, when they have a legitimate relationship with the patient or service user.

Care teams may also contain members of staff, who are not registered with a regulatory authority, but who may need access to a proportion of someone's personal data to provide care safely. Conditions and safeguards are discussed.

The chapter considers the principles underpinning a professional's right to receive personal confidential information about a patient and share it with other professionals to optimise the patient's direct care. It finds the system works for the most part on the principle of 'implied consent'. Examples of the use of implied consent include doctors and nurses sharing personal, confidential data during medical and nursing handovers without having to ask for the patient's explicit consent. A fuller discussion of the law of consent is provided in chapter 5.

Chapter 3 goes on to discuss the sharing of information with care homes, carers, friends and family. It suggests that organisations should pay closer attention to the appropriate transfer of information when people move across institutional boundaries, such as leaving hospital, coming out of the army or prison, or changing their GP.

The Review Panel looked at the problem confronting staff who have to distinguish between an individual such as a relative legitimately seeking information about a patient's progress and a 'blagger'; a person making improper inquiries. It recommends protocols to assist in good decision making and procedures for informing and helping people if mistakes are made.

This chapter also explains how the use of personal confidential data for clinical audit can be managed within the law. It discusses arrangements for sharing information with geneticists to facilitate the direct care of patients with genetic problems.

Chapter 4: Personal data breaches

In the 12 months to the end of June 2012, 186 serious data breaches were notified to the Department of Health. Most involved the loss or theft of data, but almost one-third concerned unauthorised disclosures.

Many of the breaches were reported through strategic health authorities and not through the Information Commissioner's Office (ICO), which has the power to impose financial penalties of up to £500,000. When strategic health authorities go out of existence, there will be a need for a new, consistent reporting channel to ensure that breaches of patients' confidentiality do not escape the attention of senior managers, ministers and regulators of health and social care.

The ICO told the Review Panel that no civil monetary penalties have been served for a breach of the Data Protection Act due to formal data sharing between data controllers in any organisation for any purpose. It says breaches of the Data Protection Act are usually the result of lack of due consideration. Yet it finds that organisations frequently shy away from data sharing and cite data protection as a reason. The data sharing code produced by the ICO in May 2011 helps organisations to share data in a secure and proper way. They should use it.

There should be a standard severity scale for breaches agreed across the whole of the health and social care system. The board or equivalent body of every organisation in the health and social care system should publish all such data breaches, as part of the quality report in NHS organisations or as part of the annual report or performance report in non-NHS organisations.

The chapter also considers the implication for data security of people's increasing use of social media. This has not changed any principles of confidentiality. However, there may be a need for greater vigilance among health and social care professionals as they switch from the personal side of their lives to the professional side.

Chapter 5: Information governance and the law

Every minute of every day, staff employed across health and social care services make lawful use of personal confidential data about patients and service users. For the most part, they do so on the legal basis of consent. They may have asked for the individual's explicit consent for a particular treatment or course of action. Or they may rely on implied consent. For example, when a patient agrees to the GP referring her to a hospital consultant, she can expect the GP to pass on details of the medical condition that requires the consultant's attention. The GP may legally assume she has given implied consent to the sharing of this information without having to ask her.

These assumptions should only be made if it is reasonable to expect the patient understands how the information will be used. The Review Panel did not consider it necessary to challenge this long-established approach, although we think further effort is needed to increase patients' understanding of how their personal confidential data is used.

Chapter 5 sets out the four legal bases that may provide an organisation with a justification for holding and using personal confidential data. It recommends that the use of data without a legal basis, when one is required, should be reported and dealt with as a data breach. Chapter 5 also makes a recommendation urging all organisations in the health and social care system to explain to patients and the public how the personal information they collect could be used in de-identified form for research and other purposes. Such explanations should mention what rights the individual may have to refuse to give their consent.

When people give, refuse or withdraw explicit consent, these decisions should be traceable and communicated to others involved in the individual's direct care. Patients can change their consent at any time.

New rights and pledges were set out in the Government's consultation on revisions to the NHS Constitution. The Review Panel proposes that these rights and pledges should be extended to cover the whole health and social care system. Our proposal is set out below:

- **You have the right** of access to your own personal records within the health and social care system.
- **You have the right** to privacy and confidentiality and to expect the health and social care system to keep your confidential information safe and secure.
- **You have the right** to be informed about how your information is used.
- **You have the right** to request that your confidential data is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

The NHS and adult social services also commit:

- to ensure those involved in your care and treatment have access to your health and social care data so they can care for you safely and effectively (pledge);
- to anonymise the data collected during the course of your care and treatment and use it to support research and improve care for others (pledge);
- where identifiable data has to be used, to give you the chance to object wherever possible (pledge);
- to inform you of research studies in which you may be eligible to participate (pledge); and
- to share with you any correspondence sent between staff about your care (pledge).

This section also sets out the duties of staff to protect the confidentiality of personal information and to provide access to a patient's data to other relevant professionals, always doing so securely.

Chapter 6: Research

The existence of the NHS gives a big advantage to medical researchers in Britain. As a universal service free at the point of use, the NHS has a deep well of data covering almost all of the population, across the full spectrum of medical conditions. There is also enormous untapped potential in the information captured in social care records to support better research.

The Review Panel examined how these opportunities might be realised without weakening confidentiality and trust. Researchers told us of their concern about the complexity, confusion and lack of consistency in the interpretation of the requirements they have to satisfy before research projects can proceed. However, we found there can be robust solutions to these problems that permit access to detailed patient information without compromising the confidentiality of individuals.

If data clearly identifies individuals, it must not be processed without a clear legal basis. If data is anonymised in line with the ICO's anonymisation code, it can be freely processed and publicly disclosed. However, there is a third class of data, which is of great interest to researchers, that on its own does not identify individuals, but could do so if it were to be linked to other information. This 'grey area' includes data that has been de-identified by the use of pseudonyms or coded references, but could be re-identified when combined with other data.

The Review Panel looked at solutions that allow such linkages to take place for the benefit of science without putting individuals' confidentiality at risk.

We recommend that the linkage of de-identified but still potentially identifiable information from more than one organisation should be done in specialist, well-governed, independently scrutinised environments known as 'accredited safe havens'. Chapter 6 proposes national minimum standards for safe havens, supported by a system of external independent audit and other requirements to give the public confidence.

The Health and Social Care Act 2012 provides for the Information Centre for Health and Social Care (the Information Centre) to become a safe haven. Chapter 6 considers whether it will have capacity to deal with the amount of data linkage that will be needed in the new health and social care system, or whether other safe havens should be established.

The chapter also looks at how researchers can set about identifying people with particular characteristics to invite them to take part in clinical trials.

Chapter 7: Commissioning

Commissioners cannot organise the improvement of services unless they know quite a lot about the people using them. For example, they may want to build new care pathways that are better suited to people's needs. However, knowing about service users need not necessarily require commissioners to know their identities. The arrangements for NHS and local authority commissioners to extract information were in a state of rapid, comprehensive change during the period of this Review, as the NHS Commissioning Board, clinical commissioning groups, Public Health England and local authorities prepared to take on the responsibilities set out for them in the Health and Social Care Act 2012. The chapter focuses primarily on the challenge facing NHS commissioners, however the Review Panel conclude that commissioners in local authorities and Public Health England must adhere to the same standards, guidance and good practice and be subject to the same penalties for poor practice as the NHS when commissioning services.

The Review Panel found a lack of consensus on the need for identifiable data to be used for commissioning purposes. However, after doing detailed work with primary care trusts, clusters and the NHS Commissioning Board, the Review Panel concluded that all the objectives set for commissioning over the years ahead can be achieved without compromising patients' confidentiality or the public's trust in the health and social care system.

The NHS Commissioning Board suggested that the use of personal confidential data for commissioning purposes would be legitimate because it would form part of a 'consent deal' between the NHS and service users. The Review Panel does not support such a proposition. There is no evidence that the public is more likely to trust commissioners to handle personal confidential data than other groups of professionals who have learned how to work within the existing law.

The Review Panel found that commissioners do not need dispensation from confidentiality, human rights and data protection law since, with little effort, they can operate perfectly well within it. For example, there are situations in which the commissioner will need personal confidential data to help people deal with individual care problems. It might be to help someone who is requesting NHS funding for 'continuing care' after leaving hospital, or an 'individual funding request' for drugs that are not generally available on the NHS in that area. In such cases it is entirely reasonable for the NHS to ask for the patient's explicit consent for NHS staff handling the case to be able to look at the patient's personal confidential data.

In other situations, local commissioners may be able to use safe havens, within which the personal information they want to assess may be anonymised without risk of anyone's sensitive data being disclosed. For example a clinical commissioning group might want to consider individual cases in order to monitor health inequalities, but it can do this using anonymised information.

The Review Panel deliberated with the NHS Commissioning Board and other organisations about a proposal for up to 10 Data Management Information Centres (DMICs) to act as safe havens where confidential private data would be anonymised so that it could safely be made available to local commissioners.

This chapter considers how staff in the DMICs might process data lawfully through integration with the Information Centre to ensure that their activities are sanctioned by statute and to maintain public trust in the security of personal information.

The Review Panel recommends that members of the NHS Commissioning Board, Clinical Commissioning Groups and members and officers in local authorities, should ensure their organisation complies with the legal and statutory framework for information governance, with boards, or equivalent bodies being formally responsible for their organisation's standards and practice on information governance.

Chapter 8: Public health

Healthcare professionals who are responsible for health protection sometimes need to know personal confidential data about specific individuals. For example during an outbreak of an infectious disease, public health staff may need to identify individuals who are at risk.

This side of public health resembles the direct care of patients and service users that was considered in chapter 3. While engaged in this work, healthcare professionals can be considered to have a legitimate relationship with people in the communities they serve. It

would be impractical for them to ask everyone at risk from an infectious disease to give specific consent for staff to provide appropriate information and care. Preventing the spread of infection is in the public interest and therefore the use of personal confidential data for this purpose has been provided with statutory support.

This justification for accessing personal confidential data does not apply to other aspects of public health work. Health improvement programmes can provide value to the community by contributing to longer life expectancy, healthier lifestyles and reduced inequalities in health, but they cannot be considered equivalent to the direct care of patients.

Most health improvement activities in public health do not require personal confidential data about individuals. However, understanding the complex relationships that exist between the environment, personal behaviours and disease requires information that can only be derived by linking data from several different sources. This side of public health resembles research and the Review Panel considers that the rules and procedures that have developed to provide the information governance for research can usefully be applied to public health intelligence.

A third dimension of public health is to assist people planning healthcare services to understand the health needs of the local population. This activity resembles commissioning. Although some patient level detail is needed, patients themselves do not need to be identified.

There is a lack of regulatory coherence across the public health arena. Some registries, including cancer registries, have statutory regulatory powers; others operate on a basis of consent. The Review Panel suggests detailed and consistent remedies.

Chapter 9: Education and training

Across the health and social care system, most staff are required to undertake annual training in information governance. The commitment to training is important and the associated training budget is a welcome enabler. However, the Review Panel discovered that the mandatory training is often a ‘tick-box exercise’. One nurse told us the experience was equivalent to an annual ‘sheep dip’, which staff could go through without thinking.

There needs to be a fundamental cultural shift in the approach to learning about information governance. Health and social care professionals should be educated and not simply trained in effective policies and processes for sharing of information.

They should have formal information governance education focused on their roles, and this should be at both undergraduate and postgraduate level. This education should include a professional component explaining why there may be a duty to share information in the interests of the patient, as well as the legal aspects of the common law of confidentiality, the Data Protection Act and Human Rights Act.

Networks of information governance leads should be strengthened and extended to foster greater mutual learning from experience across the health and social care system. In addition to the standard training and education, Caldicott Guardians need to demonstrate continuous professional development in information governance on an annual basis.

The chapter proposes education and training for non-registered staff and continuous professional development for senior managers to ensure they understand the practical information governance challenges their staff face.

It notes that information governance is often the responsibility of one person within an organisation, who may feel isolated. In many cases, the role is filled by inexperienced or relatively junior staff, or is one role among many that an individual must perform. The Review Panel concluded that information governance specialists should work together to establish a community of practice that could improve knowledge to solve practical challenges, develop trust in the information governance function and remove isolation.

Chapter 10: Children and families

The safeguarding of children is a well-established system, underpinned by legislation, which requires professionals to share information about a child whenever there is cause for concern.

Arrangements for sharing require constant vigilance by the relevant professionals. It has become clear, however, that professionals dealing with children and families encounter particular issues of information governance that are not covered elsewhere in this report. This chapter deals with a series of dilemmas involving children.

It references work done by the Royal College of General Practitioners to address the vexed issue of when automatic parental access to the child's medical record should be turned off and when the child's automatic access should be activated upon their reaching sufficient maturity.

Other dilemmas include the extent to which individual members of a family should have access to the 'family records'. These records have become an important dimension of children's social care following the Munro Review. The question is how to provide information to each individual family member without compromising the confidentiality of other family members.

In order to provide effective care for children, information often needs to be shared beyond the normal boundaries of health and social care services, in particular taking in organisations such as schools. The Review Panel concludes that there would be clear benefits if a single, common approach to sharing information for children and young people could be adopted. The Department of Health should work with the Department for Education to investigate jointly ways to improve the safe sharing of information between health and social care services and schools and other services relevant to children and young people, through the adoption of common standards and procedures for sharing information. The departments should involve external regulators in this work including the Care Quality Commission and Ofsted.

Government policy is increasingly seeking to use information to identify individuals or groups of people, such as families, who may benefit from specific help or early intervention. Generally, the aim of these interventions is to address problems these individuals and groups may be facing before they can escalate, potentially causing harm to themselves, their communities, or wider society. Identifying these people often requires extensive sharing, linkage and analysis of personal confidential data.

The Review Panel concludes that significant lessons regarding data sharing might be learned from public health and research communities. It suggests that the definitions of 'prevention' adopted in the influential study of public health by the Commission on Chronic Illness could be adapted to cover social welfare interventions.

Chapter 11: New and emerging technologies

Increasing numbers of patients are benefiting from new technologies that permit 'virtual consultations' with a clinician, using the telephone, emails or video links. There is also a rapidly expanding range of medical devices that use software or other technologies to record data about a patient when a clinician or other professional is not present. These devices then make the information available to the professional.

The Review Panel found a lack of clarity about a patient's right to access the record of virtual consultations and uncertainty about how long records would be kept. It proposes ground rules for ensuring patients have access to information about themselves. Providers offering virtual consultation services should be able to share, when appropriate, relevant digital information from the patient, with registered and regulated health or social care professionals responsible for the patient's care.

Medical devices permitting the monitoring of a patient's condition from a remote location present challenges, but do not raise new issues of information governance. The personal confidential data gathered through these new processes and technologies must be treated in exactly the same way as any other personal confidential data, and providers of these services must adhere to the existing legislation and best practice.

The NHS Commissioning Board and clinical commissioning groups and local authorities should ensure that services using these new technologies are conforming to best practice with regard to information governance and will do so in the future.

Chapter 12: Data management

There are many good reasons why organisations in health and social care need good quality data. Patients are at risk if clinicians base their decisions on inadequate data. Dangers multiply if there is poor handover of information between care teams or conflicting advice to patients from professionals. The Review Panel welcomes the focus that professional bodies for health and social care are placing on data quality.

The issue is particularly relevant to this review because poor data is so often cited as the reason why people running services want to reach for the files of individuals. To find out the truth, they want information about real people that includes personal confidential data.

The best solution is not to give them dispensation to ignore or circumvent legal requirements. It is to improve data quality standards. If data quality is sound, a pseudonym may be used to link data and thus protect the identity of an individual.

The Review Panel endorses the First National Data Quality Report of the Quality Information Committee of the National Quality Board, which seeks improvements in data quality in the health and social care system.

The chapter summarises some important aspects of the Administrative Data Taskforce report on *improving access for research and policy* published in 2012, with the Review Panel endorsing a number of that report's conclusions. It also examines the sharing of data to safeguard children and adults and special considerations affecting data about 'the unborn'.

The Review Panel calls for consistency in the information governance requirements for providers. It recommends that every health and social care organisation should be required to publish a declaration signed by the board or equivalent body, describing what personal confidential data it discloses and to whom and for what purpose.

The chapter seeks to clarify the legal framework for sharing personal confidential data. The Review Panel concludes that individuals should have the same level of protection under the law whether personal confidential data is shared between health service bodies, or whether the sharing is between a health service body and a non-health service body. The Review Panel also recommends that the Department of Health commission a standard template common across the health and social care system for setting up data sharing agreements, to prevent unnecessary duplication of effort.

The chapter also suggests practical arrangements to secure the safety of records when a provider's contract comes to an end and sets out the protections and safeguards which exist to prevent inappropriate sharing of patient's information with organisations such as insurers.

Chapter 13: System regulation and leadership

From an information governance perspective, there is currently no method of regulating the health and social care system as a whole. The Review Panel saw an opportunity for the Information Commissioner's Office and the Care Quality Commission to work together in ensuring the health and social care system is properly monitored and regulated in this regard. The process should be balanced, proportionate and utilise the existing and proposed duties within the health and social care system in England. This chapter sets out three minimum components.

The Review Panel calls on professional regulators to be involved more often in dealing with cases of poor information sharing that disadvantage patients.

The Information Centre is to become responsible for producing and maintaining a code of practice on collecting, analysing, publishing or disclosing confidential information. It should adopt the standards and good practice guidance contained within the green-boxed sections of this report.

The Informatics Services Commissioning Group (ISCG) is responsible for providing advice on commissioning informatics services across the health and social care system. It is proposed that a sub-group of the ISCG is established to provide specialist expertise, advice and support on information governance. The Review Panel welcomes this proposal.

The health and social care system should adopt an agreed set of terms and definitions for information sharing that everyone, including the public, should be able to use and understand.

Chapter 14: Conclusions and recommendations

In addition to the findings of individual chapters, the Review Panel reaches some overarching conclusions. After consideration of what safeguards exist to protect people's confidential information and what means of redress are available if mistakes are made, the final chapter sets out how redress should be managed by every organisation in the health and social care system in England.

There was widespread support for the original Caldicott principles, which are as relevant and appropriate for the health and social care system today as they were for the NHS in 1997. However, evidence received during the Review persuaded the Panel of the need for some updating, and inclusion of an additional principle. The revised list of Caldicott principles therefore reads:

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality.
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

These principles should underpin information governance across the health and social care services.

The Review Panel also concludes that the Secretary of State and the Department of Health should oversee the implementation of the recommendations of this review, and report on the progress made.

This section finishes by listing the full set of recommendations from the Information Governance Review.

A guide on using this report

This report is best read in sequence, as the principles, conclusions and information governance concepts established in earlier chapters are relevant to later ones.

The recommendations from the Review Panel are embedded within each chapter to provide context. A complete list is also contained in chapter 14, at the end of the report for reference. Within each chapter, the key conclusions that the Review Panel arrived at are highlighted in bold text.

Finally, there are a number of sections of text within green boxes throughout this report. These contain suggested professional standards or good practice for information governance endorsed by the Review Panel.

The guidance in this report is intended to help health and social care professionals and staff in sharing information appropriately in their day-to-day activities. There will however, always be exceptional and difficult circumstances where solutions are not obvious. In these situations, professionals and staff should seek advice from Caldicott Guardians or their professional bodies, and use their judgement to act in the best interests of their patients and clients.

1 Introduction

1.1 Confidentiality and trust

Health and social care services cannot work effectively without trust. Patients and service users need to be able to talk freely to the professionals who care for them. They should feel confident about disclosing the most intimate details of their lives to the doctor, nurse or social worker without fear that the information may be improperly disclosed — whether by malice, poor practice or simple carelessness.

This obligation to prevent information seeping outside the health and social care system should not stop it being shared appropriately within it. People expect the various professionals in the care team to communicate with each other and to share the information that is needed to provide a safe and courteous service.

There is no contradiction between demanding that services are rigorous in safeguarding the confidentiality of personal information and enthusiastic about sharing information among members of staff who need to co-operate to optimise the individual's care. All health and social care organisations must succeed in both respects if they are not to fail the people they exist to serve.

Other types of information sharing are also coming to be recognised as equally important. People need to be able to see their own personal confidential data by gaining access to their files, allowing them to make choices and participate actively in their own care. Additionally, anonymised patient data needs to be shared to enable the health and social care system to plan, develop, innovate, conduct research and be publicly accountable for the services it delivers to the people it serves.

These objectives are straightforward and, for the most part, uncontroversial. However, the practical arrangements for delivering them in health and social care organisations are complex and often unsatisfactory. This report seeks to help all staff in the health and social care system, including honorary staff, to make sound decisions about when to share and when not to share so that the interests of the patient or service user always come first.

1.2 General principles of information governance

The term used to describe how organisations manage the way information is handled within the health and social care system in England is 'information governance'. It covers the requirements and standards that the organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

Information governance applies to the balance between privacy and sharing of personal confidential data and is therefore fundamental to the health and social care system, providing both the necessary safeguards to protect patient information, and an effective framework to guide those working in the health and social care system to decide when to share, or not to share.

Key definitions

People often talk about 'data' and 'information' as if they mean much the same thing. However the terms have a precise meaning and the words are not interchangeable. Readers may understand this report more easily by grasping the distinction from the outset:

- **Data** is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'
- **Information** is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'[1]

This report also uses the phrase '**personal confidential data**' throughout.

This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

1.3 The six principles

In 1997, the *Review of the Uses of Patient-Identifiable Information*, chaired by Dame Fiona Caldicott, devised six general principles for information governance that could be used by all organisations with access to patient information:

1. **Justify the purpose(s)**
   Every proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use patient identifiable information unless it is absolutely necessary**
   Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary patient-identifiable information**
   Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to patient identifiable information should be on a strict need-to-know basis**
   Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

[1] The Information Governance Review has adapted the definitions used by the Cabinet Office and published in the Government's White Paper on Open Data.

5. **Everyone with access to patient identifiable information should be aware of their responsibilities**
   Action should be taken to ensure that those handling patient identifiable information — both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. **Understand and comply with the law**
   Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

An assessment of the 1997 Caldicott principles and their relevance to the modern health and social care system is contained in chapter 14, 'Conclusion and recommendations'.

1.4 Caldicott Guardians

The 1997 report dealt specifically with the non-clinical uses of patient information. At the time, there was widespread concern among NHS doctors that their relationship of trust with patients was being put at risk by managers seeking to upload personal information into information technology systems outside clinical control. Those concerns were allayed as NHS organisations adopted the six principles. In particular, they complied with the sixth principle by appointing 'Caldicott Guardians' to maintain legal and ethical propriety. Over time, the guardians' remit extended to provide oversight of the flows of information among clinicians involved in direct patient care. The information governance workload increased and was usually delegated from board members to managers of varying seniority. Similar arrangements were also established in other public bodies, including social care.

The 1997 report did not consider the issue of whether professionals shared information well, in the interests of patients, because that was not regarded as a problem at the time. Furthermore, its remit did not extend beyond the NHS and so it could not consider information sharing between health and social care organisations and individuals.

That omission became increasingly noticeable as the need for closer integration between health and social care became ever more apparent, creating a need to extend common principles of information governance across the NHS and local government.

1.5 Perceptions of information governance

Over recent years, there has been a growing perception that information governance is often cited as a reason not to share information, even when this is in the best interests of the patient or service user. This perception is associated with three common criticisms:

- There is a lack of understanding of information governance due at least in part to its complexity.
- There is a lack of commitment to information governance and people cannot be bothered with it.
- There is a marginalisation of information governance professionally or at least in the minds of health and social care professionals.

Paradoxically, criticism that the bureaucracy of information governance is standing in the way of sensible information sharing among professionals has gone hand in hand with equally vociferous criticism that the system is not doing enough to combat laxity in the protection of confidential data and information. There is a perception that too much information is being disclosed inadvertently as well as too little being shared deliberately. Furthermore there is uncertainty among many patients and users of services, who are unaware of how personal confidential data about them is collected and shared. If people do not know how their data will be used, it is wrong to assume they have given their implied consent to sharing.

1.6 The Future Forum and the Information Governance Review

The *NHS Future Forum* work stream on information noted these issues, and in its report, recommended that:

> *"The Government should commission a review of the current information governance rules and of their application, to report during 2012. The aim of the review should be to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care*[2]*."*

In January 2012, the Government accepted this recommendation, and the then Secretary of State for Health asked Dame Fiona Caldicott to lead a new independent review of information governance across the whole health and social care system in England. Dame Fiona agreed and in order to distinguish this review from Dame Fiona's report in 1997, it also became known as the Caldicott2 Review.

In May 2012, Dame Fiona convened a Panel of 15 experts to conduct the review. The names of the Panel members are set out in appendix 1. Between May to October 2012, the Panel took evidence from a wide range of stakeholders, holding 49 individual evidence sessions, taking evidence from over 230 people and receiving more than 200 pieces of written evidence.

The Information Governance Review took place in the context of a series of other initiatives that are relevant to information governance and have influenced the Panel's deliberations.

1.7 The Information Strategy

The views of the public were heavily canvassed in the production of the Government's Information Strategy: 'The Power of Information: Putting all of us in control of the health and social care information we need', published in May 2012[3]. It set out the need for a cultural and operational shift to enable patient access to records. It explained how the health and social care system should be better integrated by allowing data to pass from one information technology system to another, and for quality of care to be the driver for the system.

---

[2] Information: A report from the NHS Future Forum, January 2012, http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/documents/digitalasset/dh_132086.pdf

[3] The Power of Information: Putting all of us in control of the health and care information we need, Department of Health, 21st May 2012

1.8 Health and Social Care Act 2012

The Health and Social Care Act 2012[4] did not make substantive changes to the overarching legal framework for data protection, the common law duty of confidentiality, or human rights requirements, all of which are relevant to information governance. However, it introduced an important legal basis for the Health and Social Care Information Centre (the Information Centre) to access personal confidential data[5]:

- From 1st April 2013, the Information Centre will be able to obtain confidential information[6] that it has been directed to collect by the Secretary of State and NHS Commissioning Board (section 254 of the Act).
- The Information Centre will also collect confidential information following a mandatory request from a 'principal body', i.e. CQC, Monitor or NICE (section 255).

The Information Centre will be responsible for producing a code of practice on collecting, analysing, publishing or disclosing confidential information[7]. The Information Centre code will be iterative and all health or social care bodies will need to have regard to the code when providing health services or adult social care in England.

In addition, the Act gives rise to a number of changes in public health arrangements that come into force in April 2013. This includes the creation of Public Health England that brings together several bodies with significant information gathering and analysis functions such as the Health Protection Agency and cancer registries. As part of the changes in the Act, local Directors of Public Health and their teams will move from the NHS to local authorities, where they will continue to require access to health data in order to discharge their functions.

1.9 The Government's Open Data White Paper: 'Unleashing the Potential'

In June 2012, the Government published 'Unleashing the Potential', the Open Government White Paper[8]. It states:

> *"Data is the 21st Century's new raw material. Its value is in holding governments to account; in driving choice and improvements in public services; and in inspiring innovation and enterprise that spurs social and economic growth."*

The White Paper proposed a twin track approach to data. It called for greater openness and transparency of data based on a belief that "*data that can be published should be published*", coupled with a commitment to uphold public trust by promising to "*safeguard people's data from misuse and rigorously protect the public's right to privacy.*"

---

[4] Although the Act states the Information Centre may disclose information to other organisations "when necessary or expedient to their statutory function", the Review Panel has confirmed that this does not introduce a lower threshold for disclosure than that stated in the Data Protection and Human Rights Acts which sets the threshold at 'necessary', not 'necessary or expedient', http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

[5] The Information Centre generally cannot disclose or disseminate the confidential information it holds to others. However, there are exceptions set out in section 261:2 of the Health and Social Care Act 2012.

[6] The Health and Social Care Act 2012 defines 'confidential information' as (a)information which is in a form which identifies any individual to whom the information relates or enables the identity of such an individual to be ascertained, or (b)any other information in respect of which the person who holds it owes an obligation of confidence.

[7] Health and Social Care Act 2012, part 9, chapter 2, section 263 — Functions: information systems — Code of practice on confidential information, http://www.legislation.gov.uk/ukpga/2012/7/section/263/enacted

[8] http://www.cabinetoffice.gov.uk/resource-library/open-data-white-paper-unleashing-potential

The Government set out the desire to make personal data records available to those to whom they relate through a secure online portal. Details of how and when record access to central data sets will be done in the health and social care system is still in discussion at this stage, apart from the sharing associated with GP records (see section 2.3).

The Government committed to "*ensure that privacy is not considered as an afterthought but at the beginning of all discussions concerning the release of a new dataset. We will ensure we keep pace with the latest technology so anonymised datasets remain anonymised and personal data remains personal.*"

The White Paper references the Information Governance Review as part of its commitment to getting the balance right between transparency and privacy.

1.10 The NHS Constitution

The NHS Constitution sets out in one place the principles and values of the NHS in England, and the key rights and responsibilities of both patients and staff.

In November 2012, the Department of Health launched a consultation on strengthening the NHS Constitution[9]. This included proposed changes to the Constitution, intended to explain more fully how patient information is both protected and used by the NHS. The Review Panel assisted the Department and the NHS Future Forum in the development of these proposed amendments.

The Review Panel is proposing the rights, responsibilities and commitments on patient data, contained in the NHS Constitution, are extended to cover the whole health and social care system (see section 5.9).

1.11 Information Commissioner's Office anonymisation code

In November 2012, the Information Commissioner's Office (ICO) published '*Anonymisation: managing data protection risk code of practice*'[10] (the ICO anonymisation code). The Review Panel has worked to ensure alignment with the ICO anonymisation code, which is particularly relevant to section 6.3 of this report, which discusses the different states of anonymous and identified data.

1.12 Law Commission project on data sharing

The Law Commission intends to start a project on data sharing between public bodies in spring 2013. The rationale behind the work is that there are persistent reports that public bodies have difficulty in sharing data because of legal barriers that prevent them from fulfilling their duties to citizens.

[9] https://www.wp.dh.gov.uk/publications/files/2012/11/Consultation-on-strengthening-the-NHS-Constitution.pdf

[10] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx

2 People's right to access information about themselves

2.1 Our right to know

An important commitment in the 'The Power of Information', the Department of Health's Information strategy, was to give people better access to their care records. The reasoning was that people who are allowed to share their own records can be empowered to take part in decisions about their own care in a genuine partnership with professionals. The Strategy said:

> *"Electronic access to our own care records where we request it will start with GP records by 2015 and our social care records as soon as IT systems allow. Work with patient, service user and professional bodies and with industry will enable this access to expand progressively to our records across health and care."*

The Review Panel heard evidence that people's lack of access to their records under the present system is causing great frustration. People are being told they have a choice of services, but their choice is constrained if they do not have the facts about themselves.

2.2 Barriers to sharing

Repeatedly the Review Panel heard that patients' attempts to become involved in decision making were thwarted by "information governance rules" that ignored their express wishes. Examples included:

- patients and carers being denied information via email even if they explicitly consented to this and knew the risks, because of 'data protection policies';
- patients signing consent forms to allow health and social care professionals to work together but finding that the sharing is blocked by either health or local authority information governance leads;
- blind patients not being offered communications in an audio format, or other suitable media, so they are not discriminated against; and
- patients being charged a fee in exchange for access to their records.

These examples appear in the main to originate from local information governance policies, which vary between organisations. For example, the NHS Cambridgeshire and Peterborough Email Acceptable Use Policy 2012—13[11] does allow emailing to the patient and has a suitable explicit consent form included. The email policy for NHS Leeds[12] allows email communication to occur if consent is documented in the patient notes. The email policy for North East London[13] does not deal with the subject directly but suggests secure email and encryption for emails containing patient identifiable data. It also alludes to disciplinary action as a consequence of poor compliance.

[11] http://www.cambridgeshire.nhs.uk/downloads/policies/Information%20Governance/Email%20Acceptable%20Use%20Policy.pdf

[12] http://www.leeds.nhs.uk/Downloads/Corporate/FOI/Email%20Policy.pdf

[13] http://www.nelft.nhs.uk/_documentbank/IT006_Email_Policy_revised_IT006___Feb_09.pdf

Case study

A 72-year-old who is totally blind is the full-time carer for his wife, who has dementia and Parkinson's disease. He asked her hospital consultant to send letters by email. That way he could use a screen reader to convert the words into speech. His wife can no longer understand letters in any format.

The consultant refused because his NHS trust considered email to be insecure. "To preserve her confidentiality," he insisted on sending hard copies of letters so her husband had to get someone else to read them out to him. So much for confidentiality.

The Review Panel was surprised local policy was viewed as a higher authority than patient consent, which has a legal basis.

The Review Panel concludes that personal confidential data can be shared with individuals via email when the individual has explicitly consented and they have been informed of any potential risk.

In addition to giving people access to their electronic care records, the Review Panel concludes that patients who request personal on site access to the paper notes of a particular episode, or copies of particular test results should not be unreasonably refused or charged a fee. However, copies of full paper records should follow thestandard 'Subject Access Request' process[14]. The Review Panel endorses the British Computer Society publication 'Keeping your health and social care records safe and secure'[15].

The Review Panel concluded that the key test for health and social care professionals, information governance experts and the provider should be: 'Have I placed good patient care and patient satisfaction at the centre of my decision making?'

2.3 Scale of sharing

All communications between different health and social care teams should be copied to the patient or service user — there should be 'no surprises' for the patient as to who a record has been shared with.

As a rule of thumb, the stimulus or trigger for communications of this type should be when care of an individual moves between providers and settings. There are broadly two types of electronic record sharing with the patient, which are explained below.

[14] A 'Subject Access Request' is a written request made by an individual to a data controller to find out whether personal data is held about them and, if so, what personal data is held, http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject_access_requests_for_health_records.ashx

[15] http://www.bcs.org/upload/pdf/social-care-records.pdf

Definition: two types of records

Personal health and wellbeing records broadly consist of two main types. People may have both.

- **Health and social care records**
  These are the commonest type and are supported by the information strategy. A professional creates an electronic patient record, which is then shared with the patient and their relevant care teams. The health or social care professional is responsible and accountable for that record when it is for the purpose of direct care. Patients may get right of access, the ability to see, interact and request corrections but not the right to change the content because that might be clinically unsafe. This access is sometimes referred to as 'patient online access' or 'record access'.

- **Patient-owned records**
  These are less common forms of record that individuals create and manage themselves. They are kept separate from any electronic patient record and the individual has total control and responsibility for the content. Patient-owned records may include extracts from electronic patient records, but may also contain information added by the individual such as exercise monitoring data, weight etc; commercial contributions e.g. from over the counter drug purchases or from supermarket alcohol purchases; and contributions from personally acquired 'medical devices'.

The Royal College of General Practitioners, in concert with the Department of Health and other stakeholders has been leading work on providing patients with online access to their care records. In March 2013, the RCGP published *Patient Online: The Road Map*[16], which includes guidance for GP's on information governance and safeguarding for GPs in relation to online access. The Review Panel concludes that wider-scale record access needs to build on this work.

The aim for records access should be that people will be able freely to access their electronic records, such as electronic hospital records, community records and personal confidential data held by all organisations in health and social care, within a reasonable time frame after the implementation of GP record access. The Review Panel believes this should be complete within the next decade. This will not automatically happen unless there is a clear plan for implementation. See recommendation 1 below.

This approach enables variable speeds of progress, allowing GP practices and patients to forge ahead and, through this model, test and develop new possibilities. Other aspects of the RCGP's important work are considered in section 10.2.

[16] http://www.rcgp.org.uk/clinical-and-research/practice-management-resources/health-informatics-group/patient-online.aspx

One particular challenge, which arose out of this work on giving patients access to records and letters, concerned the subject of health literacy and language. Records are designed to support the professional care for the patient and so interpretation may be very difficult for patients. This difficulty is magnified when English is not the person's first language. The Review Panel discussed this issue at length and noted that different activities, with different responsible owners, could improve the situation. These are:

- Over time the health and social care system should adopt international record content data standards, which have an automated capability of representing faithfully the same concept in the patient's record in their own language as represented by the English language in the record used by the professional.
- Health literacy should be promoted through education in schools and universities and supplemented, if necessary, with services to help patients' understanding of their records.
- Patients and service users should be able to go to independent facilitators for confidential help with translating their record, if they choose not to use family and friends.

2.4 Identity management

Assuring that only persons with a legitimate reason can access information about a patient is fundamental to maintaining confidentiality. For staff with access to personal confidential data, this is relatively straightforward: their identity is checked on recruitment and processes such as passwords, smart cards and security locks control their access to systems and records stores. Care should be taken to ensure that these processes do not make the systems unworkable. For "computerised" systems, it is achieved through the presence of a sound and effective audit trail.

Case study

Community matrons were issued with handy laptops with Internet access.

They were expected to arrive in the patient's home and call up medical notes, including the latest test results. Before leaving, they were meant to update the care plan online.

However, limitations of the IT system combined with restrictions of information governance to frustrate the plan. A matron told the Review:

> *"We had to enter three passwords before we could even get to the stage of using our e-cards to access [the patient's data.] That would take 10-15 minutes and then, likely as not, the system would crash."*

The matrons stopped using the laptops.

Case study

Nurses in Derbyshire have pioneered the use of digital pen technology to record visits to patients without risk to data security.

Derbyshire Healthcare NHS Foundation Trust provided the equipment to 800 staff doing mental health work in the community. It enabled them to convert handwritten notes into data that could be fed through a mobile phone to reach the trust's database almost instantly.

The trust is confident that information cannot be intercepted. Digital pens have saved community psychiatric nurses about 15 minutes for each patient visit, without reducing face-to-face time. They contributed to savings in excess of £800,000 over two years.

The objective of increasing patients' access to their own records requires that there is a secure but straightforward means to identify and authenticate anyone who has had access. This includes patients or service users and their carers or nominees for whom they have given explicit consent to access their record or receive information, and a way of seeing that this access has been used appropriately. Health and social care organisations should ensure they align with initiatives on identity assurance, such as the 'Identity Assurance: Enabling Trusted Transactions' programme being led by the Cabinet Office[17]. These solutions should apply not only to electronic records, but also medical devices, as set out in chapter 11.

The Review Panel concludes that in addition, there is a need for an information governance standard on identity management by 2015, common across health and social care, that is appropriate to the highly sensitive nature of personal confidential data.

The Review Panel concludes that a full and meaningful audit trail, which details anyone and everyone who has accessed an individual's electronic personal confidential data, should be made available in a suitable form to patients via their health and social care records.

Patients themselves (and any other people they have given access to their record) should be treated in exactly the same way as staff and be captured on the audit trail.

[17] http://www.cabinetoffice.gov.uk/resource-library/identity-assurance-enabling-trusted-transactions

Recommendation 1

People must have the fullest possible access to all the electronic care records about them, across the whole health and social care system, without charge.

An audit trail that details anyone and everyone who has accessed a patient's record should be made available in a suitable form to patients via their personal health and social care records. The Department of Health and NHS Commissioning Board should drive a clear plan for implementation to ensure this happens as soon as possible.

3 Direct care of individuals

3.1 A culture of anxiety

When it comes to sharing information, a culture of anxiety permeates many health and social care organisations from the boardroom to front line staff. The Review Panel found the anxiety results from instructions issued by managers in an attempt to protect their organisations from fines for breaching data protection laws. This leads to a 'risk-averse' approach to information sharing, which prevents professional staff at the front line co-operating as they would like.

This anxiety must be changed to trust, in order to facilitate sharing on the front line. The constant message from caring and committed staff was that there should be a presumption in favour of sharing for an individual's direct care and that the exceptions should be thoroughly explained, not vice versa. The motto for better care services should be: 'To care appropriately, you must share appropriately'.

There is also a lack of trust between the NHS and local authorities and between public and private providers due to perceived and actual differences in information governance practice, which manifests in tension among health and social care professionals and further limits sharing.

It is clear that information governance is both part of the cultural impediment to sharing for the care of patients and clients and is used as an excuse for other impediments to sharing.

3.2 Implied consent

Most people who use health and social care services accept and expect that doctors, nurses and other professionals will need to share personal confidential data if they are going to provide optimum care. People get frustrated if they have to answer the same questions repeatedly as they move along a care pathway. It may be good professional practice for a clinician to check an item in a medical record by asking the patient to expand on a previous answer. However, it is not good practice for important information to be missing from the record. Patients and service users want the professionals to act responsibly as a team.

There is in effect an unwritten agreement between the individual and the professionals who provide the care that allows this sharing to take place. This requires the health and social care professional to treat the patient on the basis of their needs and keep the patient's information confidential. In return, the health and social care professional is able to rely on 'implied consent'[18] when sharing personal confidential data in the interests of direct care, as long as the patient does not object, or has not already done so. Patients therefore trust professionals to both protect their personal confidential data, and share information safely in the interests of their care and imply they consent to their information being shared in these settings.

[18] GMC guidance on confidentiality, http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_24_35_disclosing_information_with_consent.asp

The Review Panel found there was limited awareness of the boundaries of implied consent both among health and social care professionals who rely on it and other staff who feel it may apply to their practices. The Review Panel also found that patients and public generally assumed there was a greater level of sharing to support direct care than was actually happening[19].

The Review Panel has sought to clarify when implied consent can be used to share identifiable patient information and to identify the circumstances when another legal basis for sharing is required.

Definitions of consent

Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

Explicit consent

Explicit consent is unmistakeable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. A patient may have capacity to give consent, but may not be able to write or speak. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual[20]. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health and social care.

Implied consent

Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed. Examples of the use of implied consent include doctors and nurses sharing personal confidential data during handovers without asking for the patient's consent. Alternatively, a physiotherapist may access the record of a patient who has already accepted a referral before a face-to-face consultation on the basis of implied consent.

[19] Gentle P, Severs MP, Washbrook M, Flanagan P. Patients' and Professionals' Views on the Communication of Clinical Information between Professionals in Improving Clinical Communications. Clinical Systems Group. Department of Health, February 1998

[20] Note: unless there is a statutory basis or the public interest test can be satisfied.

The Review Panel concluded that across the health and social care system, implied consent is only applicable in instances of direct care[21].

3.3 The limits of sharing for direct care

The Review Panel found a strong consensus of support among professionals and the public that safe and appropriate sharing in the interests of the individual's direct care should be the rule, and not the exception.

However, the need to share some information does not entail the sharing of everything, for example, a patient may tell a GP she is pregnant, but not by her husband, and she does not consent to this information being shared with any other doctor. Or a professional in a particular field, such as a physiotherapist treating a patient's knee, may not need to know about his impotence.

The Review Panel concluded that in line with the original Caldicott review principles, only relevant[22] information about a patient should be shared between professionals in support of their care.

3.4 Improving sharing of information for direct care

The Review Panel has found that generally, the practice of sharing personal confidential data between those directly caring for individuals could be better. For example, The Review Panel heard evidence from a charity worker who found herself in a dangerous position with a man possessing a Samurai sword that could have been avoided, but the local authority did not share personal information with voluntary groups.

The Review Panel concludes that providers in the health and social care system may benefit from reviewing and improving their policies for sharing to ensure they are focused on the patient or service user's best interest, taking account of the safety of people providing care. In doing so, organisations should seek the advice and input of the clinicians and professionals who are required to implement these policies.

The recommendations within the NICE Guideline: *Patient experience in adult NHS services: improving the experience of care for people using adult NHS services* (Clinical Guideline138)[23] emphasise the importance of appropriate sharing (see appendix 3).

The Review Panel endorses this guideline and concludes that all provider organisations in the health and social care system should apply the guideline to audit their procedures and performance, addressing any procedures that may impede effective sharing.

---

[21] This is in line with 'Confidentiality: The NHS Code of Practice', 2003, http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

[22] In this report, 'relevant' information is defined as information that may directly influence the decision over what care is given to a patient or service user, and how that care should be given.

[23] http://www.nice.org.uk/nicemedia/live/13668/58284/58284.pdf

Recommendation 2

For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Health and social care providers should audit their services against NICE Clinical Guideline 138, specifically against those quality statements concerned with sharing information for direct care.

3.5 Professional regulation

Direct care is generally led by registered and regulated professionals with a duty of confidentiality and an obligation to use information both legally and effectively. They are answerable to regulatory bodies such as the General Medical Council, Nursing and Midwifery Council and Health and Care Professions Council, which have the authority to strike people off the professional register for serious dereliction of duty. These regulatory bodies each use different language to describe the conditions when implied consent can be relied upon. Additionally, the scope of implied consent may be interpreted differently by different professionals.

There is universal agreement that implied consent may be used as the legal basis for sharing relevant personal confidential data in communications such as letters and discharge summaries. However, there is less consensus with regard to the legal basis for sharing of whole records.

The reason is that when whole records are shared, patients do not have the ability to block access to individual pieces of information about their care, and this does not align with the principle of sharing only relevant information. However, in some instances e.g. tertiary centre paediatric services, the relevant information may be the whole record, or more commonly, when a patient transfers to a new GP, their whole GP record will need to be transferred with them.

The Review Panel concluded that consent should be obtained before sharing a patient's whole care record with other registered and regulated health and social care professionals for the purposes of direct care. Any exceptions to this guidance should be based on professional judgement in individual cases.

To allow safe and effective inter professional and organisational sharing it is imperative that regulators agree a consistent language to describe the common set of conditions when implied consent can be relied upon by all parts of the health and social care system, including professionals, commissioners and providers.

Recommendation 3

The health and social care professional regulators must agree upon and publish the conditions under which regulated and registered professionals can rely on implied consent to share personal confidential data for direct care. Where appropriate, this should be done in consultation with the relevant Royal College. This process should be commissioned from the Professional Standards Authority.

3.6 Registered and regulated professionals

Professional standards and good practice

Personal confidential data needs to be shared between registered and regulated health and social care professionals who have a legitimate relationship with the individual for the purposes of the individual's direct care. A registered and regulated health or social care professional has a legitimate relationship with the patient or client when any or all of the following criteria are met:

- The patient or client presents themselves to the professional for the purpose of their care.
- The patient or client agrees to a referral from one registered and regulated health or social care professional to another.
- The patient or client is invited by a professional to take part in a screening or immunisation programme for which they are eligible and they accept.
- The patient or client presents to a health or social care professional in an emergency situation where consent is not possible.
- The relationship is part of a legal duty e.g. contact tracing in public health.
- The patient is told of a proposed communication and does not object e.g. the consultant in the ambulatory clinic says she will communicate with the patient's social worker to let them know of events in the clinic and the patient does not object.

Sharing for direct care can take place across departmental and organisational boundaries for example, the direct care team may include physiotherapists, nurses, midwives, occupational therapists and others on regulated professional registers.

The Review Panel found some uncertainty among professionals as to whether social workers should be considered part of the care team in a health context.

The Review Panel concluded that for direct care of an individual, registered and regulated social workers must also be considered part of the care team and covered by implied consent when the social worker has a legitimate relationship to the individual concerned.

The Review Panel found that patients and the public may not fully appreciate the extent to which their personal confidential data could be shared within an organisation, after they have given it to a registered and regulated professional. For example, members of the public giving evidence to the Review Panel considered that sharing information with an individual social worker would be acceptable, but sharing with the whole local authority employing the social worker would not.

There is also a concern among some health and social care professionals that they are sometimes asked to send confidential information to generic electronic email accounts or electronic mailboxes, rather than to a named individual. Generic accounts mean there is no clarity as to who is receiving the correspondence or whether they are a registered and regulated health and social care professional.

The Review Panel concluded that where it is necessary for services to receive referrals through a generic system, this must be under the direct or indirect control of a registered and regulated health and social care professional. This is necessary in order to comply with the individual patient's consent to be referred to a professional.

When a patient does NOT want to share some or all of their personal confidential data with a health and social care professional this should be noted in the person's direct care record. The risk of not sharing the information should be explained to them, but in general, their wishes should be respected[24] (see section 5.5).

3.7 Non-regulated staff providing direct care

Some components of direct care may be delivered by non-registered and non-regulated health and social care staff. Examples include a healthcare support worker going to the home of a patient to change a catheter bag, a 'system administrator' inputting information from a hospital discharge summary into an electronic GP record or porters taking request forms and samples to the laboratory. The Review Panel found evidence that patients and the public did not always appreciate how many non-registered staff could be part of a person's healthcare team.

Professional standards and good practice

The Review Panel concluded that when providing direct care, a non-regulated individual should be able to access a proportion of a patient or service user's personal confidential data when any or all of the following criteria are met:

- The patient presents themselves to those individuals for the purposes of care e.g. NHS 111.
- They are professionally supervised by a registered and regulated health or social care professional.
- They are managerially directly responsible to a registered and regulated professional for the lawful use of personal confidential data.
- They have only necessary and very limited access to patient and client data.

[24] Reasons for not respecting the patient's wishes include if the data flow is mandated through statute or if the public interest test can be met.

Professional standards and good practice (continued)

- The patient or client has given explicit consent that this individual should access all or part of their personal confidential data.
- The staff member is registered on a voluntary register approved by the Professional Standards Authority.

And in all cases:

- The terms and contractual obligations of employment within an organisation have an explicit duty of confidentiality as part of the contract with sanctions.
- The non-regulated individual is a part of the direct care team with a 'legitimate relationship' to the patient or client.

Recommendation 4

Direct care is provided by health and social care staff working in multi-disciplinary 'care teams'. The Review Panel recommends that registered and regulated social workers be considered a part of the care team. Relevant information should be shared with members of the care team, when they have a legitimate relationship with the patient or service user. Providers must ensure that sharing is effective and safe. Commissioners must assure themselves on providers' performance.

Care teams may also contain staff that are not registered with a regulatory authority and yet undertake direct care. Health and social care provider organisations must ensure that robust combinations of safeguards are put in for these staff with regard to the processing of personal confidential data.

3.8 Care homes and home care

For patients who reside in care homes, relevant clinical and social care information should be shared with a registered and regulated professional at the care home, unless the patient objects. This can be done on the basis of implied consent.

For example, in order to ensure continuity of care is maintained after a patient is discharged from hospital, the care home may require relevant information about the patient's mobility, medication, nutritional needs and general condition.

For patients who reside in their own home with a package of care, relevant clinical and social care information should be shared with the registered and regulated professionals providing that care, unless the patient objects. This can also be done on the basis of implied consent.

However, in residential care homes and for people living at home, a considerable proportion of care is provided by staff who are not regulated by statute. It is not reasonable to assume that patients being discharged from hospital have given implied

consent for confidential personal data to be passed to these unregistered and unregulated staff. Yet it may not be safe for people to be discharged in these circumstances without some key information about their condition and medication accompanying them. The situation is further complicated by the fact that individuals needing complex care packages are more likely to lack capacity to give consent.

An increasing number of these staff are expected to be registered on a voluntary basis by the Professional Standards Authority. This will give the public a greater assurance because staff registered in this way who seriously breach specialist group rules can be dismissed for serious malpractice.

Professional standards and good practice

The Review Panel concluded that appropriate communication from a regulated and registered professional to non-regulated staff should be the norm and occur through one of the following routes:

- The patient gives explicit consent to the sharing of their personal confidential data.
- The contact point of the service is a registered and regulated health and social care professional and communication is through implied consent.
- The communication is through the social worker or equivalent professional within the local authority who has organised the package of care ('care and support plan') in line with the proposed duties in the Health and Support Bill.
- The communication is given to the patient, with or without a carer being present, and the patient makes the decision to share their copy of the communication.
- There is a specific safety concern regarding the patient, which is best resolved or mitigated by sharing some of the patient's personal confidential data in situations where consent is not possible. In these situations, professional judgement and the patient's best interests need to apply.

3.9 Sharing information with and from friends and family

If patients and clients want their personal confidential data shared with friends or family, they are entirely free to ask the health and social care professional to do this and the request should not reasonably be refused. If this request is ongoing, consent for sharing should be documented and capable of being shared between health and social care professionals as part of their normal communications.

Health and social care professionals sometimes receive important information about a patient from a third party, such as a partner or family member, a friend or a carer. This information can often be relevant to a patient's care, but may also be highly sensitive and may have been given in confidence.

Case study

A daughter was very concerned about her father's symptoms and the impact on her mother who was caring for him unsupported. She suspected that her father had dementia, but this was undiagnosed because her father had not seen the GP in a long time. The daughter wrote to the GP and received a curt reply that she must never approach him again, by letter or phone, because of patient confidentiality.

This could have gone on for years, but an unrelated event finally revealed the family's situation to Social Services and he was diagnosed with Alzheimer's. Because of too rigid an application of 'patient confidentiality' the family lost all that time when they could have helped the patient to live well with his dementia and been planning for the future. None of this is in the best interests of father, mother or daughter.

Examples: two kinds of third party data

Third party data means both data *from* third parties and data *about* third parties.

An example of data *from* a third party would be Mrs X ringing about her husband's headaches, personality change and refusal to visit the doctor.

An example of data *about* a third party includes a family history of premature stroke in the patient's siblings and other family members all listed in the patient record.

In terms of data from a third party, there is a need to consider what information can be disclosed to the patient, without breaching any obligation of confidentiality owed to the third party. In some instances, it may be possible to separate the identity of the third party giving evidence to the doctor from the information they give. This is made clear in the ICO guidance on subject access requests, which states:

> *"For the avoidance of doubt, you cannot refuse to provide subject access to personal data about an individual simply because you obtained that data from a third party[25]."*

However, it is perfectly feasible that, for example, a patient may be able to identify that the third party who provided data for his record was his wife, even if her identity was withheld. The question is should a professional explain this risk to the third party when receiving this information?

[25] See ICO guidance at: http://www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/SAR_AND_THIRD_PARTY_INFORMATION_100807.ashx

Professional standards and good practice

There are occasions when a third party, such as a family member, may offer information to a registered and regulated professional who is part of an individual's care team when the patient is absent. The Review Panel concluded the professional should explain to the third party that either at the time or sometime in the future the patient may be able to identify the source of the information even if the identity of the third party is withheld. This should be undertaken BEFORE the third party has disclosed the information they wish to share. This means the third party has the following options:

- The third party consents to the patient finding out their identity.
- The third party wants the information recorded and understands there is a residual risk of them being identified as the source of the information even if it is not readily identified to the patient by Patient online Access.
- The third party decides NOT to tell the professional the things they were planning to tell. (Clearly this option is only viable if the information about the patient has not already been disclosed.)

This new piece of professional practice is not confined to GPs, but impacts on all health and social care professionals as they communicate with one another and therefore share data which may have arisen from a third party.

With increasing patient access to records, it is therefore important that information from a third party is not put into a patient's record unless the provider of the information understands that the patient may become aware of this information and its source. For information that has already been obtained, professionals will need to use judgement and evaluate what information can be disclosed to a patient when it was originally provided in confidence by a third party[26].

The Review Panel concluded that the knowledge and skills to undertake such a dialogue is currently not taught nor widely understood by professional staff. This situation must be remedied through professional education.

[26] Note: While the ICO has said that individuals should not be prevented from access to information about them provided by a third party, information can be withheld if a professional believes there is a risk of harm to the third party if the information is shared.

Professional standards and good practice

Some friends and/or family have a special relationship with the patient in that they act as a carer[27]. Personal confidential data should be shared with the carer, when the patient has given explicit, informed consent. In circumstances where the patient cannot give valid consent, confidential information should be shared with the carer subject to open dialogue with the patient, when ALL the following criteria are met:

- the patient/service user lacks capacity;
- the carer 'cares for' the patient/service user;
- there is no legal documentation in place to prevent sharing;
- there are no contra-indications to sharing in the patient's record; and
- there are no safeguarding issues apparent.

3.10 'Blagging'

Health and social care professionals and staff may sometimes be asked for sensitive information about a patient, for example, when an individual calls an organisation seeking information about a patient they claim is a relative. Care must be taken to ensure any caller is legitimate, and that it is appropriate for personal confidential information to be shared with them. For example, the Leveson inquiry heard from one witness that:

> *"if an investigator sent a fax to a GP or a hospital saying, 'I'm his specialist, I need these details', it was incredible how many times that [the information requested] would just get sent straight back[28]."*

These can be difficult judgements, especially in relation to direct care. To support decision making, employing organisations should have clear protocols and procedures for professionals and staff. These policies should align with the guidance from professional regulators and national information governance standards and statements.

Confidentiality: NHS Code of Practice[29] provides advice on patient confidentiality issues, and states:

> *"Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (using an independent source for the phone number). Check also that they have a legitimate right to have access to that information."*

Inevitably, there are occasions when professionals and staff disclose personal confidential information by mistake. Such mistakes can result in serious consequences.

---

[27] This report adopts the definition of 'carer' used in the Health and Support Bill section 10 subsections 7 and 8. There is evidence of huge variation in the access carers can have to information about those they care for. For example, study of the unmet needs of partners and caregivers of adults with cancer found unmet needs concerning information ranging from 2.2% to 86%, see http://spcare.bmj.com/content/early/2012/07/06/bmjspcare-2012-000226.

[28] http://www.levesoninquiry.org.uk/wp-content/uploads/2011/12/Transcript-of-Afternoon-Hearing-19-December-2011.pdf

[29] NHS Confidentiality Code of Practice, November 2003, http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

In addition to reporting any such breach to managers, it is imperative that the safety of the patient whose confidence has been breached is uppermost in everyone's mind and appropriate advice is sought as soon as the error has been detected. Expert advice can be sought from:

- professional regulators;
- national standards and statements;
- organisational policies;
- Caldicott Guardians and information governance specialists;
- professional insurers; and
- line managers.

The Review Panel concludes that in order to support professionals and staff in making data sharing decisions, and to respond to mistakes when they occur, clear good practice guidance and local policies are a vital resource along with national statements, guidance and standards. These resources should be available and used in all situations of uncertainty to support professional judgement.

The Review Panel also concluded that individuals must be informed of any breach of their personal confidential data as part of maintaining public trust and supporting transparency.

Recommendation 5

In cases when there is a breach of personal confidential data, the data controller, the individual or organisation legally responsible for the data, must give a full explanation of the cause of the breach with the remedial action being undertaken and an apology to the person whose confidentiality has been breached.

3.11 Barriers to sharing

The Review Panel heard that in some cases of direct care, the transfer of necessary and relevant information between organisations was poor. This often caused frustration and distress for patients, and could potentially affect the quality of care they receive.

Five specific examples of data transfer issues across organisational boundaries were identified:

- Defence Medical Services to the NHS. A pilot project aimed at improving transfer between the Defence Medical Services and NHS showed positive results, but beyond this, information transfer is often late and partial.
- GP/NHS to Prison Health to GP/NHS. The NHS and prison health transfers were sometimes more challenging due to consent issues.
- GP to GP. Some GP to GP transfers take many months and suffer from quality issues relating to moves from paper to electronic records. However the Review Panel notes that the electronic GP to GP record transfer system appears timely and efficient when available.
- Communications between consultants when patients with complex illnesses are under more than one specialist.
- Transfers between hospitals and care homes.

The Review Panel concludes that organisations should pay closer attention to the appropriate transfer of information when people cross organisational boundaries.

3.12 Professional responsibilities when sharing

The Review Panel heard that there is considerable uncertainty in the minds of some health and social care professionals regarding who is responsible for the protection of personal confidential data when it has been shared. Some professionals are concerned that after they have shared information about a patient, they may still be held accountable for any onward sharing of that information and the decisions that ensue, when in reality it had passed beyond their control.

The Review Panel concludes that a registered and regulated professional's primary concern must be for the health and wellbeing of the individual to whom they are providing direct care and, as set out in sections 3.1 and 3.3, the presumption should be in favour of sharing for an individual's direct care.

As part of this, professionals have a responsibility for accurately communicating information, ensuring that the recipient understands any particular issues or conditions that apply, such as safeguarding issues, or whether individuals have expressed particular wishes in relation to onward disclosure that should be respected.

The Review Panel concludes that for direct care, when a professional is satisfied the recipient has a legitimate relationship with the patient, and that the recipient understands any particular issues or conditions that apply, the information can be shared with the individual's implied consent. The recipient then becomes responsible and accountable for that information in a professional capacity.

The Review Panel also concludes that organisations employing health and social care professionals must support the safe and effective sharing of personal confidential data for direct care between professionals and staff with a legitimate relationship to an individual.

While staff have a general duty to follow organisational policies, this should not be to the detriment of safe and effective care. When personal confidential data needs to be shared between professionals in different organisations, both the disclosing and receiving organisations concerned are responsible for ensuring information governance measures are in place that protect the personal confidential data they hold, but which do not inhibit appropriate sharing for direct care. Professional bodies and regulators of health and social care organisations and people have a role supporting organisations to accomplish this.

3.13 Clinical and social care audit

Another aspect of direct care is the auditing process that is used by health and social care professionals to improve the quality and effectiveness of their work through systematic review. It requires aspects of care to be selected and systematically evaluated against explicit criteria[30]. To that end, the people conducting an audit sometimes require access to information about individuals at various stages of care. They may need to link personal confidential data from different sources to ensure they are tracking the experience of the same individual while ensuring the accuracy of the data.

[30] An Information Governance Guide for Clinical Audit (Healthcare Quality Improvement Partnership, a consortium of the Academy of Medical Royal Colleges, the Royal College of Nursing and National Voices), http://www.hqip.org.uk/assets/Downloads/Information-Governance-and-Audit-Guide.pdf

The use of personal confidential data for local clinical audit is permissible within an organisation with the participation of a health and social care professional with a legitimate relationship to the patient through implied consent. For audit across organisations, the use of personal confidential data is permissible through support under the section 251 regulations where approved. (see section 6.7)

The public would expect commissioners to require specific audit activities across organisational boundaries in their area, for example auditing thrombolysis treatment in acute stroke. This enables the audit to be led by health and social care professionals with a legitimate relationship to the patient. Aggregate audit data should be made publicly available.

National audit appears to be working well using de-identified data or through legal support provided under the health service regulations[31].

3.14 Direct care and genetics

Professional standards and good practice

The information governance principles for providing direct care for patients with genetic conditions are exactly the same as the direct care of any patients. However, there is a particular challenge with regard to the creation of a legitimate relationship between a geneticist and a family member. This often involves complex practices, including consent forms, which do not arise in other areas of health and social care. The Review Panel concludes that either of the following solutions are appropriate in creating a legitimate relationship:

- The geneticist gives the patient a letter of explanation for their family members on why they should seek the attention of a geneticist either directly or through their general practitioner which the patient then shares with his or her family members.
- The patient agrees to the disclosure of some of their personal confidential data to their family, and after getting the agreement of family members discloses to the geneticist the contact details of those family members. The geneticist contacts the family members disclosing the issues agreed with the patient and advises the family member on contacting the genetics service and/or their GP for advice.

In some rare cases the patient's consent may be overruled if disclosure of data is in the public interest.

In both instances if the family member makes contact with the proposed genetics service i.e. creates a new legitimate relationship, the information can be shared by the patient's original geneticist with the geneticist of the family member, unless the patient has objected.

[31] Health Service (Control of Patient Information) Regulations 2002 (see section 6.7).

4 Personal data breaches

4.1 Evidence of continuing laxity

The last chapter explained how health and social care organisations have become excessively risk averse due to a fear of breaching confidentiality and data protection laws. This chapter looks at the breaches that nevertheless continue to occur and what can be done to prevent them.

In the 12 months to the end of June 2012, 186 serious data losses in England were notified to the Department of Health. Most of those cases involved the loss or theft of data, but almost one third concerned unauthorised disclosures.

While compiling national figures for data losses, the Department of Health found inconsistencies in the numbers of incidents reported to strategic health authorities (SHAs), which managed the performance of NHS trusts, and those notified to the Information Commissioner's Office, which was responsible for overseeing organisations' compliance with the Data Protection Act and had the power to impose financial penalties for serious breaches. Perhaps unsurprisingly, the SHA totals were higher than the ICO's.

Currently SHAs publish details of data losses affecting organisations for which they are responsible. When SHAs go out of existence, there will be a need for a new, consistent reporting channel to ensure that breaches of patients' confidentiality do not escape the attention of senior managers, ministers, and regulators of health and social care.

The Review Panel heard evidence of laxity in relation to breaches that is often not covered in the national reporting of serious data breaches. Inappropriate conversations or loss of paper records were the cause of most of the reported incidents. It is accepted that human error cannot be eradicated completely, but that where misconduct does occur it should be publicised and personnel should expect to be disciplined.

It was also noted that breaches and leaks involving technology, with or without managerial failings, were often much more significant involving many records and with great potential to do harm. For example, Brighton and Sussex University Hospitals NHS Trust was fined £325,000 when it emerged that it failed to remove confidential records from the hard drives of old computers and failed to dispose of the computers properly[32].

4.2 Information Commissioner's Office actions

The Information Commissioner's Office can engage a number of actions against organisations involved in data breaches. These range from requiring an organisation to sign an undertaking to improve processes in compliance with the Data Protection Act, to imposing a civil monetary penalty of up to £500,000, or ultimately prosecution.

[32] http://www.ico.gov.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012.aspx

Between August 2011 and August 2012, the ICO enforcement team investigated 23 cases in which the NHS had potentially breached section 55 of the Data Protection Act[33].Of these:

- one was closed with the successful prosecution of an individual;
- in 16 cases, it was deemed likely that the data controller was compliant with the Data Protection Act, so the investigations were closed without prosecution;
- one investigation was closed without a prosecution after it was deemed there may have been a data breach, but there was insufficient information to proceed; and
- five investigations remained open.

Appendix 4 contains some examples of ICO actions up to August 2012.

4.3 Deliberate sharing of information or data is not to blame for breaches

The ICO told the Review Panel that no civil monetary penalties have been served for a breach of the Data Protection Act due to data sharing which had been appropriately considered and which had a legitimate data sharing agreement. Problems had occurred when sharing had taken place without due consideration, with data subsequently lost.

In the experience of the ICO, breaches of the DPA are usually the result of a lack of care, rather than because of an issue in a well-designed data sharing agreement. Yet the ICO finds organisations frequently shy away from data sharing agreements and cite data protection as a reason.

Organisations should make the best use of the data they hold, including sharing where appropriate and lawful.

Professional standards and good practice

Any organisation deciding whether to share data or not should first consider three key questions:

- What is the purpose of the data sharing — is there a clear objective that can best be achieved by sharing the data?
- What is the risk to individuals (both the subject of the data or any third parties) of sharing the data and is this risk proportionate to the benefits to the individual that will be achieved? This includes considering if there is a risk to individuals if the data is not shared.
- How will the information be shared?

If there is a clear objective for sharing data and any risk of sharing is proportionate to this objective there will then be other matters to consider. This includes whether there is a legal basis for using the data and whether the conditions for processing, fair processing information, data protection principles, common law duty of confidence and the Human Rights Act requirements can all be met.

[33] http://www.legislation.gov.uk/ukpga/1998/29/part/VI/crossheading/unlawful-obtaining-etc-of-personal-data

At first glance these may seem onerous, but the ICO's data sharing code of practice (May 2011)[34] provides practical guidance to help organisations work through many of these considerations.

In the foreword to the ICO data sharing code of practice, the Information Commissioner said:

> *"Organisations that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness."*

The Review Panel concludes that individuals should not be discouraged from sharing simply through fear of doing this incorrectly. With the help of the ICO's data sharing code, and tools such as privacy impact assessments[35], data sharing can be achieved, where appropriate, in a secure and proper way.

4.4 Sharing information on social media

The Review Panel found no evidence to suggest that people's desire to protect their personal confidential data from unauthorised disclosure is weaker among the 'Facebook generation'. Increasing use of social media has encouraged people of all ages to share online pictures and information of a personal nature that might once have been regarded as deeply private. But a decision by an individual to share some of their personal information with other people on social media does not mean that those in the health and social care system should be any less vigilant in preserving confidentiality. It would be patronising in the extreme to suggest that a more lax approach to protecting confidentiality could be taken, or that people 'had it coming to them' for choosing to use Facebook, Twitter, LinkedIn, YouTube and assorted online blogs.

Research for the Royal Academy of Engineering investigated attitudes among around 2,900 young people, mostly aged 14—18, to having their personal confidential data stored in an electronic patient record. It found:

> *"Growing up in an era of the Big Brother television series and the expansion of social networking sites such as Facebook does not mean that young people do not care about privacy or what happens to their personal information. Privacy is indeed extremely important to young people … Facebook was not deemed to be an invasion of privacy because the young people felt in control of what information was posted and who could get access to that information[36]."*

[34] ICO Data Protection Code of Practice (May 2011), https://www.ico.gov.uk/tools_and_resources/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

[35] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

[36] The Royal Academy of Engineering, 'Privacy and prejudice: Young people's views on the development and use of Electronic Patient Records', October 2010, pp4—5.

It added:

> *"Just because something is private, does not mean young people are not willing to share the information with particular groups, provided the information is not disseminated more widely[37]."*

This attitude was corroborated in evidence to the Review Panel from young people and those providing services aimed at this age group. For example organisations running family planning clinics considered confidentiality to be an absolute requirement to maintain a relationship of trust with clients.

Figures released by the Information Commissioner's Office to the privacy campaign Big Brother Watch in October 2011 showed there were 23 incidents of patient information being posted on social networking sites by NHS staff, involving 13 medical personnel at 11 trusts across the UK[38]. In one incident at Nottingham University Hospital Trust, a doctor was dismissed after posting a picture of a patient on Facebook[39].

This suggests that the advent of social media has not changed any principles of confidentiality. However, it may call for greater vigilance among health and social care professionals as they switch from the personal part of their lives to the professional part.

In draft guidance for doctors using social media, the General Medical Council has said:

> *"The standards expected of doctors do not change because they are communicating through social media rather than face to face or through other traditional media. However, social media does raise new circumstances to which the established principles apply[40]."*

The GMC's suggested guidelines were supplemented by the Royal College of General Practitioners, which produced a 'Social Media Highway Code' to help doctors gain the potential professional benefits of using social media without experiencing the pitfalls.[41]

4.5 Defining 'data breaches'

Currently in the health and social care system in England the terms 'data losses', 'personal data breaches' and 'information governance serious incidents' are used. However, data breaches include data losses, so it is therefore unclear why the term data losses should continue. In addition, the Review Panel noted that the definition of a data breach used by the ICO is more comprehensive than that used by the NHS and includes data losses as well as other forms of data breach.

[37] Ibid p17

[38] The *Guardian*, 28 October 2011

[39] *Health Service Journal*, 20 October 2011

[40] GMC, 'Doctors' use of social media, a draft for consultation'

[41] RCGP, 'Draft Social Media Highway Code', 2012

The Review Panel concludes that there should be a single definition of a 'personal data breach' used by the whole health and social care system, and endorses the adoption of the definition below. This goes beyond the definition used by the ICO[42] to include paper breaches such as letters to the wrong address, as well as electronic records. The amended definition would read:

Definition of a data breach

A data breach is any failure to meet the requirements of the Data Protection Act. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data and inappropriate invasion of people's privacy[43].

4.6 Reporting arrangements

Reporting and management of information governance issues and related serious incidents in the NHS was included within the 'National Framework for Reporting and Learning from Serious Incidents Requiring Investigation'[44] issued by the National Patient Safety Agency in 2010. Under the guidance, primary care trusts and SHAs were responsible for monitoring and reviewing the case with their providers.

The Review Panel concludes that these reporting arrangements must be clarified, following the implementation of the Health and Social Care Act 2012, particularly for the major processors of data such as clinical commissioning groups, the Health and Social Care Information Centre, the Data Management Integration Centres, providers and local authorities.

It should be noted, however, that discussion of serious incidents has hitherto focused exclusively on things that should not happen, and does not encompass those that should, for example the appropriate sharing for patient care.

Under current arrangements, the focus of reporting has been on the scale of data losses, determined by the number of people affected and the potential for reputational damage and media attention. During the course of this review, the Department of Health was investigating more sophisticated methods of categorisation that take account of the potential for clinical harm, damage or distress to patients. This will be introduced as an on-line reporting tool associated with the Information Governance Toolkit in May 2013 and will be further refined during a review of toolkit content later in the year.

Hitherto, there has been no requirement on local authorities to provide similar reports on data breaches in relation to their social care activity, as per NHS organisations, other than reporting to the ICO. From April 2013, when local authorities take on the responsibility for public health, local authorities will be responsible for the data management previously carried out by the NHS. This opportunity should be used to enhance and strengthen the

[42] http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/security_breaches.aspx

[43] Privacy applies to public bodies, but would also apply to private sector through contract or court decision.

[44] http://www.nrls.npsa.nhs.uk/report-a-patient-safety-incident/serious-incident-reporting-and-learning-framework-sirl/

reporting of breaches not just in public health, but also adult social care, to the same standard as that proposed for the NHS. Although a high proportion of direct adult social care is provided outside the local authority's direct control, the Review Panel concludes that the commissioned services should be subject to the same requirements of any qualified provider in health, to report data breaches to the commissioner of the service.

The Review Panel concludes that organisations within the health and social care system in England should report all data breaches to their boards or equivalent bodies. These data breaches should in turn be included in each organisation's quality report in NHS organisations or as part of the annual report or performance report in non-NHS organisations.

While organisations with a national focus, such as the Department of Health, NHS Commissioning Board and Care Quality Commission (CQC), may require central reporting of personal data breaches above a certain level of severity, all personal data breaches must be managed locally.

Recommendation 6

The processing of data without a legal basis, where one is required, must be reported to the board, or equivalent body of the health or social care organisation involved and dealt with as a data breach.

There should be a standard severity scale for breaches agreed across the whole of the health and social care system. The board or equivalent body of each organisation in the health and social care system must publish all such data breaches. This should be in the quality report of NHS organisations, or as part of the annual report or performance report for non-NHS organisations.

5 Information governance and the law

5.1 The legal basis for using personal confidential data

Staff making decisions about sharing health and social care information cannot rely only on compassion and common sense. They must also act within the law. Every minute of every day, staff employed across the health and social care system make lawful use of personal confidential data about patients and service users. All uses of such data are known as 'processing', including holding, obtaining, recording, using and sharing.

Professional standards and good practice

All processing of such data must be lawful. There are four legal bases for processing personal confidential data which meet the common law duty of confidentiality. These are:

- with the **consent** of the individual concerned. Details concerning consent for direct care are fully explored in chapter 3;
- through **statute**, such as the powers to collect confidential data in section 251 of the NHS Act 2006 (see section 6.7) and the powers given to the Information Centre in the Health and Social Care Act 2012 (see sections 1.8, 6.5 and 7.3.4).
- through a **court order**, where a judge has ordered that specific and relevant information should be disclosed and to whom; and
- when the processing can be shown to meet the **'public interest test'**, meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.

In addition to having one of these legal bases the processing must also meet the requirements of the Data Protection Act and pass the additional tests in the Human Rights Act.

Any processing of personal confidential data that is not compliant with these laws, even if otherwise compliant with the Data Protection Act, is a data breach, and must be dealt with as such.

Failure to comply with the law when dealing with people's personal confidential data erodes trust, which can seriously damage the view of the public about the trustworthiness of the NHS or social services.

5.2 Anonymisation

Data ceases to be personal and confidential when it has been anonymised, as explained in chapter 6. In those circumstances, publication is lawful. Data, which has been anonymised but still carries a significant risk of re-identification or de-anonymisation, may be treated either as personal and confidential or as anonymised depending on how effectively the risk of re-identification has been mitigated and what safeguards have been put in place. This is fully explained in the ICO Anonymisation: Code of Practice and in chapter 6 of this report.

5.3 Legal aspects of sharing in direct care

As explained in chapter 3, consent may be obtained by explicitly asking for it, or it may be implied during direct care. For example, when a patient agrees to the GP referring her to a hospital consultant, she can expect the GP to pass on details of the medical condition that requires the consultant's opinion.

Professional standards and good practice

There are three tests for establishing the conditions under which consent can be implied, all of which must be met affirmatively:

- Is the person sharing the information a registered and regulated professional or one of their direct care team?
- Is the activity a type of direct care within the scope specified by the professional's regulatory body?
- Does the professional have a legitimate relationship with the person or persons concerned? (see section 3.6.)

These sit alongside the legal requirements for valid consent (See section 3.2).

The GP may legally assume the patient has given implied consent to the sharing of this information without having to ask her about each individual item. However the patient may explicitly decide she does not want some or all of her information shared and can make an explicit decision to this effect. The GP must then explain the consequences of such a decision and the patient must be fully informed about the outcome of the sharing that takes place.

Direct care is largely consent based. It relies on implied consent for much data sharing. However, if a patient makes an explicit consent decision, for example requesting that their personal confidential data is not shared (or 'actively dissenting' to share), this decision replaces any implied consent and their decision should be respected. In some instances, however, it is necessary to use or share the personal confidential data to comply with legal obligations e.g. where a court order has been issued or on public interest grounds such if the patient poses a significant risk to others.

5.4 Legal aspects of indirect care

A lot of the work within health and social care does not involve the direct treatment or support of individuals, and as a result, does not amount to direct care. Research, commissioning and much of the work done in public health are classified as 'indirect care'. They are more fully explored in chapters 6, 7 and 8.

Some aspects of indirect care need the explicit consent of the patient or service user before their personal confidential data may be accessed and used. For example, patients need to give explicit consent before they can be included in some medical research trials, or patients must explicitly consent for commissioning staff to have access to personal confidential data about their condition in order to secure funding for NHS continuing care.

However, much larger volumes of personal confidential data are shared for the purposes of indirect care using specific statutory authority, particularly section 251 of the NHS Act 2006 (see section 6.7) and powers in the Health and Social Care Act 2012 that enable the Health and Social Care Information Centre to collect and internally process personal confidential data under certain conditions. These powers giving legislative authority for sharing are known as 'statutory gateways'.

5.5 The 'data sharing model'

The Future Forum report stated that the NHS must move to using information technology systems to share data about individual patients and service users electronically — and develop consent arrangements that facilitate this — in the interests of high quality care.

The Review Panel concludes the way that personal confidential data is shared legally within the health and social care system is not deficient in itself, but the way these arrangements are communicated to the public and staff should be improved.

The Review Panel therefore does not consider it necessary to redesign the existing consent arrangements. However, the Review Panel concludes ways should be found to enhance patients' awareness of how their personal confidential data is used and strengthen staff understanding of the scope and limitations of implied consent (see section 3.2).

Recommendation 7

All organisations in the health and social care system should clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes. All organisations must also make clear what rights the individual has open to them, including any ability to actively dissent (i.e. withhold their consent).

A record must be kept of any explicit decision of consent, including withdrawal of consent previously given. If another registered and regulated professional in the patient's care team needs to be made aware of this decision, it should be communicated through the normal process for sharing in direct care.

Some organisations seek patients' consent for the processing of their personal confidential data at the point of registration. This practice is particularly prevalent in the independent sector. Consent for sharing data for specific purposes is described within the appropriate themes in future chapters.

Recommendation 8

Consent is one way in which personal confidential data can be legally shared. In such situations people are entitled to have their consent decisions reliably recorded and available to be shared whenever appropriate, so their wishes can be respected. In this context, the Informatics Services Commissioning Group must develop or commission:

- guidance for the reliable recording in the care record of any consent decision an individual makes in relation to sharing their personal confidential data; and
- a strategy to ensure these consent decisions can be shared and provide assurance that the individual's wishes are respected.

5.6 Duration of consent

Professional standards and good practice

Patients can change their consent at any time. Consent is not an open-ended decision. The Review Panel has concluded that consent pertaining to the care of a person should be reviewed when any of the following criteria apply:

- The person using the service decides to remove their consent.
- There is a significant change in the person's situation e.g. a new diagnosis and/or a referral.
- After an agreed timescale, which organisations should consider and include as part of their local policies through dialogue with their patients.

Withdrawal of consent cannot be reliably made retrospectively, as information may already have been shared and acted upon. National Information Governance Board (NIGB) guidance explains why deleting records or information from records is not advisable and that in the case of electronic records, even if a record is removed the audit trail relating to that record must remain complete[45].

5.7 The deceased

There is a lack of consistency in the approach to the data of deceased people within the health and social care system. The common law duty of confidence is generally regarded as extending to the deceased but the Data Protection Act only relates to the living. Legal representatives or those with a claim on the estate of a deceased person are able to access the health records of the deceased person through the Access to Health Records Act 1990, but there is no equivalent legal route for access to social care records. Some 'work-a-rounds' are used but these are increasingly untenable[46].

[45] 'Requesting amendments to health and social care records' (NIGB), 2010 http://www.nigb.nhs.uk/pubs/amendrecords.pdf

[46] Information Rights Tribunal (General Regulatory Chamber) Case No. EA/2011/0209, Julia Martyres v Information Commissioner and NHS Cambridgeshire, 11 January 2012. http://www.informationtribunal.gov.uk/DBFiles/Decision/i653/20120131%20Decision%20and%20Ruling%20EA20110209.pdf

As people gain more control of their information, it should be possible for a person to give custodianship of their personal confidential data after their death to someone, or to a research data bank, so that future generations can use it to learn and improve the health and wellbeing of society.

The review panel concluded that the Law Commission, in their review of the legal aspects of data sharing should consider looking at how the law surrounding deceased persons might be better harmonised. In particular, the Panel would like the Law Commission to consider ensuring there are no legal impediments to giving custodianship of their health and social care data within their last will and testament.

5.8 Genetics and consent

Genetic information should not be treated any differently from other forms of information, and genetic information in itself is not always identifiable. The Human Genetics Commission[47] principles on privacy and confidentiality (2002) should be followed. These state:

- Privacy: Every person is entitled to privacy. In the absence of justification based on overwhelming moral considerations, a person should generally not be obliged to disclose information about his or her genetic characteristics.
- Consent: Private genetic information about a person should generally not be obtained, held or communicated without that person's free and informed consent.
- Confidentiality: Private personal genetic information should generally be treated as being of a confidential nature and should not be communicated to others without consent except for the weightiest of reasons.
- Non-discrimination: No person shall be unfairly discriminated against on the basis of his or her genetic characteristics.

5.9 The NHS Constitution

The Review Panel proposes that alongside giving due regard to consent, professionals and staff within health and social care should adhere to the rights, pledges and duties set out in the NHS Constitution.

The Review Panel recommends that these rights, pledges and duties be extended to include the whole health and social care system, which includes but is not limited to the NHS, public health, researchers and local authorities. If it was extended in that way, it would read as follows:

- **You have the right** of access to your own records and to have any factual inaccuracies corrected.
- **You have the right** to privacy and confidentiality and to expect the health and social care system to keep your confidential information safe and secure.
- **You have the right** to be informed about how your information is used.
- **You have the right** to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

[47] 'Inside Information: Balancing interests in the use of personal genetic data. A summary report by the Human Genetics Commission', May 2002 http://genome.wellcome.ac.uk/doc_WTD020971.html

The NHS and adult social services also commit:

- to ensure those involved in your care and treatment have access to your health and social care information so they can care for you safely and effectively (pledge);
- to anonymise the information collected during the course of your care and treatment and use it to support research and improve care for others (pledge);
- where identifiable information has to be used, to give you the chance to object wherever possible (pledge);
- to inform you of research studies in which you may be eligible to participate (pledge); and
- to share with you any correspondence sent between staff about your care (pledge).

Staff duties:
You have a duty to protect the confidentiality of personal information that you hold.

You should aim:

- to inform patients about the use of their confidential data and to record their objections, consent or dissent; and
- to provide access to a patient's data to other relevant professionals, always doing so securely, and only where there is a legal and appropriate basis to do so.

Recommendation 9

The rights, pledges and duties relating to patient information set out in the NHS Constitution should be extended to cover the whole health and social care system.

6 Research

6.1 Why researchers need patient information

Patient information is an exceptionally valuable resource for researchers, with great potential to improve healthcare, both for individuals and populations. For example researchers use data to understand more about the causes of disease, assessing new clinical tests, treatments and interventions, and test the safety and effectiveness of drugs and medical devices.

The existence of the NHS provides a huge advantage to medical researchers in the UK. As a universal service free at the point of use, the NHS has a deep well of data covering almost all of the population, across the full spectrum of medical conditions. In December 2012 the Government announced a £100m programme aimed at sequencing the whole genome, the personal DNA sequence, of up to 100,000 cancer patients and patients with rare inherited diseases being treated by the NHS. The aim is to both offer clinicians a better understanding of how genetic information can be used to improve diagnosis and to develop new treatments. The size of the NHS population is also invaluable for research into infectious diseases.

There is also enormous untapped potential in the information captured in social care records to support better research. Social care record information is traditionally underexploited, in large part due to the difficulties in pooling social care information across providers and commissioners.

Using this data, researchers can provide direct benefit to individuals who take part in medical trials and indirect benefit to the population as a whole. The Government is well aware of this contribution and the Prime Minister wants expansion of healthcare research to boost the life sciences industry, which is already worth £50bn in turnover a year and employs 160,000 people[48].

The increasing use of electronic records opens up possibilities to conduct whole population observational studies and to address new research[49] questions by linking different data sets together. Patient records can also be used to identify people to invite them to take part in clinical trials and other interventional studies. The Review Panel looked into how these opportunities might be realised without weakening confidentiality and trust.

[48] Strategy for Life Sciences, BIS, http://www.bis.gov.uk/assets/biscore/innovation/docs/s/11-1429-strategy-for-uk-life-sciences

[49] As defined in '*Research Framework for Health and Social Care*', Department of Health (2005)

6.2 Maintaining confidentiality and trust

The balance of evidence suggests that the majority of patients and the public support research in health and social care[50], and the use of anonymised patient data to support research. Where identifiable data is needed for research, patients are content to be approached to participate in research studies by their clinicians, but patients and public do want to be asked for their consent before their identifiable information is disclosed for a given piece of research[51].

However, the Review Panel has heard that more could be done to increase awareness of the benefits of research, what it entails, and how health and social care information may be used to support it[52]. It is therefore vital that in order to improve and maintain public trust, researchers and the health and social care system more generally, must inform patients and the public of the benefits that the use of their information can bring to them, their families and the nation's health.

This should include raising awareness and understanding of how information about apparently 'well' individuals is just as important as information about patients with particular conditions e.g. for the comparison of health outcomes and the identification of risk factors.

It is also important to inform people how they can become involved in different types of research, about the rights they have in relation to the use of their information for research and how to exercise them, including when they can actively dissent (i.e. withhold their consent).

Section 5.5 of this report, 'The "data sharing model"', discusses the need to inform patients and the public of how their information is used in health and social care and sets out the Review Panel's conclusions and recommendations on this issue.

The Review Panel heard from researchers that the complexity, confusion and lack of consistency in the interpretation of legal and governance requirements can sometimes hamper research. The tendency is for data controllers to be risk-averse, erring on the side of caution rather than of public benefit. Researchers called for a more proportionate and streamlined framework to enable easier access to data.

Researchers have devised a number of robust solutions to enable access to detailed patient information, while ensuring confidentiality is protected. These solutions have been developed over many years and are still evolving. The remainder of this section discusses the approaches.

---

[50] Public attitudes to research governance: A qualitative study in a deliberative context, http://www.wellcome.ac.uk/stellent/groups/corporatesite/@policy_communications/documents/web_document/wtx038443.pdf

[51] Special Eurobarometer (EB) 359, *Data Protection and Electronic Identity in the EU* (2011), page 155, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[52] Ipsos MORI/MRC The Use of Personal Health Information in Medical Research General Public Consultation (June 2007), www.mrc.ac.uk/utilities/Documentrecord/index.htm?d=MRC003810

6.3 Protecting the identity of individuals

Using information that does not identify individual patients is the surest way to protect confidentiality. Whenever possible, anonymised data should be used for all purposes other than direct care, including research. However, the Review Panel has found that while from a legal perspective, patient data exists in one of two forms – with patients either identified[53] or anonymous, in reality, the situation is more complex. In particular, there is a 'grey area' of data that on its own, does not identify individuals, but could potentially do so if it were to be linked to other information.

Clearly, it is inappropriate to publish information that could lead to individuals being identified. Therefore, the processing and disclosure of information with a high risk of re-identification requires robust protection and governance. As with other areas of information governance, the Review Panel found that there is great variation and inconsistency in the language used to describe different kinds of information, for example using terms like 'personal' or 'identifiable' interchangeably to describe the same thing, or using the same term to mean slightly different things.

The Review Panel proposes a simple framework that describes three different forms of data and clarifies the conditions under which data can be processed and disclosed (see figure 1 over the page). This framework draws on the Information Commissioner's Office Anonymisation Code of Practice, published on 20th November 2012. In summary, the three states of data in the framework are:

'Data for publication'

This is data that has been anonymised in line with the ICO anonymisation code to the point where determining individual identities from the data is unlikely, requiring unreasonable effort. The data does not require a legal or contractual basis for processing and can be publically disclosed. This data is called de-identified data for publication.

'Personal confidential data'

This is data in which individuals are clearly identified, or are easily identifiable. This data should not be processed without a clear legal basis[54].

Personal confidential data should only be disclosed with consent or under statute[55] and any disclosure must always be limited and accompanied by a contractual agreement that mitigates the risk of misuse and inappropriate disclosure. The contractual agreement needs to set out, as a minimum, the legal basis for the data flow, the purposes to which the data can be put, the safeguards that should be in place to protect data and how the public are informed about these.

The linkage of personal confidential data from more than one organisation for any purpose other than direct care, should only take place in specialist, well governed, independently scrutinised accredited environments called 'accredited safe havens' (see section 6.5).

[53] i.e. 'Personal data' as defined in the Data Protection Act 1998.

[54] The legal basis for personal confidential data must conform with the Data Protection Act 1998 and common law duty of confidentiality.

[55] While the public interest can also provide a legal basis for disclosure it should not be relied upon for routine data flows (see also section 8.6 and recommendation 12).

‘Data for limited disclosure’

This data is called **de-identified data for limited disclosure or access**. This is data that has been through a process of anonymisation such as removing formal personal identifiers, or using coded references or pseudonyms in their place, or by aggregating data together so it is not possible to identify individuals. However, it would be relatively straightforward for a third party to re-identify individuals or de-anonymise the data, especially if combined with other data. This represents the ‘grey area’ of data.

This data should only be disclosed in accordance with the ICO Anonymisation code of practice. The disclosing and processing of this data must always have safeguards for limited access that have two components, a contractual agreement and a set of data stewardship functions.

The contractual agreement mitigates the risk of re-identification and sets out as a minimum the justification for the data flow, the purposes to which the data can be put, the penalties and liabilities and how the public are informed.

The data stewardship functions should include, but not be limited to, the technical and organisational security arrangements for security, human resource policies such as contractual obligations, any training requirements and data retention policies. A key challenge is establishing conformance to the data stewardship functions, while enhancing a vital research and innovations community.

The Review Panel concluded that where de-identified data for limited access is processed, assurance of the data stewardship component could be achieved in a number of ways, including but not necessarily limited to:

- **establishing the receiving organisation as an accredited safe haven (see section 6.5);**
- **using the facilities of an accredited safe haven; and**
- **volunteering for an audit from the ICO.**

Furthermore any data breach could result in a formal ICO investigation.

As with personal confidential data, the linking of de-identified data for limited disclosure or access from more than one organisation for any purpose other than direct care must only be done in ‘accredited safe havens’ (see section 6.5).

If it is not possible to meet both the contractual and data assurance criteria, then de-identified data for limited disclosure or access must be treated in the same way as personal confidential data, only being disclosed with either consent or under statute.

Figure 1: Simplified framework of data processing from a legal perspective

Class of data according to ICO code	Status of data	Description*	Legal basis required for processing?	Need to inform Public?	Conditions for onward disclosure
Anonymised	De-identified data for publication	Personal confidential data which has been anonymised with a low residual risk of re-identification. This means third parties can only re-identify the persons with unreasonable effort.	Not applicable	Desirable	No conditions for disclosure. Data may be published.
	De-identified data for limited disclosure or limited access	Personal confidential data that has been anonymised but with a residual high risk of re-identification. This means that the data does not identify persons on its own, but there is a significant risk that third parties could re-identify the persons with reasonable effort. A defining characteristic is a data set containing a single identifier such as NHS number or postcode**.	Legal basis requires safeguards that maintain anonymity. This means: • a contract that prevents re-identification; and • assured data stewardship arrangements***. Linkage of this data from more than one organisation for any purpose other than direct care must only be done in the Health and Social Care Information Centre OR an accredited safe haven.	Recom-mended	Either as de-identified data for publication OR to an environment covered by the same contractual arrangements as the disclosing party and confirmed data stewardship arrangements.
Identifiable	Personal confidential data	Personal confidential data that has not been through anonymisation and that may or may not have been redacted. Examples include: • any data set with greater than one direct identifier** OR • pseudonymised data with access to key for reversibility OR • pseudonymised data and holding one or more of source data sets in identified form.	Legal basis for processing is required that meets the common law duty of confidentiality, Human Rights Act 1998 and Data Protection Act 1998. This means: • consent OR • statute OR • exceptionally on public interest grounds. Linkage of this data from more than one organisation for any purpose other than direct care must only be done in an accredited safe haven.	Required unless exempt	With consent for direct care OR under statute OR anonymised AND with appropriate contract or agreement***.

* Please refer to ICO Anonymisation: Code of Practice with any associated health and social care system specific information governance statements or standards for detailed documentation support.

** Appendix 5 contains a list of direct identifiers. Named data should be regarded as personal confidential data.

*** Appendix 6 provides further detail on contracts.

6.4 Pseudonymising data at source

Pseudonymisation at source is a process that replaces identifiers in a data set with a coded reference or pseudonym so information about an individual can be distinguished without their 'real-life' identity being revealed. If the process of pseudonymisation is 'enterprise wide', meaning it is standard across the whole health and social care system, it is then possible for it to be safely linked with another data set and the identity of the individual protected. The Review Panel heard evidence that the health and social care system should adopt a single mechanism to pseudonymise data at the source it is collected and consider seriously an enterprise-wide pseudonymisation at source, in theory allowing improvements in linkage, protection of data and the use of information for activities such as service improvement.

The Review Panel heard evidence that the banking and card payment industry have a duty of care to protect the identity and sensitive data of clients. Following significant investment a Banking and Payment Card Industry Data Security standard[56] was adopted in 2010. The health and social care system has a similar duty of care and could consider adopting a similar single standard.

However, there is a lack of clarity as to the costs, risks and benefits involved in adopting such a system for the whole of health and social care. The Review Panel concluded that there should be an evaluation of benefits, costs, risks and management issues of adopting such a system (or systems).

6.5 Accredited safe havens

There is one particularly challenging area from a privacy perspective, which is linking data sets. Effective linkage must ensure that data for the same individual is brought together from two or more data sets. This usually requires personal data.

The *Data Sharing Review*[57] (Thomas and Walport) stated that 'safe havens' "should be developed as an environment for population based research and statistical analysis".

The Review Panel recommends that data sets containing personal confidential data, or data that can potentially identify individuals (de-identified data for limited disclosure or limited access), are only disclosed for linkage in secure environments, known as 'accredited safe havens'. The purposes for such linkage should be expanded to cover audit, surveillance and service improvement.

Within the accredited safe haven, de-identified data for limited disclosure or access must not be linked to personal confidential data unless there is a clear legal basis to do so, and contracts must forbid this. This would re-identify the de-identified data for limited access, and be a data breach.

[56] https://www.pcisecuritystandards.org/security_standards/index.php

[57] Data Sharing Review, Thomas and Walport, July 2008. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf

The Health and Social Care Act 2012 provides primary legislation for the creation of an accredited safe haven, called the Health and Social Care Information Centre (Information Centre, see section 1.8).

The amount of data linkage required by the new health and social care system may be beyond the resources of the Information Centre as currently envisaged. Additionally, much of this linkage may be required at a local level, which is at odds with the Information Centre's national focus. This gives rise to the question of whether further accredited safe havens will be required to support the health and social care system.

The Review Panel has found there are plans for at least 20 accredited safe havens. These include safe havens within Royal Colleges, National Clinical Audit contract holders, approximately 10 Data Management Integration Centres (discussed in more detail in the Commissioning chapter), Public Health England[58] and the Clinical Practice Research Datalink service of the MHRA. These accredited safe havens will need a clear legal basis to link data[59]. Being an accredited safe haven does not necessarily mean that the organisation is receiving personal confidential data, but does mean it can receive de-identified data for limited disclosure or limited access.

Recommendation 10

The linkage of personal confidential data, which requires a legal basis, or data that has been de-identified, but still carries a high risk that it could be re-identified with reasonable effort, from more than one organisation for any purpose other than direct care should only be done in specialist, well-governed, independently scrutinised and accredited environments called 'accredited safe havens'.

The Health and Social Care Information Centre must detail the attributes of an accredited safe haven in their code for processing confidential information, to which all public bodies must have regard.

The Informatics Services Commissioning Group[60] should advise the Secretary of State on granting accredited status, based on the data stewardship requirements in the Information Centre code, and subject to the publication of an independent external audit.

[58] From 1st April 2013, a number of organisations will exist within Public Health England that will link data using section 251 as the legal basis. These include cancer registries, registries for other diseases such as congenital anomalies, and health protection (see also section 8.6 and recommendation 12).

[59] The Health and Social Care Act 2012 provides the legal basis for the Health and Social Care Information Centre.

[60] The Informatics Services Commissioning Group is responsible for providing advice on commissioning informatics services across the health and social care system. Information governance is one of the key informatics services.

6.6 Governance and data stewardship of accredited safe havens

Data stewardship refers to the principles and recommended practices for the handling of data.

The Review Panel concludes that there is a need for a consistent national minimum standard of data stewardship, with the leadership (Boards or equivalent body) of organisations with accredited safe havens held accountable for any failings. This should be supported by a system of external independent audit, which is published, and an accreditation process for all organisations that act as an accredited safe haven.

Professional standards and good practice

Data stewardship requirements for accredited safe havens

The Review Panel concludes that accredited safe havens should be required to meet the following requirements for data stewardship:

- Attributing explicit responsibility for authorising and overseeing the anonymisation process e.g. through a Senior Information Risk Officer.
- Appropriate techniques for de-identification of data, the use of 'privacy enhancing technologies' and re-identification risk management.
- The use of 'fair processing notices'.
- A published register of data flowing into or out of the safe haven including a register of all data sets held.
- Robust governance arrangements that include, but are not limited to, policies on ethics, technical competence, publication, limited disclosure/access, regular review process and a business continuity plan including disaster recovery.
- Clear conditions for hosting researchers and other investigators who wish to use the safe haven.
- Clear operational control including human resources procedures for information governance, use of role-based access controls, confidentiality clauses in job descriptions, effective education and training and contracts.
- Achieving a standard for information security commensurate with ISO27001[61] and the Information Governance Toolkit (see section 12.9).
- Clear policies for the proportionate use of data including competency at undertaking privacy impact assessments and risk and benefit analysis.
- Standards that are auditable.
- A standard template for data sharing agreements and other contracts that conforms to legal and statutory processes.
- Appropriate knowledge management including awareness of any changes in the law and a joined up approach with others working in the same domain.
- Explicit standard timescales for keeping data sets including those that have been linked, which should be able to support both cohort studies and simple 'one-off' requests for linkage.

[61] ISO27001 is the international best practice standard for an Information Security Management System. See: http://www.27000.org/index.htm

6.7 Exceptional disclosure in the public interest (section 251 of the NHS Act 2006)

Sometimes researchers require specific information about individuals that cannot be anonymised or pseudonymised in a safe haven, and gaining explicit consent may be highly impractical. Legislation is in place that allows personal confidential data to be processed for medical purposes such as research.

Regulations under section 251 of the NHS Act[62], often referred to simply as 'section 251', allows the common law duty of confidence to be set aside under specific circumstances. Applicants must demonstrate that the aim of the processing is in the public interest, that anonymised information could not be used to achieve the required results, and that it would be impractical, both in terms of feasibility and appropriateness, to seek specific consent from each individual affected. For research the approval of a Research Ethics Committee is also needed. The key test is one of necessity, not convenience.

The powers under the section 251 regulations only provide relief from the common law duty of confidence. Any activity taking place with the support of section 251 must still comply in full with the Data Protection Act.

Example: difficulties obtaining explicit consent

The Academy of Medical Sciences report, 'Personal data for public good: using health information in medical research'[63], identified a number of circumstances where it may not be practicable to seek consent for the use of identifiable patient records in research:

- the risk of introducing bias that will endanger the validity of the results: certain segments of the study population may be particularly difficult to get in touch with for consent, but excluding these people could bias the sample population, causing the study to produce misleading results which may not be applicable to underrepresented groups;
- seeking consent may compromise effective population coverage;
- the size of the study population and the proportion likely to be untraceable which might make contact impracticable;
- the overall financial and time burdens imposed; and
- the risk of inflicting harm or distress by contacting people. For example, the Medical Research Council (MRC) gives the example that contacting people about a study examining correlations between parents' mental health and unexplained child deaths might cause serious distress[64].

[62] Originally enacted under section 60 of the Health and Social Care Act 2001.

[63] 'Personal data for public good: using health information in medical research', 2006, http://www.acmedsci.ac.uk/p48prid5.html#description

[64] See MRC Personal Information in Medical Research, p19.

The Health Research Authority and the Confidentiality Advisory Group

The Health Research Authority (HRA) was established in 2011 with the purpose of protecting and promoting the interests of patients and the public in health research. From April 2013, the HRA will take over the advisory functions on use of data from the Ethics and Confidentiality Committee, including applications under section 251.

As part of this, the HRA has convened the Confidentiality Advisory Group to review applications to access patient information without consent and provide expert, independent advice on whether the applications should be approved. In the case of research applications, the Confidentiality Advisory Group will provide advice to the HRA, for non-research applications the advice will be provided to the Secretary of State for Health.

As the Confidentiality Advisory Group formally replaces the Ethics and Confidentiality Committee of the National Information Governance Board on 1st April 2013, it is too early for this review to have a view on how successfully it manages the balance of risks and benefits from sharing personal confidential data.

6.8 Consent for consent

In some cases, researchers may need to access personal records to identify people with particular characteristics to invite them to take part in clinical trials and other interventional studies. The researcher must first establish a clear legal basis before they can access the data. This process is often referred to as 'consent for consent' and can present a barrier for researchers although section 251 will provide a way forward in some instances.

Professional standards and good practice

The searching of patient records for potential research subjects can be done legally by fulfilling any of the following criteria:

- The researcher gains the explicit consent of every patient with a record in the population pool being assessed.
- The search is conducted by a health or social care professional who has a 'legitimate relationship' with the patient, such as a clinician or social worker (see section 3.6).
- The search is conducted by a researcher who is part of the clinical team[65].
- The search makes use of 'privacy enhancing technologies' (see below).
- Support under section 251 regulations is granted for the research.

[65] GMC's guidance on confidentiality (2009), http://www.gmc-uk.org/mobile/confidentiality_40_50_research_and_secondary_issues (points 48 and 50)

Case study

Taken from: '*The regulation and governance of health research*', Academy of Medical Sciences (2011)[66]

Recruitment to swine flu study

In autumn 2009 the Clinical Research Network fast-tracked studies into pandemic flu in response to the high national priority given to rapid research into the disease.

In one NIHR-funded study conducted across several sites there was a need to send out questionnaires to patients who had been identified through anonymous data sets as eligible for inclusion in the study, to ask them whether they would like to consent to be involved. The involvement of the research team was required to print out address labels to send out the questionnaires. At one site the local Research Ethics Committee and university governance teams would not approve the research team having access to patient's names and addresses before they had consented to take part in the study, and therefore a member of the clinical care team was required to take on this role. Although a member of the clinical care team agreed to undertake this activity, they were unable to complete it due to other (understandable) priorities. Consequently, for that site, instead of 200 questionnaires only 30 were sent out.

'Privacy enhancing technologies' in this case means analytical computer software that can trawl clinical databases, selecting only those patients who are eligible for a specific study, and only reveal the identities of potential participants to someone with a legitimate relationship to the patient, such as their clinician or social worker. Where someone in the health and social care team is to undertake the search, the researcher (and funder) should provide adequate resource to facilitate this if necessary.

In most cases, once selected as a potential research subject patients should be contacted by an established member of their care team inviting them to take part in a study and notifying them a researcher may be in touch.

The Review Panel concludes that, wherever possible, privacy enhancing technologies should be used to minimise the need for access to identifiable information.

The approach taken by the Clinical Practice Research Datalink Service and the South London and Maudsley Trust provide examples of an approach that allows appropriate individuals to be selected and approached to take part, without giving researchers direct access to identifiable information before consent is obtained.

[66] http://www.acmedsci.ac.uk/p47prid88.html

Example: South London and Maudsley Trust safe haven

The South London and Maudsley Trust has a 'safe haven' environment that gives researchers access to de-identified data to select relevant individuals. Once the researcher has made their selections, the administrator of the patient electronic health record system then checks whether or not those individuals have provided consent to be approached about relevant research. The list of those who have given consent is then released to the researcher at one of the King's Health Partners organisations to approach the individual with details of the relevant study and obtain their consent to participate.

7 Commissioning

7.1 Context

The previous chapter explained how researchers have devised robust solutions to aspects of information governance so they can extract the information that they need without breaching individuals' confidentiality. Those arrangements took many years to evolve and are still in the process of development. By contrast, the arrangements for NHS and local authority commissioners to extract information on the health and social care service in England were in a state of rapid, comprehensive change during the period of this review.

The NHS Commissioning Board, clinical commissioning groups, Public Health England and local authorities in England were preparing to assume the responsibilities laid out for them by the Health and Social Care Act 2012 to achieve a smooth administrative transfer in April 2013. In such circumstances, it was perhaps not surprising that the Review Panel found a lack of consensus concerning the extent of the need for identifiable data to be used for commissioning purposes.

This chapter is primarily focused on the issues facing NHS commissioners and offers potential solutions for the NHS Commissioning Board and clinical commissioning groups. However, the Review Panel concludes that commissioning arrangements in local authorities and in Public Health England must adhere to the same standards, guidance and good practice and be subject to the same sanctions for poor practice as the NHS when commissioning services.

Clearly, commissioners cannot plan and implement the improvement of services unless they know a certain amount about the people using them. For example, they may want to establish new care pathways that are better suited to people's needs. Or they may need to check whether a hospital or care home has provided the services for which it is seeking payment. However, knowledge of service users need not necessarily require that commissioners know their identities. The question for this Review Panel has been how far commissioners can fulfil their responsibilities without needing personal confidential data about individuals.

In November 2012, during the course of the Review Panel's work, the Government published its mandate to the NHS Commissioning Board for the period April 2013 to March 2015[67]. Although it included no specific references to confidentiality, information governance or privacy, the mandate did contain strong references to better use of technology. In particular, it covered technology for sharing information to help people manage their own healthcare (section 2.6 of the mandate), better integrate services (section 2.9 of the mandate), reduce violence, particularly domestic violence (section 7.3 of the mandate), and support better outcomes (section 12 of the mandate).

The Review Panel concluded that all these objectives could be achieved without challenging the confidential nature of NHS services and without compromising public trust in them.

[67] Mandate to the NHS Commissioning Board, 2012, http://mandate.dh.gov.uk/2012/11/13/nhs-mandate-published/

7.2 What sort of information will commissioners need to collect?

Commissioners will need information to fulfil their responsibilities for organising a wide range of activities, including:

- procurement of services;
- financial and contract management;
- performance management of services;
- performance reporting;
- outcomes monitoring;
- patient satisfaction assessment;
- promotion of integration; and
- assurance that providers have robust processes for dealing with untoward issues, including but not limited to serious incidents, never events and data breaches.

In evidence to the Information Governance Review, representatives of the NHS Commissioning Board and clinical commissioning groups (CCGs) said there would be occasions when there would be no alternative to using personal confidential data, for example to hold the system to account or innovate to improve services.

They suggested that anonymised data would sometimes be of such poor quality that it could not be relied upon. In such circumstances, commissioners might need the data about individuals to find out the truth of the matter. Further reasons given for using personal confidential data were to allow the linkage of data from multiple sources and the need for access to more extensive data than is currently possible from the Information Centre, and much more rapidly than at present.

The Review Panel heard that the use of such data for commissioning purposes would be legitimate because it would be part of a proposed "consent deal" between the NHS and its service users. In return for receiving treatment, the patient would be agreeing to allow data to be used by the health and social care system for a variety of purposes including those under the umbrella of commissioning.

The Review Panel does not support such a proposition. If identifiable data is to be used, a clear justification and a legal basis for doing so must be established and made known to patients.

In theory, the Government could change the law to give commissioners a special dispensation to access and use personal confidential data. However any such general dispensation would not align with the rights and commitments proposed in the NHS Constitution consultation, or in section 5.9 of this report.

In order to understand the current commissioning landscape, a team from the Information Governance Review worked with a group of primary care trusts and their cluster and also co-operated with a team from the NHS Commissioning Board to identify the types of commissioning activity for which access to personal confidential data may be required. The team then investigated whether the desired outcomes could be achieved without giving such access. The results were encouraging.

7.3 Analysis of commissioning requirements for personal confidential data

The NHS Commissioning Board identified seven major commissioning challenges, which might require access to personal confidential data. These were as follows:

- Commissioning specific services for individuals might require review of their individual needs and validation to establish that those patients belong to a particular clinical commissioning group and are receiving the correct treatments.
- Aspects of service planning and monitoring on geographic criteria might require postcodes for certain types of analysis.
- Understanding populations and inequalities in outcomes might require consideration and monitoring of individual cases.
- Specialist commissioning is organised beyond local areas and might require discussions about individual patients and their associated costs.
- Ensuring appropriate clinical service delivery and process might require access to records.
- Integrated care monitoring services including outcomes and experience might require linkages across sources.
- Targeted support for patients at highest risk might require data from several sources linked together.

After thorough analysis, the Review Panel gained assurance from the NHS Commissioning Board and primary care trust colleagues that most of these challenges could be overcome without legal difficulty by using a number of techniques:

- by asking for the consent of individual patients;
- by ensuring that commissioners, when assessing performance across whole care pathways, should require the analysis to be provided by the providers as part of the contract (see figure 2 in section 12.10);
- by improving data quality; and
- by anonymising data so that commissioners can get the information they need without being able to identify individuals.

Only a small percentage of situations requiring personal confidential data remained without an immediately obvious legal basis and these were confined to a small proportion of situations. Possible solutions to these residual problems are included in sections 7.3.4 and 7.4 below.

7.3.1 Situations where commissioners can ask for patients' consent

There are a number of situations when commissioners may need personal confidential data to help people deal with specific problems. For example patients may want to ask the NHS to provide "continuing care" so they do not have to pay themselves for care in their own homes after leaving hospital. They may make "individual funding requests" for drugs that are not generally available on the NHS in that area. They may have specialist commissioning needs or other reasons why the local clinical commissioning group needs to look in detail at their individual circumstances.

In each case, the individual is asking for specific assistance and it is entirely reasonable for the NHS to ask for the patient's consent for NHS staff involved in handling the case to look at the patient's personal confidential data, without which help cannot be forthcoming.

7.3.2 Commissioning whole care pathways

Commissioners told the Review Panel that they want access to confidential personal data so they can check the quality of care at every stage of a patient pathway, as the individual moves among a series of health and social care providers. They suggested that the surest way of doing this was to look at a sample of personal files. They said this approach would be particularly helpful in specialist commissioning, which has an additional degree of sophistication. The Review Panel did not understand why the use of identifiable information was necessary.

An alternative would be to commission the whole care pathway from a consortium of providers led by a prime provider and ask for the data that demonstrates effectiveness. Another alternative, if different providers were commissioned across the care pathway, would be for the commissioner to commission audit reports on the whole care pathway from the local health and social care professionals who have a legitimate relationship to the patient. In general, it would appear that many commissioners have had little exposure to this type of performance review, which is why they ask for this data themselves.

The Review Panel concluded there did not appear to be a robust case for commissioners holding personal confidential data for the commissioning of whole care pathways and any exceptions should be argued on an individual case-by-case basis.

7.3.3 Poor data quality

Commissioners also told the Review Panel that because the quality of local demographic or administrative data is sometimes poor, they often require three identifiers[68] to ensure they are distinguishing the correct individual. This means that instead of using de-identified data for limited disclosure or limited access, for which Commissioning Support Units could have a legal basis, commissioners are reliant on personal confidential data for which they may have no legal basis.

All providers need to ensure that their patients are correctly identified by checking their data against the Personal Demographics Services in the 'Spine'[69] to improve data quality and hence remove the requirement for commissioners to have personal confidential data.

7.3.4 Using de-identified data

In order to use personal confidential data, commissioners require legal bases for both collecting and for disclosing the data to the various parties involved in the commissioning process.

[68] See appendix 5.

[69] For information on the NHS 'Spine' see: http://www.connectingforhealth.nhs.uk/systemsandservices/spine

The 2012 Health and Social Care Act 2012 established that the Information Centre will become a safe haven within which personal confidential data can be collected and de-identified without the risk of any individual's personal confidential data being disclosed. It is accepted, however, that the Information Centre will not have the capacity and capability in the foreseeable future to collect and de-identify all the information that commissioners will want to use. In particular, it is unlikely that the Information Centre will have the capacity to de-identify information that local commissioners want to extract from local providers.

The NHS Commissioning Board has set out its views on some of the information governance issues that will need to be addressed by 1st April 2013. Its vision was to streamline data collection, storage and linkage with a view to "collect once and use many times". The plan included proposals for up to 25 Commissioning Support Units (CSUs), of which, up to 10 would host Data Management Integration Centres (DMICs).

The key role proposed was for the DMIC to process personal confidential data on behalf of the clinical commissioning groups through data collection, cleaning, linking, de-identifying and making de-identified data available to their customers. The key role for CSUs would be analysis of data particularly for innovation and improvement.

The NHS Commissioning Board has been working with the Information Centre, Public Health England, Local Authorities and others to ensure that the DMICs would also support the purely local work of Public Health England and Local Authorities in relation to data collection.

To ensure that the DMICs have a sound legal basis for processing personal confidential data, representatives of the NHS organisations concerned put forward a proposal to integrate the part of the DMICs that will do this work into the Information Centre. The part of the DMIC function that moves to the Information Centre should be distinct from the DMICs and be a clearly separate service offered by the Information Centre. It is unclear, at present, whether this will fully address legal requirements.

The Review Panel have to present this report to the Secretary of State before a legally robust solution reaches maturity, and before being made aware to its satisfaction of the safeguards that will be required to give the Information Centre adequate control of information governance in their part of the DMICs. This important issue constitutes crucial unfinished business.

The Review Panel urges the NHS Commissioning Board and other commissioning bodies to adopt the following principles when the commissioning architecture as set out in the Health and Social Care Act is implemented from April 2013:

- **All personal confidential data used for commissioning purposes must be processed legally, kept to a minimum and anonymised data must be used whenever possible.**
- **Robust safeguards must be created to ensure that commissioning bodies (including their structural components e.g. CSUs and DMICs) are processing personal confidential data legally. Such safeguards include that staff from DMICs who are working in the Information Centre's Data Service for Commissioners must be accountable to and**

overseen by the Information Centre. They must work according to the rules set out for the Information Centre in the Health and Social Care Act 2012. Any necessary disciplinary action should be solely determined by the Information Centre.

- **The Information Centre's Data Service for Commissioners will process personal confidential data for DMICs and CSUs. Any other processing of personal confidential data by a DMIC or CSU must be justified according to its own definitive legal basis and is not covered by the general legal powers available to the Information Centre.**
- **There needs to be clarity about data controllership and clear lines of accountability both between data controllers, and between data controllers and the bodies they contract as data processors.**
- **The risk of unlawfulness must be reduced, if necessary by use of section 251 exceptions, but these must be kept to the absolute minimum and subject to explicit fixed time limits.**

There was one area of some confusion among commissioners. Some members of clinical commissioning groups believed it was appropriate for them to access personal confidential data because they were providing a form of direct care. The Review Panel does not believe that this is the function of clinical commissioning groups, as set out in the Health and Social Care Act 2012.

Even if commissioners could undertake some direct care they would need to establish a legitimate relationship with the patients concerned and would not be able to use section 251 of the NHS Act 2006 (see section 6.7 of this report) to utilise personal confidential data on the basis of exceptional disclosure. The Review Panel noted that section 251(6) of the NHS Act 2006 prohibits the Health Service (Control of Patient Information) Regulations from being used to require processing of confidential patient information "solely or principally for the purpose of determining the care and treatment to be given to particular individuals".

Should individual data controllers, such as GP practices, wish to use a commissioning support unit or data management integration centre as a data processor, then a robust legal framework and contractual arrangement must be in place (see section 12.10). At the time of writing, this would require a contract between the GP practices and NHS Commissioning Board, as CSUs and DMICs are part of the NHS CB. Similarly, GP practices wishing to use other services such as health informatics services as data processors would also need a robust legal framework and contractual arrangement to be in place with the acute trust or other legal entity hosting such services.

7.4 The individual's right to object

Both Article 8 of the European Convention on Human Rights and the European Data Protection Directive[70] require reasonable objections to the disclosure of personal confidential data to be respected[71]. Indeed the Review Panel noted that the Health and Social Care Act 2012 would not be adequately protected from legal challenge if it failed to be compatible with Article 8.

[70] Both Article 8 of the European Convention on Human Rights (ECHR) and the European Data Protection Directive were enacted in UK law through the Human Rights Act 1998 and Data Protection Act 1998.

[71] Where there are "compelling legitimate grounds".

In addition, the NHS Constitution reflects the patient's legal right to request that personal confidential data is not used for purposes beyond his or her care and treatment and to have any objections considered. This report proposes extending this right to cover adult social care (see section 5.9). The Review Panel noted with interest the argument that the law requires *any reasonable objection* to the disclosure of personal confidential data to be respected[72].

During the course of the review, the Review Panel heard that many people are content for their information to be used in order to help medical advances and to improve the health system. However, the Panel also heard from a small but significant minority who objected to this and who, for a variety of well-articulated personal reasons, did not want their personal confidential data used for purposes other than their direct care.

To take account of the implications of the European Convention on Human Rights, the NHS Constitution and the views of people, the Review Panel concluded that reasonable objections from individuals must be considered. To help people to make informed decisions over whether or not to object, they must be given as much information, in an accessible form, as is practicable about how their data will be used for purposes other than their direct care (see section 5.5).

The Review Panel considered the practicalities of how objections may be raised, considered and acted upon. Two illustrative examples are set out below:

Example 1

Mr S has a mental health disorder. A result of which means he believes the Government is seeking to harm him. He is attending his psychiatrist in a community clinic and reads the public information about data collections and extractions flowing from providers to the Health and Social Care Information Centre. He gets very agitated but then reads in bold large type that he can object and have his objections considered. In the dialogue with his psychiatrist it becomes apparent that if his data is sent to the Information Centre he will not attend further outpatient sessions. When challenged what he will do when he is very ill, he replies that he may have to seek the 'ultimate solution'.

The psychiatrist concludes that there is a demonstrable risk to the patient unless his objection is upheld.

In this case the risk is sufficient to satisfy the conditions in section 10 of the Data Protection Act, which states that objections should be upheld:

- if the processing is likely to cause substantial damage or distress; and
- if that damage or distress is or would be unwarranted[73].

[72] Jamie Grace, Mark JK Taylor 'Disclosure of Confidential Patient Information and the Duty to Consult: the Role of the health and Social Care Information Centre' (2013) Medical Law Review (Forthcoming).

[73] Section 10 of the Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/section/10

In the case of example 1, the effect of the patient's objection is to stop his personal confidential data flowing TO the Information Centre.

Example 2

Mr W asks his GP about the pamphlet describing the role of the Information Centre. He explains that he is 'privacy aware' and always checks the 'please don't share my data with third parties' option when registering on websites. He feels inclined to object to his information being shared with the Information Centre. The GP explains that Mr W's data would be used for research to improve medicine and to improve the health and care system and that his data will be de-identified to protect his identity. The GP adds that occasionally data could be requested in identifiable form to help a specific study or analysis, unless individuals have a particular objection to that. Mr W concludes that he is happy for data that does not identify him to be used, but he remains concerned about his identity being revealed to anyone. The GP agrees that Mr W has made a *reasonable objection* and marks Mr W's record to show that data may flow to the Information Centre, but may not leave the Information Centre in a form that could identify him[74].

Whether or not the disclosure of Mr W's identity would have caused him 'substantial damage and distress' within the meaning of section 10 of the Data Protection Act, Mr W's rights under Article 8 of the European Convention on Human Rights might have been infringed without this attention to his objections.

In the case of example 2, the effect of the patient's objection is to stop his patient identifiable data flowing FROM the Information Centre.

Standards and good practice

The Review Panel concluded that the process for considering objections should:

- **explicitly include the most senior registered and regulated health and social care professional caring for that individual;**
- **explicitly include in the consideration whether not supporting the objection will damage the effectiveness of care;**
- **explicitly include whether there is a demonstrable risk that the safety of the patient will be reduced by not upholding the objection; and**
- **explicitly include whether there are compelling legitimate grounds relating to the individual's situation.**

[74] There are exceptions to this where it is in the public interest to do so.

If after due consideration the objection is upheld, there are two courses of action:

- If an individual has objected to their personal confidential data flowing TO the Information Centre (as in example 1 above), the provider must NOT pass on the individual's personal confidential data to the Information Centre.
- If an individual is content for their personal confidential data to flow TO the Information Centre, but not content for their personal confidential data to flow FROM the Information Centre (i.e. be disclosed as in example 2 above), the GP or other service provider must ensure the objection is noted in the individual's record. In addition, an objection 'flag' must be transmitted to the Information Centre in any subsequent collections.

The objection 'flag' will be used by the Information Centre to determine whether that individual's data may be disclosed from the information centre using statutory gateways.

The Review Panel concluded that whenever new permissive statutory gateways are enacted, or whenever new support under section 251 regulations is granted, an explicit decision must be taken on how patients who have had an objection upheld will have their concerns addressed.

In general, these types of disclosures should respect the individual's objection 'flag'. However, there may be occasions when it is inappropriate to do so, based on 'an alternative necessity'[75]. If the Information Centre decides to overrule objections and permit a disclosure, it must publish the decision and the reason for it in a form that is easily accessible by the public but without identifying the individual. The detail of this process should be described and published as part of the Information Centre's code of practice in processing confidential information.

In order to establish a fair and consistent objection process, the Review Panel concluded that the number of objections at provider and practitioner level should be kept under review.

The Review Panel also concluded that the Information Centre, in conjunction with key stakeholders, should regularly review objection statistics and other evidence as part of a continuing process for ensuring fairness and consistency. Criteria by which to assess reasonable objections should be independently reviewed on an ongoing basis.

[75] The word necessity is used as there may be valid exceptions, e.g. emergencies under the Civil Contingencies Act 2004, health protection and even sometimes potentially under 251, e.g. for research into child abuse.

Recommendation 11

The Information Centre's code of practice should establish that an individual's existing right to object to their personal confidential data being shared, and to have that objection considered, applies to both current and future disclosures irrespective of whether they are mandated or permitted by statute.

Both the criteria used to assess reasonable objections and the consistent application of those criteria should be reviewed on an ongoing basis.

7.5 Disclosure of data from the Information Centre to commissioners

The remaining sections of this chapter are written on two assumptions. The first is that the Data Services for Commissioners functions relating to personal confidential data are integrated into the Information Centre, and are therefore not a function of the DMICs (see section 7.3.4). The second is that when an individual has objected to their personal confidential data being released from the Information Centre, and this objection has been upheld, then their wishes will be respected as set out in out in section 7.4.

The Information Centre needs to process data in line with the Health and Social Care Act (paragraphs 260—262), the Data Protection Act, the Human Rights Act and as set out in figure 1 in section 6.3 of this report.

Although the Health and Social Care Act provides statutory authority for the Information Centre to collect data, it only provides authority for some specific disclosures of personal confidential data[76].

Generally speaking, the Information Centre will only disclose anonymised and aggregated data sets. Without explicit patient consent, any other disclosure can only happen through a statutory gateway or with specific section 251 approval[77].

The Information Centre can also disclose data sets with a single identifier to accredited safe havens where it is covered by an effective contract with liabilities and penalties (see 'De-identified data for limited disclosure or limited access' in figure 1 in section 6.3). This is to safeguard against re-identification and onward disclosure. Where the context poses unusually high risks of re-identification, the data should be treated as if it were personal confidential data and support under section 251 regulations may be considered to provide the appropriate legal basis.

[76] Under section 261 of the Health and Social Care Act 2012.

[77] Or exceptionally on public interest grounds in line with section 261(5) and (6) as the common law duty of confidence continues to apply in these circumstances.

There is a potential issue in that when 'health service bodies' contract with one another, the contracts are not legally enforceable[78]. Consequently, there is no effective deterrent preventing organisations linking and re-identifying de-identified data and thereby re-creating personal confidential data. In order to overcome this problem, the review panel concludes that new regulations under section 251 of the NHS Act 2006 are considered to provide more targeted support for the disclosure of de-identified data for limited access. The purpose of such regulations would be to ensure that if the contract was not adhered to, it would break the terms of the regulations, and consequently would be a breach reportable to the Information Commissioner's Office.

For the rare occasions where commissioners justifiably require personal confidential data (see principles in 7.3.4) and no other options are available, then the existing section 251 regulations could be used to support the disclosure provided approval is granted[79].

If implemented effectively, the breaching of any the safeguards highlighted in this section will be unlawful and an automatic breach of the first principle of the Data Protection Act 1998 that would need to be reported to the Information Commissioner's Office (see section 12.10).

7.6 Competence of commissioning with regard to information governance

The 'Standards for members of NHS boards and clinical commissioning group governing bodies in England' produced by the Professional Standards Authority during the period of the review includes a technical competence section relevant to information governance. This states that members should:

> *"[respect] … patients' rights to consent, privacy and confidentiality, and access to information, as enshrined in data protection and freedom of information law and guidance*[80]*."*

The Review Panel concludes it is vital that the leadership of the Department of Health, NHS Commissioning Board (including leadership within the Commissioning Support Units and Data Management Integration Centres), clinical commissioning groups, Public Health England and local authorities ensure their organisations have due regard for the legal and statutory framework of information governance[81].

---

[78] Health Service Body contracts are defined under s9 of the National Health Service Act 2006 [which re-enacts S4 of the NHS Health Service and Community Care Act 1990 ('the NHSCCA'). The expression 'NHS Contract' means an arrangement under which one health service body arranges for the provision to it, by another health service body, of goods or services which it reasonably requires for the purposes of its functions. In addition, subsection 5 states: "it must not be regarded for any purpose as giving rise to contractual rights or liabilities." The means that a breach in the contract is a painless event for the NHS as the contract is not enforceable. This raises the issue of whether NHS contracts are adequate to satisfy the 7th Data Protection principle. The Information Commissioner's Office has advised that they are not adequate, at least in relation to contracts with data processors. Additionally, because health service bodies have access to data and services which can be used to re-identify individuals from the de-identified data there is a need for legal safeguards to prevent re-identification in order to satisfy both common law and data protection requirements.

[79] Via application to use the class support mechanism under regulation 5 which will be considered in the first instance by the Confidentiality Advisory Group of the Health Research Authority, which will make a recommendation to the Secretary of State for Health.

[80] http://www.professionalstandards.org.uk/library/document-detail?id=89114436-21e2-47df-b5a0-7d5308b66b8e

[81] Should Commissioning Support Units become legal entities in their own right, they too should have regard to the legal and statutory framework for information governance.

The boards or equivalent bodies of these organisations must take responsibility for ensuring that the organisation contains the required competence and capability in information governance practice, and that information governance is a part of organisation risk management.

Recommendation 12

The boards or equivalent bodies in the NHS Commissioning Board, clinical commissioning groups, Public Health England and local authorities must ensure that their organisation has due regard for information governance and adherence to its legal and statutory framework.

An executive director at board level should be formally responsible for the organisation's standards of practice in information governance, and its performance should be described in the annual report or equivalent document.

Boards should ensure that the organisation is competent in information governance practice, and assured of that through its risk management. This mirrors the arrangements required of provider trusts for some years.

8 Public health

8.1 A hybrid system

Protection and improvement of the nation's health are prime objectives of health policy. Public health has been left to a later chapter of this report not because of its relative importance, but because of its overarching spread and complexity. In information governance terms, it is a hybrid of the various systems covered in previous chapters.

There are three 'domains' of public health, and the legal basis for staff to handle information about people differs across the domain boundaries. They are:

- health protection, including prevention, control, communication and surveillance from infectious diseases, environmental hazards and emergency preparedness;
- health improvement, including contributing to increased life expectancy and healthier lifestyles as well as reducing inequalities in health and addressing the wider social determinants of health; and
- health services, including assisting those who plan healthcare to understand the health profile and health needs of the local population, and plan services to meet those needs, as well as evaluating how successful services are in meeting needs.

8.2 Sharing information for health protection

Healthcare professionals who are responsible for health protection sometimes need to know personal confidential data about specific individuals. For example during an outbreak of an infectious disease, public health staff may need to identify people who are at risk, perhaps because they have not been vaccinated, or because they have been exposed to an infectious disease or environmental hazard.

This side of public health work resembles the direct care of patients and service users that was considered in chapter 3. While engaged on this work, healthcare professionals can be considered to have a legitimate relationship with people in the communities they serve. It would be impractical for them to ask everyone at risk from an infectious disease to give specific consent for staff to provide appropriate information and care. Furthermore, it would not be the most effective way of bringing the infection under control. This is not a problem. They have statutory support for these activities through the Health Protection (notification) (and related) regulations 2010[82] and the Health Service (control of patient information) regulations 2002[83].

Section 8.7 below considers the implications for members of the public health staff who are not registered and regulated healthcare professionals.

[82] http://www.legislation.gov.uk/uksi/2010/659/contents/made, http://www.legislation.gov.uk/uksi/2010/658/contents/made, http://www.legislation.gov.uk/uksi/2010/657/contents/made

[83] http://www.legislation.gov.uk/uksi/2002/1438/made?view=plain

8.3 Sharing information for health improvement and research

With the exception of screening programmes[84], most health improvement activities in public health do not require personal confidential data about individuals. However, understanding the complex relationships that exist between environment, personal behaviours and disease occurrence and outcome requires information that can only be derived by linking data from several different sources, for example dietary data being linked to data on heart disease. Sufficient data is required to distinguish one person from another and avoid double counting. However, this does not mean the person must be identifiable.

De-identified information (see section 6.3), which can allow an individual to be distinguished, but not identified, may sometimes be necessary for some public health intelligence analyses, or to enable standardisation in statistical terms, so that biases and spurious results/conclusions are avoided.

There is general recognition that research that uses patient information is in general subject to rigorous governance processes (such as scrutiny by ethics committees) that provide important reassurance to the public and to professionals. There is no reason why the public should not be given similar confidence in the use of their information for these public health purposes.

There are other areas of commonality in a rigorous approach between research and aspects of public health. For example:

- Epidemiology, which requires scientific rigour, underpins both surveillance and health review.
- Although research tends to be time-limited and surveillance continuous, a continual test of utility could be applied.
- Both of these utilise peer review and funding is usually obtained through business cases which are subject to rigorous review including the information governance and security arrangements.

However, a key difference is that public health intelligence is in general based on what is already known, and is intended to improve health directly.

The Panel concluded that Public Health Intelligence should seek to use anonymised data (see section 6.3) wherever possible, and should be treated like research from an information governance standpoint when it is not using de-identified data for limited disclosure or limited access.

[84] In this report, 'screening' is defined as a special public health activity that requires access to both demographic and to clinical or other forms of personal information to ensure the correct individuals are included. Examples include programmes to screen groups of people for specific diseases such as breast cancer or eye disease caused by diabetes (diabetic retinopathy). Screening programmes should have unequivocal support from NICE, ideally through the National Screening Committee to ensure that the benefit of screening the individuals concerned outweighs any potential harm due to loss of autonomy in relation to their data.

8.4 Sharing information for commissioning

The public health function that exists within local authorities must support commissioning activity for the local authority itself, and for the clinical commissioning groups within the area. To support the 'assess, plan, do, review' cycle, some patient level detail is needed, but patients themselves to not necessarily need to be identified.

Epidemiology, planning and analysis of socio-economic factors such as gender, ethnicity and deprivation to ensure equality of service delivery are key parts of commissioning and public health. In addition, the information that supports both public health in practice and commissioning is derived from the same patient data, This aspect of commissioning can therefore be seen as a process that, like public health, seeks to improve population level health.

The Review Panel concluded that there is a need for greater clarity as to how the analysis of data for public health relates to the analysis of data for commissioning; in order to prevent overlap and duplication.

8.5 Emergency planning and response

Public Health England will be a lead organisation in planning for and responding to emergency situations. This activity requires information to be shared across boundaries and between different organisations[85].

The Cabinet Office publication '*Data Protection and Sharing — Guidance for Emergency Planners and Responders*' provides guidance on protecting personal information in these emergency circumstances. This document has been endorsed by the Ministry of Justice, the Information Commissioner's Office, the Department of Health, the Local Government Association and the Association of Chief Police Officers among others[86].

8.6 Legal and regulatory issues

The Review Panel also found a lack of coherence in regulations across the public health arena. Some registries, including cancer registries, have a regulatory basis and are covered by the Health Service (Control of patient information) Regulations 2002. Other registries operate on a basis of consent. Health Protection functions are also largely covered by these regulations but not wider public health functions, as there is no immediate risk to others' health. There are also the Sexual Health Directions 2000 prohibiting the disclosure of information relating to sexually transmitted diseases, other than for treatment and prevention.

The Review Panel recognises the need for a better balance in these regulations across public health or at least across surveillance, tempered with the need to minimise the use of personal confidential data. Those aspects of public health that relate to health of populations should be reviewed for potential inclusion in Regulation 3 of the Health Service (Control of patient information) Regulations 2002[87].

[85] There is statutory support, both mandatory and permitted for such sharing under the Civil Contingencies Act 2004.

[86] https://www.gov.uk/government/publications/data-protection-and-sharing-guidance-for-emergency-planners-and-responders

[87] http://www.legislation.gov.uk/uksi/2002/1438/made?view=plain

Recommendation 13

The Secretary of State for Health should commission a task and finish group including but not limited to the Department of Health, Public Health England, Healthwatch England, providers and the Information Centre to determine whether the information governance issues in registries and public health functions outside health protection and cancer should be covered by specific health service regulations.

8.7 Non-regulated staff

There are a number of ways in which public health staff may require access to personal confidential data. Section 8.2 explains how healthcare professionals and staff working in health protection could be considered to have a long-term 'legitimate relationship' with patients and, by definition, a right to access and use their clinical information.

However, not all staff working in health protection are regulated professionals. These staff should be dealt with as set out in section 3.7.

Some public health staff provide direct care for example undertake screening or immunisation as providers, they too should be dealt with as set out in section 3.7.

Occasionally public health staff working in other areas of public health will need access to personal confidential data. In these situations their organisation needs to have a legal basis for holding the data and if they are linking data they should be employed in an accredited safe haven.

9 Education and training

9.1 The current situation

Across the health and social care system, most staff are required to undertake annual training in information governance. The commitment to this training is important and the associated training budget is a welcome enabler in organisations facing pressures on costs.

However, evidence to the Review Panel showed that rather than being a process of education to enable staff to both protect data, and make informed decisions about sharing information appropriately in the interests of patient care, the mandatory training is often a 'tick-box exercise'. Although mandatory training such as the online NHS Information Governance Training Tool[88] may provide an introduction to some information governance issues, this 'one size fits all' approach is too often focused on processes and policies in organisations, especially around data security. One nurse described the experience as equivalent to an annual 'sheep dip', which staff could go through without thinking. In fact it is possible to pass the training tool by answering the questions at the end without bothering to read the text.

In addition to the basic, mandatory training on information governance, some staff such as information governance leads and Caldicott Guardians receive much more advanced education and training. However, the Review Panel found there is often nothing in between these to allow staff to develop a level of understanding appropriate to their role. This lack of understanding often means staff do not have the ability or confidence to appropriately share information with others, especially with staff in other organisations. The Review Panel also heard that when staff such as clinicians or social workers seek advice from their managers or even information governance leads, they are often told not to share as the 'safe option', even in cases where sharing is appropriate.

To address these concerns, the Review Panel concludes there needs to be a fundamental cultural shift in the approach to learning about information governance across health and social care, to ensure appropriate sharing of information is seen as an enabler of better patient care.

9.2 Education and training for health and social care professionals

The Review Panel concludes that there needs to be a greater emphasis on ensuring health and social care professionals take ownership of the underlying principles of information governance, rather than simply receive training in processes for sharing of information. As part of this, education of professionals needs a properly balanced focus on the benefits of safe sharing, not just on the risks of inappropriate sharing and should be a continuous process throughout the professional's career.

The Review Panel concludes that health and social care professionals should have formal information governance education focused on their roles, and this should be at both undergraduate and postgraduate level. This education should include a

[88] https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

professional component explaining why there may be a duty to share information in the interests of the patient, as well as the legal aspects around common law of confidentiality the Data Protection Act and Human Rights Act.

Undergraduate level education should cover confidentiality requirements, record keeping, information technology and systems, and the application of informatics principles to practice. The postgraduate level would cover aspects of law, professional standards and how to anonymise data. Employers should provide continuous professional development of information governance knowledge within each organisation. Professional bodies, trade associations and specialist societies must also take greater ownership of this agenda, so information governance is not seen as a management task.

Health and social care professionals and their professional bodies should be adapting their learning for modern situations. For example, one of the most important step changes in learning will be that associated with record access across all sectors of health and social care in the next 10 years. If possible, professional guidance should be consistent across all professions so that patients and the public have one standard of excellence. In addition, the use of multi-disciplinary and multi-agency training could help improve professionals' understanding of information governance issues faced by their peers.

Recommendation 14

Regulatory, professional and educational bodies should ensure that:

- information governance, and especially best practice on appropriate sharing, is a core competency of undergraduate training; and
- information governance, appropriate sharing, sound record keeping and the importance of data quality are part of continuous professional development and are assessed as part of any professional revalidation process.

9.3 Education and training for non-registered staff

The Review Panel has found that in many cases, staff are not provided with sufficient education and skills in information governance to enable them to make informed decisions and judgements in their day-to-day work. The Review Panel concludes information governance needs to be embedded into organisational culture and not seen as a peripheral role carried out by specialist staff. To support this, information governance should be integrated into core education and training, and not seen as a stand-alone topic. A greater degree of variety in the delivery of education would be beneficial and, as with regulated and registered professionals, education and training should be role based and contextualised with real-life examples relevant to staff roles.

Information governance training should be focused on improving knowledge and understanding and help instil the ethos that in some cases, especially for direct care, sharing information can be as important as protecting privacy.

There should be a mandatory minimum standard of information governance training, but staff should not be compelled to take the mandatory training if they can demonstrate they have completed suitable alternative training and education at an equivalent or higher level.

All health and social care staff should be competent in sharing information in cases of concern around vulnerable adults. The Review Panel strongly supports the ICO's ambitions to have information rights and the handling of personal data included within the national vocational qualification curriculum.

The Review Panel concludes it is vital that senior managers understand the practical information governance challenges staff face. They should demonstrate continuous professional development in information governance in at least 3-year cycles. Development of senior managers should have a high minimum standard, and senior managers should participate in education with regulated professionals, information governance specialists and Caldicott Guardians.

9.4 Information governance staff

Every individual who works in a health and social care organisation should have an appropriate level of competence in the sharing of information. However, some staff are required to have a greater level of competence in order to help others, develop policy and practice within the organisation and most importantly help resolve issues and manage risks of data sharing. Broadly speaking there are three types of specialist staff: Caldicott Guardians, Senior Information Risk Owners and Information Governance Leads.

9.4.1 Caldicott Guardians and Senior Information Risk Owners

Caldicott Guardians were recommended by the *Review of the Uses of Patient-Identifiable Information* chaired by Dame Fiona Caldicott in 1997. They were defined as:

> *"A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information."*

The Review Panel heard that Caldicott Guardians held important roles, which when done well, provided much value to their organisations and to patients. However the picture was mixed and the variation was most often related to the competencies and time available to the individuals undertaking these roles. The picture was further complicated by the fact that the Caldicott Guardians were dealing with increasingly complex challenges, in which there was no obvious correct answer. Finding a solution to these problems requires judgement, often based on discussion and reflection. Similarly, there was concern about the education and understanding of Senior Information Risk Owners about their roles.

The Review Panel concludes that in addition to the standard training and education, Caldicott Guardians should demonstrate continuous professional development in information governance on an annual basis. Furthermore, they should be encouraged not only to work with their information governance leads but also with Caldicott Guardians and Senior Information Risk Owners in other organisations, for example to help manage conflicts of interest.

9.4.2 Leadership on information governance within organisations

The Review Panel heard that information governance is often the responsibility of one person within organisations, and specialist information governance staff often felt isolated from other functions. The role of the information governance lead is often perceived to be to keep the organisation out of trouble by preventing any breaches rather than being a source of knowledge and guidance for staff. This can sometimes be to the extent of clinical decisions being overruled on 'information governance grounds'.

The Review Panel found information governance staff tended to have backgrounds as health and social care professionals, information specialists or management or legal services staff. However, there is little consistency in the competence and experience of information governance staff across the health and social care system. In many cases, the role is filled by inexperienced or relatively junior staff. In others it is one role among many that an individual must perform or is filled by staff who do not appreciate or understand the clinical context. Where specific competencies exist, they usually focus on the Data Protection Act with few people understanding the professional regulatory or legal framework or other legislation such as the common law duty of confidentiality and Human Rights Act.

The boards or equivalent bodies in health and social care organisations should ensure that information governance staff understand the need to support the safe sharing of personal confidential data for direct care as well as the need to protect individual's confidentiality. Health and social care professionals and staff also have a responsibility to know the information governance policies of the organisations they are employed by, and should be prepared to challenge policies and guidance that inhibit the appropriate sharing of personal confidential data for safe and effective direct care.

The Review Panel concluded that information governance specialists should work together across organisational boundaries to enhance the community of practice to improve knowledge and best practice, solve practical challenges, develop trust in the information governance function and remove isolation. This report does not exclude the possibility of small organisations sharing Caldicott Guardians or information governance staff to develop expertise and ensure consistency.

Recommendation 15

The Department of Health should recommend that all organisations within the health and social care system which process personal confidential data, including but not limited to local authorities and social care providers as well as telephony and other virtual service providers, appoint a Caldicott Guardian and any information governance leaders required, and assure themselves of their continuous professional development.

10 Children and families

10.1 Context

Children are no less entitled than adults to protection from unauthorised disclosure of personal confidential data. For a child, to be laughed at in the classroom over a sensitive medical condition or family circumstance that is known to social workers would be just as embarrassing as for an adult who is confronted with a similar disclosure – possibly even more so. Guidelines on good professional practice recognise the importance of confidentiality. For example the General Medical Council advises: "Without the trust that confidentiality brings, children and young people might not seek medical care and advice, or they might not tell you all the facts needed to provide good care.[89]"

However, professionals in health and social care know that it is not only the confidentiality of children and young people that needs to be protected, but also their safety. The safeguarding of children is a well-established system which works well when followed properly.

The mechanisms for sharing have changed from time to time, often in response to child abuse tragedies including the deaths of Victoria Climbié and Peter Connelly (Baby P.) During the period of this review, the Government announced a further change, involving plans to link NHS records of children attending Accident and Emergency with registers held by local authority children's services departments, in an attempt to identify cases of abuse[90].

Arrangements for sharing require constant vigilance by the relevant professionals, but the system generally works provided the guidance to people working with children and young people is clear and well understood. There is no knowledge of sharing information in this context causing harm and the Review Panel has found no reason to disturb the fundamental principles of this approach.

It has become clear, however, that professionals dealing with children and families encounter particular issues of information governance that are not covered elsewhere in this report:

- Children become competent and able to make their own decisions at different ages. This raises questions about when they should have the right to access their personal electronic records and when parents' access should be curtailed.
- There is ambiguity around definitions. For example, what is the definition of a 'family' and does it include closely-knit groups of people who are not in a traditional familial relationship? This becomes important when deciding how to share family records. Doing so may require difficult judgements about how to disclose information to individual members of the family without compromising the confidentiality of others.
- The Health and Social Care Information Centre does not have the statutory right to collect children's social care confidential data.

[89] http://www.gmc-uk.org/guidance/ethical_guidance/children_guidance_42_43_principles_of_confidentiality.asp

[90] DH press release 27/12/12, http://www.dh.gov.uk/health/2012/12/abuse-alert-system/

- The care team looking after the interests of a child or a family often includes agencies from outside the normal boundaries of health and social care, from both public and independent sectors. Working in such teams may require health and social care professionals to share information with people who are not on a professional register and may not follow the same information governance rules and procedures.
- Children comprise the only aspect of health and social care policy with two lead government departments — the Department of Health for children's health and Department for Education for children's social care. The terms of reference for this review cover children, but our report is to the Secretary of State for Health.
- Cross-government policy is increasingly focusing on early intervention to improve 'public welfare'. These initiatives use data to identify 'at risk' individuals and groups in order to offer support e.g. to help troubled families or to combat domestic violence, trafficking and grooming.

10.2 Parents, children and young people: access to electronic records

In general, parents or people with parental responsibility should have access to their child's health and social care records. However, children should also be involved in decisions about their care, subject to their capacity to understand and have a view.

As children develop and gain the ability to make their own decisions, there comes a time when parents should not automatically be able to access the child's record. The point at which this transition occurs is different for every child, and is influenced by circumstance, the parents and the child. Health and social care professionals are accustomed to making a judgement about when this transition should take place. These professional judgements can be further complicated in difficult circumstances, for example if the child is living in an abusive environment. It is not the intention of this review to reduce the discretion available to professionals to make these subjective decisions on a case-by-case basis.

However, we have to consider the implications for children and parents of our recommendation in chapter 2 that people should have access to all the personal electronic records about them, across the whole health and social care system. When should the parent's automatic right of electronic access to the child's record be turned off and at what stage of maturity should the child's automatic access be turned on?

The Royal College of General Practitioners explored this difficult problem as part of its recommendations on patient online access. Although clearly each individual case will require professional judgement, the college's standard assumption was that, initially, both the child and the parent(s) should have full online access. 'Full' access should automatically be switched off when the child reaches the age of 12, although transactional online services, such as making appointments with a professional, would still be possible. 'Full' patient online access would be reinstated to the child when they reach 16 years old if they have capacity, or earlier if the health or social care professional judges, after discussions with the child, that they are competent.

10.3 Family records

Following the Munro Review[91] there has been a trend in children's social care to move back to maintaining 'family records'. This is not instead of individual case records, but rather using technology more effectively to maintain both individual and family views of the data.

The challenge in such systems is two-fold:

- To be able to present a meaningful record to each individual family member without compromising the privacy/confidentiality of other family members (but recognising what they do or are likely to know about each other).
- The ability to deal differentially with information provided by third parties which may be shared with some agencies and not others; or some family members and not others.

In this context it is likely that, as a minimum, the child or young person's record would hold a family 'tree' extending beyond the household, but including any non-relatives sharing or significantly influencing the household.

The increasing creation and use of family records is a contentious issue, the ICO Anonymisation code of practice states[92]:

> *"Information about a large family group might not be personal, but its disclosure may well breach the privacy rights of the family.*
>
> *It is advisable to seek specialist advice if you believe a disclosure has novel or potentially contentious Article 8 implications."*

Recommendation 16

Given the number of social welfare initiatives involving the creation or use of family records, the Review Panel recommends that such initiatives should be examined in detail from the perspective of Article 8 of the Human Rights Act. The Law Commission should consider including this in its forthcoming review of the data sharing between public bodies.

10.4 Consent relating to children and families

Health and social care professionals may be confronted with extremely complex scenarios involving the care of children and families, and the obtaining of consent, which require professionals to exercise judgement of the highest order. Examples are given below:

- Young carers; these can be children as young as five or six. This raises capacity and sharing challenges.
- There are circumstances where two or more people who have specific needs, are caring for each other. Examples are married couples or an ageing parent and an adult child with needs. It may well be that one half of the 'partnership' may choose to share

[91] The Munro Review of Child Protection: Final Report — A child-centred system, DfE, 2011, https://www.education.gov.uk/publications/standard/publicationDetail/Page1/CM%208062

[92] Anonymisation: managing data protection risk code of practice, ICO, 2012 page 35.

everything while the other may choose to be exceptionally selective. This creates many challenges for people involved in their care.
- On becoming an adult, children who lack capacity present a particular issue as their parents lose the right of intervention unless they have attained a power of attorney, or are appointed as deputies of the Court of Protection.
- Evidence from the Information Commissioner's Office is clear that if consent is sought it should not normally be over-ridden. However for young people and those with parental responsibility, there is significant scope for opposing views on consent to be presented.

For individual case-work or direct care of children or young people, the general principles relating to consent are no different to caring for adults. The differences are related to the overall process. In all cases where consent to share is the appropriate route the process should be as follows:
- Check the capacity of the child or young person to make the decision.
- If the child/young person has capacity, seek their consent including consent to share with those with parental responsibilities and act on the decision.
- If the child/young person does not have capacity, it may still be appropriate to seek their views and if no concerns seek consent of those with parental responsibility.
- If there are concerns, professional judgement needs to be carefully exercised in accordance with appropriate ethical and process guidance.

10.5 Cross-agency sharing

In order to provide effective care for children, information often needs to be shared beyond the normal boundaries of health and social care, in particular taking in organisations such as schools.

The Review Panel found there is some good practice around information sharing between health and social care services and organisations such as schools, particularly where there is a lead professional co-ordinating the care of an individual child. However, there is a great deal of variation in the processes and standards used for sharing information. For example, the Review Panel heard that poor information sharing was almost always often a key characteristic when children's social care systems were found to be unsafe.

The Review Panel concludes that there would be clear benefits if a single, common approach to sharing information for children and young people could be adopted, that aligns with the standards set out in this report.

However, there is an added complexity in that children comprise the only aspect of health and social care policy with two lead government departments — the Department of Health for children's health and Department for Education for children's social care, and a number of external regulators, including Ofsted and the Care Quality Commission.

The Review Panel concludes that the Department of Health and the Department for Education should jointly investigate ways to improve the safe sharing of information between health and social care services and schools and other services relevant to Children and young people through the adoption of common standards and procedures for sharing information.

Local authorities and their staff face further challenges in information sharing, even when a legal basis exists and well-established sharing agreements are in place under section 75 of the NHS Act 2006[93].

Data sharing arrangements can be extremely complex and subject to significant regulation. There can be difficulties when clients make the transition from children to adult social care, where different information technology systems impede the sharing of information. Further complexity is added through the lack of common internal sharing requirements across different children and family services, youth offending teams, housing and benefits services. The development of academies and free schools adds another dimension to consider, as they are not subject to local authority direction and do not have to employ registered and regulated staff as teachers.

In practice there are two types of cross-agency sharing:

- exchanges of information among teams from different disciplines, both inside and outside local authorities, to produce a wider 'welfare' care plan; and
- linkage of information held by teams from different disciplines, both inside and outside local authorities, as part of a process of identification of children or 'families' for early help or intervention.

These are considered briefly in the paragraphs that follow.

10.6 Managing and protecting children's identities

At the time of this review there was a transition in progress in circumstances where children are adopted. This would see children keeping the same NHS number when they are adopted with the exception being in circumstances of safeguarding, when a child's identity needs to be protected. In these cases a new NHS number may sometimes be allocated.

The Review Panel concluded that changing of a child's NHS number should be avoided wherever possible. Should the NHS number be utilised more widely in children's social care services, the current NHS rules and guidelines will need to be reviewed by the Department of Health and Department for Education.

In addition, in cases where the location and/or the identity of a child needs to be protected, for example from family members in cases of abuse, 'shielding requirements' are placed on the child's records.

The Review Panel concluded that where 'shielding requirements' exist, they must be shared appropriately as a priority with health and social care professionals whenever relevant information about the child is shared.

[93] http://www.legislation.gov.uk/ukpga/2006/41/section/75

10.7 Welfare care plans

The Review Panel has found that care plans for children and young people often extend beyond the immediate scope of health and social care to include broader welfare interventions. For the purposes of this report, we refer to these extended plans as 'welfare care plans'.

Welfare care plans will typically be generated from case conferences involving a range of professions and agencies, who will, of necessity, and in accordance with best professional practice and the law, share a range of information pertinent to the planning of care for the child. This may result in a plan involving a wider range of professions and individuals to deliver the plan. This could include teachers, teaching assistants, play workers, youth workers, etc.

They are not part of the health and social care registered and regulated professions, nor directly under their supervision. But they are critical to successful interventions. In such cases there is a duty on the relevant health or social care professional taking the lead in the case to ensure that those delivering the 'welfare care plan' are appropriately informed about the individual.

10.8 Identifying cases for early help or intervention

Government policy is increasingly seeking to use information to identify individuals or groups of people, such as families, who may benefit from specific help or early intervention. Generally, the aim of these interventions is to address problems these individuals and groups may be facing before they can escalate, potentially causing harm to themselves, their communities, or wider society. Identifying these people often requires extensive sharing, linkage and analysis of personal confidential data.

The Review Panel heard a variety of concerns about whether this identification work always complies with data protection, human rights and confidentiality law. On the other hand, it also heard criticism of healthcare professionals for citing information governance rules and procedures as reasons for refusing to engage in this work.

The Review Panel concluded that significant lessons regarding data sharing could be learned from public health and research communities. Additionally there are significant opportunities arising from the transfer of public health to local authorities to enable swifter progress on such welfare programmes. We do not suggest that social problems affecting troubled families or other groups in society are similar to the diseases that interest directors of public health and research scientists. However the approach to information governance adopted in public health and research may be helpful.

10.9 Parallels with public health and research

The definitions of 'prevention' adopted in the influential study of public health by the Commission on Chronic Illness[94] could be adapted to include social welfare interventions [changes in italics]:

[94] http://jama.jamanetwork.com/article.aspx?articleid=321887

- Primary Prevention, which seeks to decrease the number of new cases of a disorder or illness *or adverse social welfare events such as crimes, exploitation, incidence of domestic violence etc.*
- Secondary Prevention, which seeks to lower the rate of established cases of a disorder or illness *or adverse social welfare events* in the population (prevalence).
- Tertiary Prevention, which seeks to decrease the amount of disability *and failures of participation* associated with an existing disorder or *adverse social welfare situation.*

The benefit of viewing social welfare interventions in this way is that the public health and research communities have developed sophisticated methods for assessing interventions and managing information governance. Adapting these approaches to social welfare would allow the development of rigorous, evidence-based social interventions.

The Review Panel concludes that these three levels of prevention are relevant to the broader social care and public welfare arenas. At the primary prevention level, there are initiatives seeking to identify individuals or 'families' that are displaying, or are highly likely to display in the absence of intervention, behaviours that have negative implications for themselves and for society at large. The secondary prevention level is where individuals or families have come to the attention of the relevant authorities and their needs are being assessed. This may be through referral, including self-referral, or through an early identification system. Tertiary prevention is where the individual or group is in receipt of services or interventions in response to their needs. This may extend well beyond health and social care, for example reducing the number of people entering the criminal justice system.

The Review Panel concluded that applying the lessons from research and public health to this rapidly changing area of social welfare interventions could overcome many of the perceived information governance barriers.

Professional standards and good practice

The Review Panel concludes that from an information governance perspective there is a need to ensure that the process of identifying individuals or groups of people for early intervention or help (as well as the interventions themselves) are properly underpinned by meeting all the following criteria:

- There is a basis in law for processing personal confidential data.
- There are appropriate approaches to linking data (see sections 3.14, 6.3, 6.5 and 12.6).
- There are appropriate contractual arrangements in place to process de-identified data for limited disclosure or limited access (see sections 6.3, 6.5 and 12.10 and appendix 6).
- If help is to be offered, a clear legitimate relationship should exist between the individual or family identified and the person making contact with them (see section 3.6).

10.10 Information sharing guidance

A range of Information sharing guidance has been produced in the past decade or more. Some of the guidance deals with broad information sharing needs in a variety of settings, for example, the material produced by the Information Commissioner's Office. Other guidance has been produced relating to specific purposes and settings such as mental health, missing persons and domestic violence. The cross-government guidance available on the Department for Education website has been particularly commended to the review as a good basis for developing updated guidance and advice. Guidance is also available from the Department of Health website[95].

[95] http://www.education.gov.uk/childrenandyoungpeople/strategy/integratedworking/a0072915/information-sharing

11 New and emerging technologies

11.1 The virtual consultation

Increasing numbers of patients are benefiting from new technologies that permit 'virtual consultations' with a clinician, using the telephone, emails or video links rather than relying on a face-to-face contact between a clinician and the patient. These 'at a distance' services have the potential to greatly increase patients' ability to manage their own care, especially for individuals with specialised or long term conditions.

Data gathered from these virtual consultations can be used to update an existing patient record and in some instances the data from the virtual consultation becomes a patient record in its own right[96]. The Review Panel found there is no standard among providers of virtual consultation services as to how long data gathered from consultations should be kept, and in practice the decision is left to individual organisational choice.

The Review Panel concluded that, while many providers have policies for giving patients a copy of communications between professionals about the outcome of a consultation, there is sometimes a lack of clarity as to how patients can access their actual record.

The Review Panel concluded that providers of direct care services using virtual consultations should offer patients access to their record and a copy of all ongoing communications from that record.

The Review Panel also concluded that any provider offering virtual consultation services should be able to share, when appropriate, relevant digital information from the patient, with registered and regulated health or social care professionals responsible for the patient's care. This includes both written text or numbers and images, such as photographs.

11.2 Medical devices

There is a rapidly expanding range of medical devices that may use software or other technologies to record data about a patient when a clinician or other professional is not present. These devices then make the information available to either the patient, the professional or both.

These new processes and technologies present some potential challenges for the health and social care system, raising questions such as:

- How can a health or social care professional be sure that a measurement from a patient does indeed reflect a biometric measure of the patient and not someone else's readings?
- Is the patient able effectively to use the device so the result is reliable?
- Is the provider aware that the monitoring service is actually creating a personal record and hence must conform to all current and future legislative duties around personal records concerning personal confidential data? Does the provider communicate this to the patient?

[96] Where the virtual consultation becomes a record in its own right, a classification for that record and a retention and review policy should be applied in line with the NHS Records Management Code of Practice. Current Department of Health advice is that electronic records should be retained indefinitely. This may not be appropriate for virtual consultations, particularly given the likelihood that the service will be provided by and the data held by a data processor under contract which at some point is likely to come to an end.

- Patients may decide on their own initiative to use a monitoring device, rather than being recommended to do so by a professional. Are they made aware of the terms and conditions, particularly regarding the use of personal confidential data?

However, the Review Panel concluded that although services based on these new and emerging technologies may create some operational challenges, they do not require any additional information governance principles. The personal confidential data gathered through these new processes and technologies must be treated in exactly the same way as any other personal confidential data, and providers of these services must adhere to the existing legislation and best practice on protecting and appropriate sharing of personal confidential data.

Recommendation 17

The NHS Commissioning Board, clinical commissioning groups and local authorities must ensure that health and social care services that offer virtual consultations and/or are dependent on medical devices for biometric monitoring are conforming to best practice with regard to information governance and will do so in the future.

12 Data management

12.1 The relationship between data quality and information governance

There are many good reasons why organisations in health and social care need good quality data. Patients are at risk if clinicians base their decisions on inadequate data. Dangers multiply if there is poor handover of information between care teams or conflicting advice to patients from professionals. The issue is particularly relevant to this review because poor data is cited by managers in health and social care as a reason why they need access to information about individuals. If they cannot trust the accuracy and relevance of anonymised data, they may think the only way to discover the truth is to look at a selection of real cases involving real people. For this reason, poor data quality may be used as an excuse for ignoring the principles of sound information governance. The Review Panel found the excuse unsatisfactory. The correct solution to these problems is to improve the quality of data and not to compensate for poor data by adopting poor information governance.

12.2 Record access and direct care

Poor data quality can directly affect the quality of direct patient care. Examples include clinicians making decisions about treatment on the basis of incorrect information, poor handover of information between care teams and instances where patients receive differing, sometimes conflicting advice from professionals providing their care. Incidents like this serve to erode the trust between professionals and patients. In addition, the recording and sharing of inaccurate data is a breach of principle 4 of the Data Protection Act.

Poor data quality can be caused by poor practice, such as professionals recording data inaccurately, or can result from poor standards or procedures, for example having systems that do not allow an accurate or suitably detailed expression of a patient or client's condition.

Adopting the Review Panel's recommendations in chapter 2 to give patients and service users fuller access to their records can improve data quality by providing an opportunity for the individual to see errors and call for their correction.

The review welcomes the focus that professional bodies for health and social care are placing on data quality and endorses the recent public statement from the Royal College of Physicians[97], which encapsulates what is needed for the future from all professions and their associated teams. It says:

> ***"We must revolutionise the way we use information***
> *We must create pathways in which information moves with patients across the system in real-time. We must enhance electronic patient records and promote common record standards. Information and systems need to support clinical decision-making, reflective practice, quality improvement and meaningful patient choice."*

These issues are also picked up from a primary care perspective in the *Good Practice Guidelines for GP electronic patient records v4* (2011) from the Department of Health[98].

12.3 Data quality and linkage of sets of data

Previous chapters have explained why researchers, commissioners and others may often want to link different sets of data about an individual. When doing so, they need to be sure that the two sets of data really do belong to the same person.

However, that does not necessitate the use of personal confidential data. If the data quality is sound then a pseudonym may be used to link data and thus protect the identity of an individual. This is more fully explained in the ICO Anonymisation Code of Practice.

Linking sets of data is very important for aspects of direct care, including audit of care, delivery of care and merging of records. It is also important for aspects of indirect care, such as registries and the derivation of data to support care pathway commissioning. Equally both indirect and direct care can benefit from linkage to support the identification of high risk groups, obviously supported by an appropriate legal basis.

During the evidence gathering the Review Panel heard frequent complaints that local data sets are too poor to enable data linkage without multiple direct identifiers which therefore creates a dependence on personal confidential data being used.

For example, research has shown that when planning services it is possible to link data and match individuals using de-identified data for limited disclosure or access and the NHS number as an identifier in up to 99.8% of cases[99]. However, this still leaves a minority of cases, such as Cancer Registries looking for individuals suffering from rare forms of cancer, where this approach will be insufficient, and individuals have to be matched using personal confidential data.

[97] http://www.rcplondon.ac.uk/projects/hospitals-edge-time-action

[98] http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_125310

[99] Lyons et al, 16 January 2009, http://www.biomedcentral.com/1472-6947/9/3

The Review Panel concluded that in such cases, a two-stage approach should be adopted. This would mean initially using de-identified data for local disclosure or access and a single identifier, such as NHS number to narrow down a data set, before using personal confidential data to complete the matching. Personal confidential data should not be used from the outset.

12.4 Data quality and indirect care

In general, there are two main causes of poor quality data for indirect care. The first is when data for indirect care is derived from professional health and social care records for direct care that are themselves of insufficient quality. The second stems from the way in which indirect care data sets are created. This is done by either using an automated approach to produce new data sets from health and social care records (sometimes called 'mapping'), or more frequently, relying on human transcription; taking data from one source and recording it in another system or database. Data transcription errors can be significant with rates of 6.5% or 650 errors per 10,000 fields quoted in research studies[100]. However depending on context these error rates may be even higher[101], especially when the transcribing process requires the source data to undergo a change or transformation. The use of human transcription therefore not only increases the exposure of personal confidential data it also reduces data quality.

The Review Panel endorses the First National Data Quality Report of the Quality Information Committee of the National Quality Board[102], which seeks improvements in data quality in the health and social care system.

12.5 Record management incidents

The records management systems of any organisation is integral to the quality of its data. Health and social care organisations need to ensure they have robust procedures in place for transferring, archiving and disposing of data in an appropriate and timely way. A significant number of serious incidents happen because of a failure to manage data appropriately, for example 'wrong-site' surgery or incorrect treatment being provided to an individual. Some of these feature failures of information systems. There have also been a number of incidents resulting in breaches of the Data Protection Act when data has been archived or destroyed in an inappropriate or insecure manner.

While these will be reported as serious clinical incidents allowing key lessons to be learned, they may not identify more systemic failures. This means that issues caused by poor information management may not be identified and addressed as quickly as they could be.

The Review Panel concludes that serious clinical incidents in which any data management issue is identified should be reported in a similar manner to data breaches (see section 4.6).

---

[100] Wahi et al, Reducing Errors from the Electronic Transcription of Data Collected on Paper Forms: A Research Data Case Study, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2409998/

[101] Automated quality checks on repeat prescribing, J E Rogers, C J Wroe, A Roberts, et al, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1314725/

[102] http://www.dh.gov.uk/health/category/policy-areas/nhs/nqb/

12.6 Administrative Data Taskforce and 'What Works' Centres

The Administrative Data Taskforce was formed in December 2011 by the Economic and Social Research Council, the Medical Research Council and the Wellcome Trust. The Administrative Data Taskforce has been working with a range of government departments, academic experts, the funding agencies and representatives from all four nations in the UK to examine the best procedures and mechanisms to make administrative data available for research, safely.

The Administrative Data Taskforce report, *Improving Access for Research and Policy* (December 2012)[103], proposes a UK Administrative Data Research Network responsible for linking data between government departments. The Review Panel endorses the approach in this report and believes that it should provide a basis for providing the linkage service to support identification for early help or intervention with effective information safeguards.

In particular, the Review Panel supports:

- the recommendation to establish an Administrative Data Research Centre in each of the four countries of the UK;
- the potential legislation to facilitate pan-government work on research and statistics through access to administrative data and to allow data linkage between departments to take place more efficiently using their recommended methods; and
- the model of using a 'trusted third party'[104] to provide linkage of data while maintaining appropriate security and confidentiality.

The Economic Social Research Council is also involved in 'What Works' networks that are undertaking separate initiatives[105]. Such approaches may be appropriate for the early identification and help social welfare intervention initiatives.

12.7 Safeguarding

Across the health and social care system, the resistance and fear that exists about sharing information is less evident in instances of safeguarding children. Professionals (and their organisations) do not want to be left holding crucial information that could have been used to prevent harm, and professionals would sooner defend a situation of a breach in confidentiality by sharing, rather than defend an unnecessary death through not sharing.

The difference is not just in attitudes, but also in time and resources. The Review Panel heard professionals could spend up to ten times the amount of time on cases involving safeguarding and associated sharing than on routine care and sharing.

[103] The UK Administrative Data Research Network: Improving Access for Research and Policy Report from the Administrative Data Taskforce, December 2012, http://www.esrc.ac.uk/_images/ADT-Improving-Access-for-Research-and-Policy_tcm8-24462.pdf

[104] Model Three in the ADT report.

[105] Examples include: www.centreformentalhealth.org.uk/pdfs/briefing37_Doing_What_Works.pdf, http://www.primarycarefoundation.co.uk/what-we-do/urgent-care-centres, http://www.barnardos.org.uk/reaching_families_in_need.pdf

The Review Panel took into consideration a number of reports on safeguarding children and concluded that considerable progress was being made but as the Edlington Report and the report from the Office of the Children's Commissioner entitled 'I thought I was the only one. The only one in the world[106]' make clear, there is still more to do.

With regard to safeguarding adults the new Care and Support Bill highlights this subject in several sections. It was noted that there is no provision for a statutory gateway for reporting safeguarding concerns.

The Review Panel concludes that the good practice in sharing around safeguarding children is improving. There are concerns about inconsistent practice relating to identifying young people at serious risk. In addition, serious consideration should be given to reporting safeguarding concerns involving adults and whether patient consent should be sought or whether safeguarding concerns should be raised utilising a statutory gateway particularly about adults being cared for away from home.

Multi Agency Safeguarding Hubs (MASH) address a problem that has been brought up in almost every serious case review — lack of information sharing. The first MASH was the developed by Nigel Boulton, area commander of the Devon police. Professionals from children's care, police, education and health sitting alongside one another, with their respective IT systems, using shared information to inform an appropriate safeguarding response to a vulnerable person.

Example

A police report on a drugs warrant noted a young woman present who was in possession of a high quantity of valium pills. On processing it through the MASH, it was discovered that the woman was seven months pregnant, living in temporary accommodation, had exhibited anti-social behaviour, poor engagement with antenatal services and had a history of involvement with social services. The case was immediately passed to an assessment team and a child protection plan was drawn up due to fears of neglect[107].

12.8 'The unborn'

Within the NHS, a foetus does not have a record and its details are recorded as part of the mother's record. Additionally foetuses are not allocated an NHS number. Within the social care system in England, however, a record may be opened for a foetus if a pre-birth assessment is required. This difference of approach poses problems when it comes to data sharing.

[106] The Office of the Children's Commissioner's Inquiry into Child Sexual Exploitation In Gangs and Groups — Interim report, November 2012.

[107] http://www.communitycare.co.uk/articles/07/06/2011/116936/multi-agency-safeguarding-centre-for-childrens-referrals.htm

For example, a pregnant woman showing symptoms of alcohol abuse might be assessed in a pre-birth plan. She would almost certainly be assessed if she had a previous child adopted or taken into care. The national statistics show clearly the increases in babies being born with foetal alcohol syndrome, and this is becoming an increasing challenge to the health and social care system, not least as many of these children may become subject to the adoption services.

Children's social care providers do not hold case records on adults. Therefore, details of the mother are recorded in the foetus's electronic record. A duty to share relevant information concerning a child's welfare is set out in 'Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children' (March 2010)[108]. This is generally supplemented with local policies and procedures.

To give an idea of scale, a local authority with responsibility for a population which has a significant drug and alcohol problem would have as many as a dozen 'unborn' cases at any one time.

Data sharing and service integration will present serious challenges when the NHS, Local Authorities and social care services adopt such different legal, cultural, organisational, operational and technical approaches. The Review Panel recognise that this is a complex issue, but conclude that further consideration should be given to finding a solution. As the issue starts at the point that different government departments are involved in the social care of adults and children any lasting solution needs to begin at this level.

Recommendation 18

The Department of Health and the Department for Education should jointly commission a task and finish group to develop and implement a single approach to recording information about 'the unborn' to enable integrated, safe and effective care through the optimum appropriate data sharing between health and social care professionals.

12.9 Information governance framework

As a general point, the same standards and rules across health and adult social care, including domiciliary care, would be extremely helpful. A recurring theme was the diversity and inconsistency of advice and guidance from a wide range of sources, which made it difficult to share data even to support the care of individuals. The Review Panel concludes there is a need for improvement in the appropriate sharing of information across sectors, with simple messages communicated to patients, staff and carers.

Small care providers may not have the capacity or capability to reach an adequate standard of information governance performance or understanding and may need support from their local principal commissioner.

[108] https://www.education.gov.uk/publications/standard/publicationdetail/page1/DCSF-00305-2010

The Review Panel concludes that consistency in the information governance requirements for providers is key.

In many instances providers are having to meet five or six different sets of requirements from different commissioners or government departments creating an undue burden. The position may be further complicated in the future, with the ability to commission from any qualified provider, designing specific new processes, perhaps in agreement with the provider.

The Information Governance Toolkit is an online resource that allows NHS organisations and other bodies to assess themselves against the Department of Health's information governance standards and policies. In practice, there is no independent audit of the self-assessments submitted and it is questionable how well they reflect actual information governance practice in organisations, particularly given the obligations to publish the results. Version 8 of the toolkit had required both supporting evidence of the self-assessment score to be submitted and for the scoring and evidence for some of the requirements to be internally audited. As a consequence, there was a marked decline in the results[109]. Additionally, the Department of Health subsequently initiated a 'deep dive' assessment of the scoring of five of the requirements in a number of acute trusts[110], looking at the efficacy of the internal audit process. The quality of the audit was found to be variable and the consistency of scoring across organisations to be poor.

The Review Panel concludes that Information Governance Toolkit self-assessments could be strengthened and their profile raised by inclusion of declarations in the Statements of Internal Control accompanying the annual quality reports of NHS organisations or for non-NHS organisations, in the annual report or performance report, signed off by the organisation's board or equivalent body.

The Review Panel concludes that in order to encourage openness and transparency, every health and social care organisation should publish a description of what personal confidential data it discloses, to whom and for what purpose. This information should already exist within the Data Protection Act privacy notices and data sharing agreements that organisations have produced.

Recommendation 19

All health and social care organisations must publish in a prominent and accessible form:

- a description of the personal confidential data they disclose;
- a description of the de-identified data they disclose on a limited basis;
- who the disclosure is to; and
- the purpose of the disclosure.

[109] NIGB Information Governance Toolkit Review, March 2013 http://www.nigb.nhs.uk/pubs/wgreports/index_html

[110] https://www.igt.connectingforhealth.nhs.uk/Bulletins/Information%20Governance%20Bulletin%20No%201%20July%202011%20(Vers%201).pdf

12.10 Contractual arrangements for data sharing

There are broadly three types of legal arrangement when data is shared. These are shown in the table below. A fuller explanation of the health service body to health service body contracts is set out in section 7.5.

Figure 2: Information governance contractual agreements for the legal sharing of data

Type of contractual agreement	Enforced by the ICO?	Requirement for contractual agreement to contain explicit penalties and liabilities?	Requirement for section 251 support for health service body to health service body sharing? **
Disclosure of de-identified data for limited access	Yes, if the data becomes re-identified	Yes	Yes
Disclosure of personal confidential data from one data controller to another data controller*	Yes	No	No
Disclosure of personal confidential data: from a data controller to a data processor	Yes	Yes	Yes

* Although it may appear that there are fewer safeguards in agreements for disclosing personal confidential data from one data controller to another data controller, this type of sharing already requires a legal basis of consent, statute or exceptionally, public interest.

** This section 251 is to convert an unenforceable contract into an enforceable contract.

The Review Panel concludes that suitable section 251 support is required for data controller to data processor disclosures and disclosures of de-identified data for limited access from one health service body to another health service body (see section 7.5).

Based on the evidence gathered during the review, the Review Panel is aware of the significant resources used by health and social care organisations to produce Data Controller to Data Controller data sharing agreements. Given the resource constraints the whole system is under, the Review Panel believes that designing and implementing a single health and social care system process or template for data controller to data controller sharing agreements could reduce unnecessary duplication and prevent people re-inventing wheels.

Recommendation 20

The Department of Health should lead the development and implementation of a standard template that all health and social care organisations can use when creating data controller to data controller data sharing agreements. The template should ensure that agreements meet legal requirements and require minimum resources to implement.

12.11 Provider service contracts

When a commissioner changes provider, the fate of the records held by the original provider, both for services with episodic data and for services with continuity of care responsibilities, remained unclear to those giving evidence. This point was made eloquently in respect of independent sexual health services[111].

Professional standards and good practice

All patient records held by provider organisations should be kept in line with health and social care system record retention requirements. The Review Panel concludes there are two ways this could be done:

- The provider holding the records could be funded to deliver this retention and security of the records as part of their commissioning contract. If the provider is providing care services they will need to retain the data for a period for their own financial probity and clinical or care governance. If the provider is purely a data processor then they should not need to retain the data beyond the contracted period.
- Another part of the health and social care system, for example the Health and Social Care Information Centre, could be commissioned to provide a 'safe vault' for this data which can only be accessed when there is anonymisation at source, or when there is complaint, legal challenge or criminal investigation.

[111] Note: Between 30% and 56% of people accessing sexual health services do not want their GP to be informed. Therefore, storing records with the GP is not always an option.

12.12 Access to patient records from insurers and mortgage providers

The Panel also heard concerns that insurers and mortgage lenders may seek to use their influence to request whole records from GPs, as a condition of supplying insurance or a mortgage. The General Medical Council has issued specific guidance for GPs[112] and the British Medical Association and the Association of British Insurers (ABI) have produced joint guidelines[113] to allow relevant data about patients to be shared appropriately with insurers on a basis of explicit, written consent.

In addition, principle 3 of the Data Protection Act[114] offers further safeguards as it allows organisations to hold only "adequate, relevant and not excessive" personal data about an individual. This means insurers and mortgage lenders cannot hold more information about an individual than they need. The act also requires organisations to identify in advance and then request only the minimum amount of data needed for a particular purpose.

The Review Panel concluded that these guidelines, combined with the safeguards offered by the Data Protection Act offer sufficient to prevent inappropriate sharing of whole records with insurers and mortgage lenders.

[112] 'Confidentiality: disclosing information for insurance, employment and similar purposes', General Medical Council, 2009, states that:

- "[GPs] must inform patients about disclosures for purposes they would not reasonably expect, or check that they have already received information about such disclosures"; and
- "as a general rule, you should seek a patient's express consent before disclosing identifiable information for purposes other than the provision of their care or local clinical audit, such as financial audit and insurance or benefits claims."

http://www.gmc-uk.org/Confidentiality_disclosing_info_insurance_2009.pdf_27493823.pdf

[113] 'Medical information and insurance: Joint guidelines from the British Medical Association and the Association of British Insurers, March 2010' states:

- "Consent for disclosure of information is valid only where applicants understand the nature and extent of the information that is being requested, and the use to which it will be put. If doctors are in any doubt about whether valid consent has been given, they should check with the applicant."

www.abi.org.uk/Information/64827.pdf

[114] http://www.ico.gov.uk/for_organisations/data_protection/the_guide/information_standards/principle_3.aspx

13 System regulation and leadership

13.1 System-wide regulation

From an information governance perspective, there is currently no method of regulating the health and social care system as a whole. There are organisations that regulate particular aspects of information governance, notably the Information Commissioner's Office, which has a duty to ensure organisations adhere to the Data Protection Act, and the Care Quality Commission (CQC). The Health and Social Care Act 2012 describes the CQC's role in monitoring the processing of information across all providers, making the results known to the NHS Commissioning Board and Monitor. Perhaps more importantly, the CQC must, in exercising those functions, seek to improve the practice followed by registered persons in relation to the processing of relevant information.

Given the importance of information governance to public trust and the dependence of the health and social care system on data, the Review Panel saw an opportunity for monitoring and system wide regulation of information governance. In order to achieve this, the following existing components need to be brought together:

- CQC and the ICO should have a Memorandum of Understanding to allow the sharing of any concerns revealed by monitoring. This should include, but not be limited to non-notification to the ICO of an organisation processing personal information[115] and non-adoption of a publication scheme under Freedom of Information Act 2000[116]
- CQC monitoring should include but not be limited to:
  - data breaches as reported to the boards of health and social care system organisations;
  - failures to take due regard for the Information Centre code for processing confidential information;
  - any failure to inform the public how their personal confidential data was being disclosed; and
  - failures of sharing or excessive sharing as reported by the Parliamentary and Health Service Ombudsman.
- CQC monitoring of information governance should be reported annually, to allow any improvement or deterioration in practice over time to be seen.
- The CQC annual report and the breaches reported to the ICO from the health and social care system should be presented to the Informatics Services Commissioning Group, which is responsible for providing advice on commissioning informatics services, including information governance, across the health and social care system, where action should be taken to improve a deteriorating situation through the leadership of NHS Commissioning Board and Monitor.

[115] All organisations processing personal data are legally required to register with the Information Commissioner's Office (unless they are exempt), all organisations providing care and therefore responsible for care records are required to register, see http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx

[116] The obligation on public bodies to have a publication scheme is set out under sections 19 and 20 http://www.legislation.gov.uk/ukpga/2000/36/part/I/crossheading/publication-schemes, and is enforceable under section 52 of the FOIA http://www.legislation.gov.uk/ukpga/2000/36/section/52

The Review Panel heard that there were likely to be a large number of non-registered providers. It would not be realistic to monitor all these providers. Therefore they should gain access to confidential patient information only through the patient or their legal representative.

13.2 System alignment

The Review Panel is clear that the remit for the Data Protection Act remains with the Information Commissioner, but individual breaches or failures to share information by registered and regulated health and social care professionals may be a failure of professional duty.

The Review Panel concluded that the professional regulators should be involved more often in both serious breaches and instances of poor information sharing when it is clear it has hampered direct care.

There needs to be a way of holding the health and social care system to account on information governance. The Health and Social Care Information Centre will be responsible for producing and maintaining a code of practice on collecting, analysing, publishing or disclosing confidential information. Every organisation in the health and social care system should conform to this code.

The Review Panel concludes that the Information Centre code of practice should adopt the standards and good practice examples contained throughout this report.

Recommendation 21

The Health and Social Care Information Centre's Code of Practice for processing personal confidential data should adopt the standards and good practice guidance contained within this report.

13.3 Information governance terminology

The Review Panel found that the variety of definitions and terms relating to information and information governance leads to confusion among both professionals and the public. This in turn leads to misunderstandings of relevant legal duties and responsibilities and contributes to the lack of confidence and unwillingness to share information.

The Review Panel recommends there should be an agreed set of terms and definitions for information sharing, in line with legal definitions, for the whole health and social care system. The aim should be that everyone, including the public, should be able to use and understand.

Recommendation 22

The information governance advisory board to the Informatics Services Commissioning Group should ensure that the health and social care system adopts a single set of terms and definitions relating to information governance that both staff and the public can understand. These terms and definitions should begin with those set out in this document. All education, guidance and documents should use this terminology.

Recommendation 23

The health and social care system requires effective regulation to ensure the safe, effective, appropriate and legal sharing of personal confidential data. This process should be balanced and proportionate and utilise the existing and proposed duties within the health and social care system in England. The three minimum components of such a system would include:

- a Memorandum of Understanding between the CQC and the ICO;
- an annual data sharing report by the CQC and the ICO; and
- an action plan agreed through the Informatics Services Commissioning Group on any remedial actions necessary to improve the situation shown to be deteriorating in the CQC-led annual 'data sharing' report.

14 Conclusions and recommendations

In addition to the findings of individual chapters, the Review Panel has reached some overarching conclusions.

14.1 Redress

The terms of reference for this review included examination of what safeguards exist to protect people's confidential information and what means of redress are available if mistakes are made. We were asked to consider whether the current safeguards and means of redress remain sufficient to provide assurance to the public, both in terms of the duty of care and breaches of confidence.

We have dealt with these issues in various chapters, but the Review Panel believes the question of redress is so important that it is worth drawing the threads together. The list of actions below set out how redress should be managed by every organisation in the health and social care system in England from 1st April 2013:

- Individuals affected by a breach must be told what happened, how it happened, what will be done to put matters right, and be given an apology (section 3.10 and recommendation 5).
- Penalties should be administered via the Information Commissioner's Office which can impose civil monetary penalties of up to £500,000 and potentially criminal prosecution for serious breaches of the Data Protection Act.
- If there has been a breach of section 55 of the Data Protection Act, even if the ICO decides not to prosecute, the health or social care organisation concerned must take remedial action; and the Care Quality Commission must assure itself that the action has been taken and is fit for purpose.
- All data breaches should be reported to the organisation's full senior management board; it should report the breaches and the remedial actions in its annual report (section 4.6).
- If there is a complaint or serious incident in which the management or recording of data is a significant feature, then these events should be treated as data breaches (section 12.5).
- Failure to inform the public properly on how their personal confidential data is being shared (section 12.8: recommendation 18) should be actively monitored by the Care Quality Commission with a view to securing an improvement in performance, with or without the assistance of the NHS Commissioning Board and Monitor.
- If there is poor professional practice with regard to information sharing that is hampering direct care, and if education and professional development fails to improve matters, then organisations have a duty to involve the professional's regulator (section 13.1).

The Care Quality Commission's performance in carrying out its legal duties to monitor data sharing practice, inform the NHS Commissioning Board and Monitor, and improve practice must be explained in a publication that demonstrates practice is improving.

Recommendation 24

The Review Panel recommends that the Secretary of State publicly supports the redress activities proposed by this review and promulgates actions to ensure that they are delivered.

14.2 The Caldicott principles

There was widespread support for the original Caldicott principles, which are as relevant and appropriate for the health and social care system today as they were for the NHS in 1997. However, evidence received during the review has persuaded the Panel of the need for some updating, and inclusion of an additional principle.

Professional standards and good practice

The revised list of Caldicott principles therefore reads as follows:

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.
2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. **Use the minimum necessary personal confidential data**
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
4. **Access to personal confidential data should be on a strict need-to-know basis**
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. **Everyone with access to personal confidential data should be aware of their responsibilities**
   Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Professional standards and good practice (continued)

6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Recommendation 25

The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the health and social care system.

14.3 Implementing the findings of the Information Governance Review

The principles, conclusions and recommendations within this report seek to maintain the optimum balance between safeguarding patients' sensitive information and encouraging responsible and appropriate sharing of information for the benefit of all users of health and social care services. The Secretary of State for Health, and the Department of Health, are ultimately accountable for ensuring information governance works across the system.

The Review Panel therefore concludes that the Secretary of State and the Department of Health should oversee the implementation of the recommendations of this review, and report on the progress made.

Recommendation 26

The Secretary of State for Health should maintain oversight of the recommendations from the Information Governance Review and should publish an assessment of the implementation of those recommendations within 12 months of the publication of the review's final report.

Those recommendations are as follows:

14.4 Recommendations of the Information Governance Review

Recommendation 1 (section 2.4)
People must have the fullest possible access to all the electronic care records about them, across the whole health and social care system, without charge.

An audit trail that details anyone and everyone who has accessed a patient's record should be made available in a suitable form to patients via their personal health and social care records. The Department of Health and NHS Commissioning Board should drive a clear plan for implementation to ensure this happens as soon as possible.

Recommendation 2 (sections 3.3 and 3.4)
For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual.

Health and social care providers should audit their services against NICE Clinical Guideline 138, specifically against those quality statements concerned with sharing information for direct care.

Recommendation 3 (section 3.5)
The health and social care professional regulators must agree upon and publish the conditions under which regulated and registered professionals can rely on implied consent to share personal confidential data for direct care. Where appropriate, this should be done in consultation with the relevant Royal College. This process should be commissioned from the Professional Standards Authority.

Recommendation 4 (sections 3.6 and 3.7)
Direct care is provided by health and social care staff working in multi-disciplinary 'care teams'. The Review recommends that registered and regulated social workers be considered a part of the care team. Relevant information should be shared with members of the care team, when they have a legitimate relationship with the patient or service user. Providers must ensure that sharing is effective and safe. Commissioners must assure themselves on providers' performance.

Care teams may also contain staff that are not registered with a regulatory authority and yet undertake direct care. Health and social care provider organisations must ensure that robust combinations of safeguards are put in place for these staff with regard to the processing of personal confidential data.

Recommendation 5 (section 3.10)
In cases when there is a breach of personal confidential data, the data controller, the individual or organisation legally responsible for the data, must give a full explanation of the cause of the breach with the remedial action being undertaken and an apology to the person whose confidentiality has been breached.

Recommendation 6 (section 4.6)
The processing of data without a legal basis, where one is required, must be reported to the board, or equivalent body of the health or social care organisation involved and dealt with as a data breach.

There should be a standard severity scale for breaches agreed across the whole of the health and social care system. The board or equivalent body of each organisation in the health and social care system must publish all such data breaches. This should be in the quality report of NHS organisations, or as part of the annual report or performance report for non-NHS organisations.

Recommendation 7 (section 5.5)
All organisations in the health and social care system should clearly explain to patients and the public how the personal information they collect could be used in de-identified form for research, audit, public health and other purposes. All organisations must also make clear what rights the individual has open to them, including any ability to actively dissent (i.e. withhold their consent).

Recommendation 8 (section 5.5)
Consent is one way in which personal confidential data can be legally shared. In such situations people are entitled to have their consent decisions reliably recorded and available to be shared whenever appropriate, so their wishes can be respected. In this context, the Informatics Services Commissioning Group must develop or commission:

- guidance for the reliable recording in the care record of any consent decision an individual makes in relation to sharing their personal confidential data; and
- a strategy to ensure these consent decisions can be shared and provide assurance that the individual's wishes are respected.

Recommendation 9 (section 5.9)
The rights, pledges and duties relating to patient information set out in the NHS Constitution should be extended to cover the whole health and social care system.

Recommendation 10 (section 6.5)
The linkage of personal confidential data, which requires a legal basis, or data that has been de-identified, but still carries a high risk that it could be re-identified with reasonable effort, from more than one organisation for any purpose other than direct care should only be done in specialist, well-governed, independently scrutinised and accredited environments called 'accredited safe havens'.

The Health and Social Care Information Centre must detail the attributes of an accredited safe haven in their code for processing confidential information, to which all public bodies must have regard.

The Informatics Services Commissioning Group should advise the Secretary of State on granting accredited status, based on the data stewardship requirements in the Information Centre code, and subject to the publication of an independent external audit.

Recommendation 11 (section 7.4)
The Information Centre's code of practice should establish that an individual's existing right to object to their personal confidential data being shared, and to have that objection considered, applies to both current and future disclosures irrespective of whether they are mandated or permitted by statute.

Both the criteria used to assess reasonable objections and the consistent application of those criteria should be reviewed on an ongoing basis.

Recommendation 12 (section 7.6)
The boards or equivalent bodies in the NHS Commissioning Board, clinical commissioning groups, Public Health England and local authorities must ensure that their organisation has due regard for information governance and adherence to its legal and statutory framework.

An executive director at board level should be formally responsible for the organisation's standards of practice in information governance, and its performance should be described in the annual report or equivalent document.

Boards should ensure that the organisation is competent in information governance practice, and assured of that through its risk management. This mirrors the arrangements required of provider trusts for some years.

Recommendation 13 (section 8.6)
The Secretary of State for Health should commission a task and finish group including but not limited to the Department of Health, Public Health England, Healthwatch England, providers and the Information Centre to determine whether the information governance issues in registries and public health functions outside health protection and cancer should be covered by specific health service regulations.

Recommendation 14 (section 9.2)
Regulatory, professional and educational bodies should ensure that:

- information governance, and especially best practice on appropriate sharing, is a core competency of undergraduate training; and
- information governance, appropriate sharing, sound record keeping and the importance of data quality are part of continuous professional development and are assessed as part of any professional revalidation process.

Recommendation 15 (section 9.4.2)
The Department of Health should recommend that all organisations within the health and social care system which process personal confidential data, including but not limited to local authorities and social care providers as well as telephony and other virtual service providers, appoint a Caldicott Guardian and any information governance leaders required, and assure themselves of their continuous professional development.

Recommendation 16 (section 10.3)
Given the number of social welfare initiatives involving the creation or use of family records, the Review Panel recommends that such initiatives should be examined in detail from the perspective of Article 8 of the Human Rights Act. The Law Commission should consider including this in its forthcoming review of the data sharing between public bodies.

Recommendation 17 (section 11.2)
The NHS Commissioning Board, clinical commissioning groups and local authorities must ensure that health and social care services that offer virtual consultations and/or are dependent on medical devices for biometric monitoring are conforming to best practice with regard to information governance and will do so in the future.

Recommendation 18 (section 12.8)
The Department of Health and the Department for Education should jointly commission a task and finish group to develop and implement a single approach to recording information about 'the unborn' to enable integrated, safe and effective care through the optimum appropriate data sharing between health and social care professionals.

Recommendation 19 (section 12.9)
All health and social care organisations must publish in a prominent and accessible form:

- a description of the personal confidential data they disclose;
- a description of the de-identified data they disclose on a limited basis;
- who the disclosure is to; and
- the purpose of the disclosure.

Recommendation 20 (section 12.10)
The Department of Health should lead the development and implementation of a standard template that all health and social care organisations can use when creating data controller to data controller data sharing agreements. The template should ensure that agreements meet legal requirements and require minimum resources to implement.

Recommendation 21 (section 13.2)
The Health and Social Care Information Centre's Code of Practice for processing personal confidential data should adopt the standards and good practice guidance contained within this report.

Recommendation 22 (section 13.3)
The information governance advisory board to the Informatics Services Commissioning Group should ensure that the health and social care system adopts a single set of terms and definitions relating to information governance that both staff and the public can understand. These terms and definitions should begin with those set out in this document. All education, guidance and documents should use this terminology.

Recommendation 23 (section 13.3)
The health and social care system requires effective regulation to ensure the safe, effective, appropriate and legal sharing of personal confidential data. This process should be balanced and proportionate and utilise the existing and proposed duties within the health and social care system in England. The three minimum components of such a system would include:

- a Memorandum of Understanding between the CQC and the ICO;
- an annual data sharing report by the CQC and the ICO; and
- an action plan agreed through the Informatics Services Commissioning Group on any remedial actions necessary to improve the situation shown to be deteriorating in the CQC-led annual 'data sharing' report.

Recommendation 24 (section 14.1)
The Review Panel recommends that the Secretary of State publicly supports the redress activities proposed by this review and promulgates actions to ensure that they are delivered.

Recommendation 25 (section 14.2)
The Review Panel recommends that the revised Caldicott principles should be adopted and promulgated throughout the health and social care system.

Recommendation 26 (section 14.3)
The Secretary of State for Health should maintain oversight of the recommendations from the Information Governance Review and should publish an assessment of the implementation of those recommendations within 12 months of the publication of the review's final report.

Glossary

Aggregated data: Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

Anonymisation: The process of rendering data into a form which does not identify individuals and where identification is not likely to take place.

Audit: An audit is an official internal or external examination of an organisation. See 'Clinical audit' and 'Independent audit'.

Audit trail: An audit trail (or audit log) is a record of everyone who has looked at or changed a record, why and when they did so and what changes they made.

Caldicott Guardian: A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing by providing advice to professionals and staff.

Care at home: Social care services provided to a person who remains in their own home; also known as 'domiciliary care'. This care is usually purchased by Social Services on behalf of an individual following an assessment of their needs or is bought directly by someone if they are funding their own care.

Care pathway: A care pathway is anticipated care placed in an appropriate time frame, written and agreed by a multi-disciplinary team. It has locally agreed standards based on evidence where available to help a patient with a specific condition or diagnosis move progressively through the clinical treatment. 'Whole care pathways' refer to the end-to-end process of care for particular conditions from the point of entry to the point of departure from care.

Carer: An individual who provides unpaid care to a patient or service user, most commonly a member of their family or friend. For paid workers, the term 'care worker' should be used.

Care records: Care records are personal records. They comprise documentary and other records concerning an individual (whether living or dead) who can be identified from them and relating:

- to the individual's physical or mental health;
- to spiritual counselling or assistance given or to be given to the individual; or
- to counselling or assistance given or to be given to the individual, for the purposes of their personal welfare, by any voluntary organisation or by any individual who:
  - by reason of the individual's office or occupation has responsibilities for their personal welfare; or
  - by an order of a court has responsibilities for the individual's supervision.

This record may be held electronically or in a paper file or a combination of both.

Care team: The health and/or social care professionals and staff that directly provide or support care to an individual (see sections 3.6 and 3.7).

Care worker: An individual who is paid to care for a service user. People who are not paid are referred to as carers.

Child protection: The process of protecting individual children identified as either suffering, or likely to suffer, significant harm as a result of abuse or neglect.

Children and young persons (or young people): People under 18. 'Young persons' refers to young people where Fraser (Gillick) competency is a consideration (see Fraser Guidelines for Competency).

Clinical audit: Clinical audit is a tool for improving practice, patient care or services provided. It is used to measure current practice and care against a set of explicit standards or criteria, identify areas for improvement, make changes to practice and re-audit to ensure that improvement has been achieved. The findings of the clinical audit provide evidence of the quality of practice and care[117].

Commissioning (and commissioners): Commissioning is essentially buying care in line with available resources to ensure that services meet the needs of the population. The process of commissioning includes assessing the needs of the population, selecting service providers and ensuring that these services are safe, effective, people-centred and of high quality. Commissioners are responsible for commissioning services.

Common Assessment Framework: Common Assessment Frameworks are shared, integrated approaches to assessing the health, social care and wider support needs of individuals. Separate Common Assessment Frameworks exist for both adults and for children and young people.

Confidential data or information: See 'Personal confidential data'.

Consent: See section 3.2.

Continuing care: Care provided over an extended period of time to a person aged 18 or over to meet physical or mental health needs which have arisen as the result of disability, accident or illness. It may involve both health and social care services. The healthcare services are funded by the NHS and the social care services are funded by the local authority and/or the service user.

[117] NICE guidance.

Data: Qualitative or quantitative statements or numbers that are (or are assumed to be) factual. Data may be raw or primary data (e.g. direct from measurement), or derivative of primary data, but are not yet the product of analysis or interpretation other than calculation[118].

Data breach: Any failure to meet the requirements of the Data Protection Act, unlawful disclosure or misuse of personal confidential data and an inappropriate invasion of people's privacy.

Data controller: A person (individual or organisation) who determines the purposes for which and the manner in which any personal confidential data are or will be processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act[119].

- ***Joint data controllers*** control how data is processed jointly i.e. they must agree and make such decisions together.
- ***Data controllers in common*** agree to pool data and are both responsible for how it is used but each may process the data independently for its own purposes. All of the data controllers in common are still responsible for ensuring it is adequately protected.

Data loss: A breach of principle 7 of the DPA or an inappropriate breaking of confidentiality.

Data processor: In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Data processors are not directly subject to the Data Protection Act. But the Information Commissioner recommends that organisations should choose data processors carefully and have in place effective means of monitoring, reviewing and auditing their processing and a written contract (detailing the information governance requirements) must be in place to ensure compliance with principle 7 of the Data Protection Act.

De-anonymisation: See 'Re-identification'.

De-identified data: This refers to personal confidential data, which has been through anonymisation in a manner conforming to the ICO Anonymisation code of practice. There are two categories of de-identified data:

- ***De-identified data for limited access:*** this is deemed to have a high risk of re-identification if published, but a low risk if held in an accredited safe haven and subject to contractual protection to prevent re-identification.
- ***Anonymised data for publication:*** this is deemed to have a low risk of re-identification, enabling publication.

[118] Royal Society (2012) Science as an open enterprise.

[119] Taken from the Data Protection Act and Information Commissioner's Office definitions.

Demographic data: Information relating to the general characteristics of an individual or population e.g. ethnicity, gender, geographical location, socio-economic status.

Direct care: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

Epidemiology: The study of the frequency, distribution and cause of disease in order to find ways of prevention and control. It includes social and environmental factors that influence a disease[120].

Fraser Guidelines for Competency: A set of guidelines used by clinicians to determine whether a young person is mature and capable of understanding the issues and consequences of a decision and being able to evaluate relevant information and make a reasoned decision for themselves. Also sometimes referred to as Gillick competency.

Genetic information: Genetic information is information about the genotype, or heritable characteristics of individuals obtained by direct analysis of DNA, or by other biochemical testing. Genetic information in itself is not always identifiable; personal genetic information refers to information about the genetic make-up of an identifiable person[121].

Genome: The total genetic complement of an individual.

Health service body: Organisations (or individuals) with specific functions, obligations and powers defined in law. In England, the health service bodies from 1 April 2013 are: the Secretary of State for Health (includes the Department of Health, and its Executive agencies such as Public Health England and the MHRA), the NHS Commissioning Board, clinical commissioning groups, NHS Trusts (including Foundation Trusts), special health authorities such as the NHS Business Services Authority, CQC, NICE, and the Health and Social Care Information Centre. Local authorities are not health service bodies.

Honorary/seconded staff: Staff working in the one organisation e.g. a hospital, but employed by other organisations e.g. a university. Another example would be where social workers employed by the local authority are based in a hospital to work alongside health professionals. The agreement between the two organisations ensures that in the event that the individual breaches host organisation rules and procedures their employer will take appropriate disciplinary action on behalf of the host organisation.

[120] http://genome.wellcome.ac.uk/resources/glossary

[121] The Human Genetics Commission identified four categories of personal genetic information: observable or private information and sensitive or non-sensitive genetic information. The Commission concluded that not all personal genetic information should be treated in the same way in every set of circumstances.

Identifiable information: See 'Personal confidential data'.

Identifier: An item of data, which by itself or in combination with other identifiers enables an individual to be identified. Examples are included in Appendix 5.

Independent audit: An audit conducted by an external and therefore independent auditor to provide greater public assurance. See 'Audit' and 'Clinical audit'.

Indirect care: Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit.

Individual funding request: A request to a clinical commissioning group to fund healthcare for an individual which falls outside the range of services and treatments that the clinical commissioning group has agreed to commission.

Information: Information is the "output of some process that summarises, interprets or otherwise represents data to convey meaning." Data becomes information when it is combined in ways that have the potential to reveal patterns in the phenomenon[122].

Information governance: How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning as well as requirements and standards organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

Information governance specialist: A staff member specifically appointed to provide advice, guidance and governance in relation to legal requirements such as the duty of confidence and data protection, the legal basis for information sharing, key requirements in relation to information security, record management, and freedom of information.

Legitimate relationship: The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care.

Linkage: The merging of information or data from two or more sources with the object of consolidating facts concerning an individual or an event that are not available in any separate record.

Never events: 'Never events' are very serious, largely preventable patient safety incidents that should not occur if the relevant preventative measures have been put in place[123]. The list is updated annually and includes for example wrong site surgery and wrong route administration of chemotherapy.

[122] Taken from Royal Society (2012) 'Science as an open enterprise'.

[123] Taken from Department of Health, http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_124552

Personal confidential data: This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'Personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

Personal data: Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Personal information: See 'Personal confidential data'.

Personal record/personal health and wellbeing record: See 'Care records'.

Potentially identifiable: See 'De-identified data for limited access'.

Primary care: Primary care refers to services provided by GP practices, dental practices, community pharmacies and high street optometrists.

Privacy impact assessment: A systematic and comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure for personal data prior to the introduction of or a change to a policy, process or procedure.

Processing: Processing in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data.

Pseudonymisation: The process of distinguishing individuals in a data set by using a unique identifier, which does not reveal their 'real world' identity (see also 'Anonymisation' and 'De-identified' data).

Public interest: Something 'in the public interest' is something that serves the interests of society as a whole. The 'public interest test' is used to determine whether the benefit of disclosing sensitive information outweighs the personal interest of the individual concerned and the need to protect the public's trust in the confidentiality of services.

Re-identification: The process of analysing data or combining it with other data with the result that individuals become identifiable. Also known as 'de-anonymisation'.

Safeguarding: The process of protecting children and vulnerable adults from abuse or neglect, preventing impairment of their health and development, and ensuring they live in circumstances consistent with the provision of safe and effective care. It enables children to have optimum life chances and enter adulthood successfully and adults to retain independence, wellbeing and choice and to access their human right to live a life that is free from abuse and neglect.

Safe haven: An accredited organisation with a secure electronic environment in which personal confidential data and/or de-identified data can be obtained and made available to users, generally in de-identified form. An accredited safe haven will need a secure legal basis to hold and process personal confidential data. De-identified data can be held under contract with obligations to safeguard the data (see section 6.5).

Screening
Screening is a process of identifying apparently healthy people who may be at increased risk of a disease or condition. They can then be offered information, further tests and appropriate treatment to reduce their risk and/or any complications arising from the disease or condition.

Sensitive personal data: Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual. See also 'Personal confidential data'.

Serious incident: A serious event that has led, or may have led to harm to patients, service users or staff — this can apply to both clinical safety incidents and data incidents. Also called 'serious untoward incidents'.

Service user: An individual receiving social care services.

Specialist commissioning: This relates to the purchasing and planning of specialised services for diseases and disorders. Specialised services are defined in law as those services with a planning population of more than one million people. The NHS Commissioning Board is responsible for commissioning specialised services.

Third party: In relation to personal data, any person other than the subject of the data, the data controller, or a data processor.

Unborn: Foetuses between 24 weeks gestation and birth. Different approaches are taken between health and social care in relation to record keeping relating to 'the unborn'.

Appendix 1: Membership of the Information Governance Review

Review Panel Members

Dame Fiona Caldicott (Chair)
Chairman, Oxford University Hospitals NHS Trust

John Carvel
Former Social Affairs Editor, The *Guardian*
Member, Healthwatch England Committee

Professor Mike Catchpole
Head of Epidemiology and Surveillance, Health Protection Agency

Terry Dafter
Director of Adult Social Care, Stockport

Janet Davies
Director of Nursing and Service Delivery, Royal College of Nursing

Professor David Haslam
National Professional Adviser, Care Quality Commission
Co-Chair of NHS Future Forum Information work stream

Dr Alan Hassey
GP with informatics expertise and Academy of Medical Royal Colleges

Dawn Monaghan
Group Manager, Information Commissioner's Office

Terry Parkin
Executive Director, Education and Care Services London Borough of Bromley

Sir Nick Partridge
CEO, Terrence Higgins Trust and Involve

Professor Martin Severs
School of Health Sciences and Social Work, University of Portsmouth

Caroline Tapster
Former CEO, Hertfordshire County Council

Jeremy Taylor
Chief Executive, National Voices
Co-chair of NHS Future Forum Information work stream

Sir Mark Walport
Director, Wellcome Trust

Dr David Wrigley
Commissioning GP

Review Support Team

Launa Broadley
Secretariat

Steve Collins
Department of Health lead

Jenny Craggs
Theme support

Wally Gowing
Theme lead

Suzanne Lea
Head of programme

David Lockwood
Head of drafting

Christina Munns
Theme lead

Karen O'Brien
Secretariat

Eileen Phillips
Media and communications lead

David Riley
Theme lead

Carole Sheard
Theme lead

Clive Thomas
Theme lead

Karen Thomson
Information governance lead

Richard Wild
Review director

Appendix 2: Information Governance Review — terms of reference

The Review will examine:

- the current and future purposes for which patient and social care service user information may be used, in particular, as needed to fulfil the requirements of the Health and Social Care Act 2012;
- the information flows needed to support these purposes where they require information which may be identifiable;
- how the Government's Open Data policy may be facilitated while protecting the confidentiality, privacy and security of personal information;
- when explicit consent for information sharing needs to be sought and recorded, and when may consent reliably be implied and objection/active dissent recorded;
- when should anonymised and pseudonymised data be used;
- when may statutory support or public interest be relied upon, and when should statutory support be sought;
- current guidance/requirements with regards to the publication of statistical analyses that are based on small numerator or denominator sizes;
- information governance education and training for staff to ensure that they have the confidence to share information appropriately;
- current information governance requirements and reporting for organisations, and to consider whether these remain appropriate both for the new and continuing organisational structures;
- current national information governance roles and responsibilities, and to consider how to ensure effective, system wide information governance, following implementation of the Health and Social Care Act 2012;
- what is currently communicated to patients, service users and the public about how their information is used, and what needs to be communicated in future;
- current safeguards and means of redress, and to consider whether they remain sufficient to provide assurance to the public both in terms of the duty of care and breaches of confidence; and
- the potential for facilitation of patient and service user control over their personal data through technology.

Appendix 3: Excerpt from NICE Clinical Guideline 138

These quality statements are from the NICE quality standard on Patient experience in adult NHS services: improving the experience of care for people using adult NHS services in England [CG138].

Quality statement	
1	Patients experience co-ordinated care with clear and accurate information exchange between relevant health and social care professionals.
2	Patients' preferences for sharing information with their partner, family members and/or carers are established, respected and reviewed throughout their care.
3	Clarify with the patient at the first point of contact whether and how they would like their partner, family members and/or carers to be involved in key decisions about the management of their condition. Review this regularly. If the patient agrees, share information with their partner, family members and/or carers.
4	Ensure clear and timely exchange of patient information: between healthcare professionals (particularly at the point of any transitions in care) between healthcare and social care professionals (with the patient's consent).
5	Give the patient (and their family members and/or carers if appropriate) information about what to do and who to contact in different situations, such as 'out of hours' or in an emergency.
6	Patients are actively involved in shared decision making and supported by healthcare professionals to make fully informed choices about investigations, treatment and care that reflect what is important to them.
7	Patients experience effective interactions with staff who have demonstrated competency in relevant communication skills.

Recommendations, or parts of recommendations, that underpin the development of the quality statements and associated measures are denoted [QS] within the Guideline.

Appendix 4: Examples of Information Commissioner's Office actions up to August 2012

In January 2012, a former health worker was prosecuted and pleaded guilty to unlawfully obtaining patient information by accessing the medical records of five members of her ex-husband's family in order to obtain their new telephone numbers.

In December 2011, a receptionist who unlawfully obtained her sister-in-law's medical records in order to find out about the medication she was taking was found guilty of an offence under section 55 of the Data Protection Act.

In June 2012, a personal injury claims company employee was prosecuted for illegally obtaining NHS patients' information.

In August 2012, a monetary penalty of £175,000 was issued to Torbay Care Trust after personal confidential data relating to 1,373 employees was published on the Trust's website.

In May 2012, a monetary penalty notice for £90,000 was served on Central London Community Healthcare NHS Trust for a serious contravention of the DPA, which occurred when personal confidential data was faxed to an incorrect and unidentified number. The contravention was repeated on 45 occasions over a number of weeks and compromised 59 data subjects' personal data.

In April 2012, an undertaking to comply with the seventh data protection principle was signed by Leicestershire County Council, following the theft of a briefcase containing personal confidential data from a social worker's home.

In February 2012, a monetary penalty of £100,000 was issued to Croydon Council after a bag containing papers relating to the care of a child sex abuse victim was stolen from a London pub.

Source: ICO

Appendix 5: List of identifiers for figure 1, simplified framework of data processing from a legal perspective

The following list of direct identifiers was adapted from those published as part of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. The HIPAA Privacy Rule is the first comprehensive federal protection for the privacy of personal health information. More information is available at the website: http://privacyruleandresearch.nih.gov/pr_08.asp

1. Names.
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, Postcode, and their equivalent geographical codes, except for the initial four digits of a postcode if, according to the current publicly available data from the Office for National Statistics and/or the Information Commissioner's Office:
   a. The geographic unit formed by combining all postcodes with the same four initial digits contains more than 20,000 people.
   b. The initial three digits of a postcode for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. National Insurance numbers.
8. NHS number and medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/licence numbers.
12. Vehicle identifiers and serial numbers, including licence plate numbers.
13. Device identifiers and serial numbers.
14. Web universal resource locators (URLs).
15. Internet protocol (IP) address numbers.
16. Biometric identifiers, including fingerprints and voiceprints.
17. Full-face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Information Commissioner's Office.

Appendix 6: Contracting arrangements

This appendix sets out the requirements for contracting arrangements in relation to the use of personal confidential data and de-identified data for limited access. Data should be utilised in the health and social care system for legitimate purposes that are in the public interest. However, it is imperative that both personal confidential data and de-identified data for limited disclosure or limited access are protected to ensure that the confidentiality and privacy of individuals is not breached.

Contracts are a key mechanism in providing this protection and must be legally enforceable. The Panel recognises that this raises difficulties for 'health service bodies' (as defined in legislation) where they contract with one another. They are required to use 'NHS contracts' that are not legally enforceable. Health service bodies should act as though NHS contracts are legally binding. Regulations under Section 251 of the NHS Act 2006 have been proposed to create a mechanism for enforcement.

Contracting requirements

The elements that need to be included in contract provisions are set out below. It is important to recognise that the contract itself is only one aspect to contracting and that there are four stages to the contracting process. Documentation of each stage is required to demonstrate due diligence. The four stages are:

- procurement requirements — pre-contract checks;
- legal provisions of contract (and supplementary Service Level Agreement/DSA provisions where applicable);
- contract performance management — this includes having a nominated manager and audit and will need to be resourced; and
- contract exit management.

Where the contract is for the supply of services, these contract provisions form part of the NHS Standard terms and conditions to ensure there is consistency across the content of each contract. It may be that many of these provisions would be included within a schedule to the contract. This could allow for amendment of the Schedule without the full contract needing to be re-signed, but the changes would need to be agreed and signed by appropriate senior responsible officers. The contracts should be prepared or at least reviewed by legal counsel to ensure that they are lawful, and legally binding (with the above exception for NHS contracts).

Table of contract requirements in relation to the use of data

This table is intended to be comprehensive but may be incomplete. There may also be instances where some of the requirements are not applicable but the Review Panel concludes that these requirements will apply in most circumstances. Additionally, there may be elements that overlap with other contracting requirements, so these will need to be drawn together appropriately.

Requirements	
1	Define the status and relationship of the parties as data controller or data processors. This includes clarity about sole, joint or in common data controllership, and where an organisation's relationships with data may fall across these categories in different circumstances, to clarify the circumstances in which the different relationships with the data will apply.
2	Define scope and term of the contract.
3	Whether the contract will be supported by Service level/data sharing agreements (where applicable to define data set and disclosures for specific purposes. This should include any variation to the data controller relationships set out in the contract).
4	Define terminology used.
5	Legal, professional and contractual requirements. Definition of the governing law (i.e. England), requirement to adhere to legal and professional requirements, and the provisions of this contract in particular in relation to Data Protection, Human Rights and common law obligations such as the duties of care and confidentiality. This includes but is not limited to: • when personal confidential data may lawfully be disclosed; • for de-identified data for limited disclosure or access the requirement for this data to be held separately from personal confidential data within a safe haven (to ensure it does not become identifiable, and therefore personal data requiring a legal basis to process); • having mechanisms to prevent re-identification where de-identified data may be linked together in a safe haven; • a requirement not to disclose data to other parties other than in anonymised form, or as authorised by the data controller, or where required by law; and • for data processors the requirement only to process data as instructed by the data controller.
6	Duty to co-operate with other parties.
7	In relation to personal confidential data, a definition of the purposes and the legal basis for processing for each specified purpose, with a restriction to confine processing to these purposes, where there is a need to re-identify individuals, this must be in the purposes and authorised. It is helpful to include this within the contract so all parties are assured of the legal basis for processing and the boundaries of that legal basis. (Privacy impact assessments are helpful in clarifying whether there is a secure basis in law and the nature of that basis as part of the pre-contract checks and ongoing management of the contract.) In relation to de-identified data for limited disclosure or access, clarity of the purposes and assurance that the purposes of processing are in the public interest.
8	Confidentiality and protection of commercially sensitive information and intellectual property.

9	Fair processing information responsibilities — service user involvement in its development.
10	Policies and procedures on: consent both for treatment and for the use of data; conflicts of interest management; and agreement more broadly about whose policies are used. This may be specific to the policy in question.
11	Timely communication of transfer or discharge information to other care professionals.
12	Online access to records and communication of care plans to the service user.
13	Conformance with requisite Information and Data Standards.
14	Staff recruitment checks, education and training, and terms and conditions of employment — this also needs to address honorary and seconded staffing arrangements to ensure the failure to adhere to policies and procedures are addressed through disciplinary action via the substantive contract of employment.
15	Maintenance of Information Asset Registers, data flow mapping and data sets for extraction and reporting requirements.
16	Data extraction processes.
17	Responsibility for FOI, EIR and subject access requests — in particular attention needs to be given to who will undertake the clinical review of records for Subject Access Requests to ensure that seriously harmful information, or information provided by third parties is not disclosed.
18	Housekeeping measures: • business continuity; • disaster recovery; • monitoring and auditing of access controls and reporting; and • transfer, retention, archiving, and disposal of records at end of data lifecycle in line with DH record retention schedules or termination of contract.
19	Security requirements (ISO 27001 and 2) ISMS to include: • network security; • device security (including encryption); • software security including protection against malware; • data and system back-up; • secure transfer of data; • physical security; • access control functionality, logging, alerts, auditing and reporting; • software control of printing and USB devices; • use of security and privacy enhancing technologies; • risk assessment, audit and reporting (including penetration testing); • review and updating; and • incident reporting.
20	Registration Authority (RA) — Legitimate Relationship (LR) and Role Based Access Control (RBAC) authorisation and implementation.

21	Change control, authorised officers and approvals processes.
22	Sub-contracting notification to data controller of intent to sub-contract, identity of sub-contractor(s), contracting and oversight arrangements of sub-contractor and authorisation by data controller requirements.
23	Location of data storage and arrangements i.e. within EEA, outside EEA, or cloud. Need for binding corporate rules or other means of satisfying DP principle 8.
24	Serious incidents/data breaches (duty of candour): monitoring, reporting, investigating, publishing with outcomes.
25	DC contract performance management including right of access to visit site(s) and audit procedures/use of data including any sub-contractors. Additionally, mandatory independent audit of the IG Toolkit submission or equivalent statements of compliance should also be considered, with the scope set annually by the data controller.
26	Process for agreeing variations to the contract including novation to new bodies.
27	Dispute resolution process.
28	Exit from contract: • natural end of contract considerations such as record management; • premature end of contract from failures of any party e.g. bankruptcy, serious data breach; and • continuing obligations, e.g. not using data subsequently for own purposes and maintaining confidentiality of personal data indefinitely.
29	Charges, liability and indemnity, remedies and penalties for breach of contract — care needs to be taken to ensure that this clause includes unlimited recovery of costs arising from a breach by data processor and data processors need to maintain insurance supporting liability in the contract.
30	Definition of roles and responsibilities — senior responsible officers for implementation and oversight of different elements of the contract for each party to the contract.
31	Signatures of senior responsible officers of all parties.
32	An appendix to the contract, with the day to day contact details for the senior responsible officers and other key staff.

Sources:

CEN WORKSHOP AGREEMENT CWA 15292 May 2005

Commissioning Board SLA Mock Template and Collaborative Commissioning Agreement http://www.commissioningboard.nhs.uk/resources/resources-for-ccgs/

National Standard Contracts

PASA IT Documentation — NHS Supplementary conditions of contract relating to information security August 2009

ICO — Model Contract Clauses – International transfers of personal data

ICO — Privacy Impact Assessment

DH guidance on completing national variation deeds for all national contracts

2900774 March 2013
Produced by Williams Lea for the Department of Health