Building the Information Core

Protecting and Using Confidential Patient Information

A Strategy for the NHS

Information Policy Unit
December 2001

CONTENTS

1. EXECUTIVE SUMMARY

1.1 Introduction

1.1.1 The Government has made it clear that the fundamental principle governing the use of information that individuals provide in confidence to the NHS is that of ***informed consent.*** This is rooted in both legal and ethical requirements, but is also an essential element of an open and honest partnership between patients and the NHS that is based on trust.

1.1.2 Even in circumstances where consent is not required, the requirement to inform still applies and again this requirement has both a legal and an ethical basis. Consent is not required where information has been effectively anonymised or where the law requires its disclosure. However, patients have a right to know that it is intended that their information will be anonymised for a range of appropriate purposes and to know that there are legal requirements and why these requirements exist.

1.1.3 The NHS has not got a good track record in this area. In 1997, the Caldicott Committee found that there was little awareness of requirements around confidentiality and consent and that practice was generally poor. Awareness has grown steadily since then with the introduction of new legislation and more recently through high profile and justifiably critical attention on Bristol and Alder Hey. Work centred around implementing the Caldicott recommendations has begun raising standards, but in many organisations has not been given great priority to date amongst a host of competing needs.

1.1.4 If the principle of informed consent to the use of confidential information is to be made real, then considerable change is needed. This document outlines a strategy for delivering this change.

1.2 What changes are required?

1.2.1 There are two broad objectives:

- building an NHS that uses confidential information with the informed consent of the patients who provide it; and
- ensuring that the NHS uses confidential patient information fairly and lawfully and meets all relevant ethical standards.

1.2.2 Little attention has been given to these objectives in the past. Decisions about the use of confidential patient information have generally been made out of the sight of patients. This is no longer tenable. As already stated, patients have a right to be informed about how information they provide in confidence may be used and who, in broad terms, may see it. Transparency however, whilst essential, does not in itself provide a sound basis for processing confidential patient information. When information is provided in confidence, one of the following must apply:

- a legal requirement to disclose information must be complied with;
- the public interest may, in exceptional cases, after consideration of the individual circumstances, justify disclosure;

In other circumstances, where practicable,

- the information must be anonymised, either irreversibly or, with appropriate safeguards, reversibly (termed pseudonymisation);

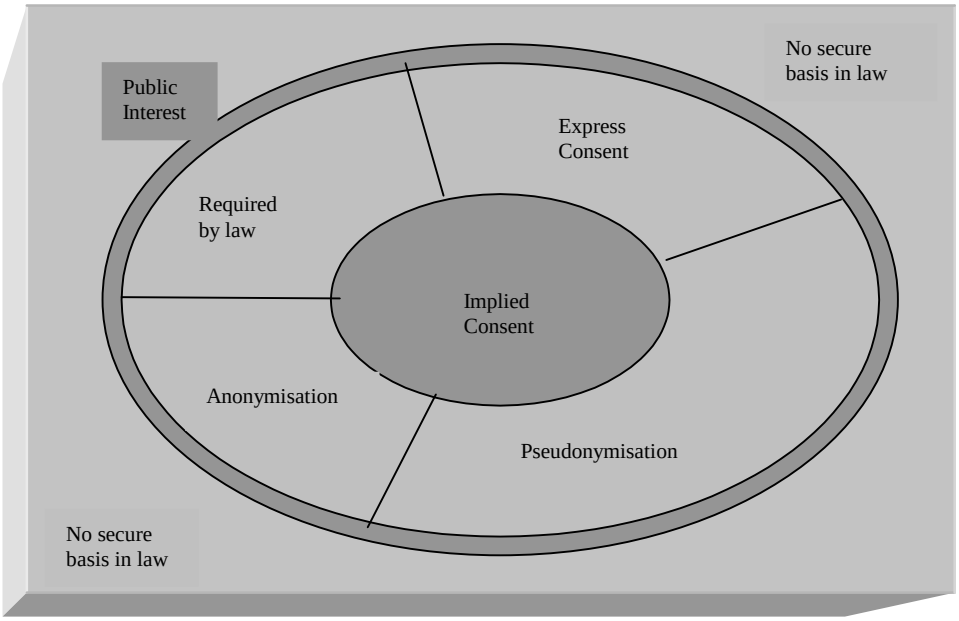
Where there is no legal requirement to disclose, the public interest is not clearly sufficient justification and anonymisation is impracticable, the consent of patients is required.

- valid consent can reasonably be implied in some circumstances
- consent must be sought and expressed, orally or in writing, in circumstances where it can't be implied

1.2.3 The following diagram illustrates all these different possibilities and highlights the fact that when confidential information is used to support a particular purpose (i.e. the information is processed in data protection terms) then it is either within the circles and therefore has a basis in law, or it is outside and therefore has no secure basis.

1.2.4 Where a person does not have the capacity to provide a valid form of consent, other legal mechanisms come into play, but these supplement rather than detract or deflect the approaches required where consent is attainable.

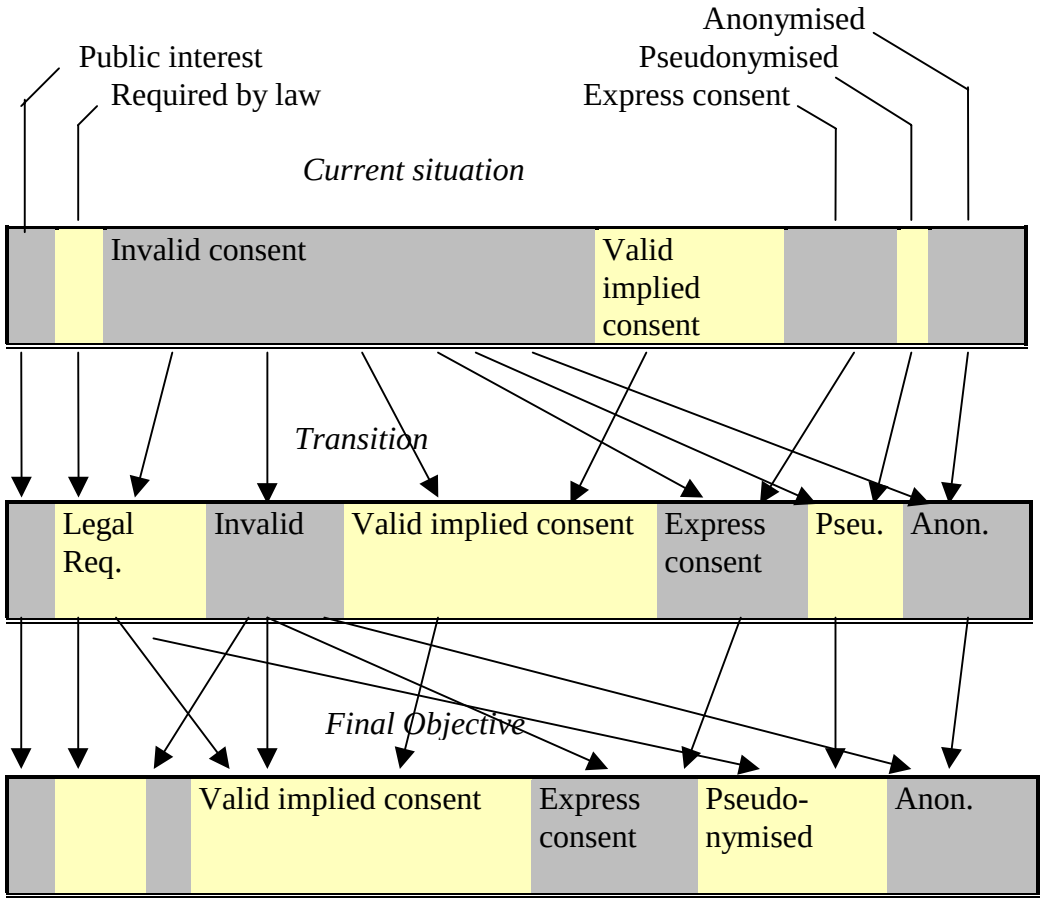
Figure 1: The basis in law for processing confidential patient information



1.2.5 The next diagram illustrates where the NHS is now, how this must change during a transitional period – starting immediately - and where it must aim to be in five years time. Change will be easier, and will therefore occur sooner, in some areas and not in others.

1.2.6 During this transitional period there is a need to inform and educate patients to maximise the validity of implied consent. There is also a need to increase reliance upon anonymised data and make pseudonymisation a practicable alternative for many areas of work, to ensure that express consent is sought where this is required and to provide transitional support in law for essential activity whilst changes are made to systems and processes.

Figure 2: Legitimising the use of confidential information over a 3-5 year period



1.3 How do we get there?

1.3.1 Change on the scale envisaged will require careful management and will need to be phased. Key to this is the building of consensus amongst all stakeholders on what might reasonably achieved by when. There are a number of issues to be resolved if we are to successfully make the changes that are required. These can be grouped under the following headings:

- **Preparing the Ground**
  There is a need to promote a clear understanding of what is meant by informed consent, express consent, public interest, anonymisation and pseudonymisation. Options for change need to be identified and action prioritised according to the availability of resources and risk. Procedures for justifying use of new legal powers must also be agreed.

These need to be tightly controlled and limited to circumstances where need and justification have been robustly and publicly demonstrated.

- **Communications with the Public**
  The provision of information is the key to transparency and underpins valid consent and public awareness of rights. There is also a need to convey the importance of NHS activity that relies upon confidential patient information and to reinforce and build on patient trust in the NHS.

- **Cultural Change**
  NHS staff need to be trained and prepared for the changing relationship with patients and need to know how to deal with expressions of concern and requests for information. They also need to be aware of the requirements of law, ethics and policy and should work to agreed codes of practice.

- **Securing the Confidentiality of Patient Information**
  Some of the change that is required to record and respect patient preferences needs new technology to be put in place and new ways of working to be developed. A far better understanding of how information is used is required at a local level and appropriate security measures and privacy enhancing technologies, up to and including encryption, need to be put in place.

- **Information Governance and Caldicott**
  The work that is needed to improve standards needs to be clearly understood, effectively resourced, and constructively managed. The Caldicott work programme needs to be strengthened and extended into partner organisations. A process for challenging traditional uses of confidential information is required and barriers to increased reliance on anonymisation and pseudonymisation dismantled.

1.4 Implementation

1.4.1 The following table summarises the required actions identified in this strategy document.

Preparing The Ground	Communications with the Public	Cultural Change	Securing Confidential Information	Information Governance & Caldicott
❑ The NHS Executive Information Policy Unit will ensure that all key patient and professional groups are aware of and understand the Strategy on Protecting and Using Confidential Patient Information. ❑ A new Standing Advisory Committee – the Patient Information Advisory Group (PIAG) - will be created to steer implementation of the strategy, agree standards and advise on the use of new legal powers to support certain uses of confidential patient information. ❑ The definitions and terms relevant to work on confidentiality will be agreed with all key parties. ❑ The possibility of developing guidance on public interest justification for disclosing confidential patient information will be explored	❑ A communication strategy, with both national and local components, that will effectively inform patients of how confidential information is used and will satisfy the requirements of law, ethics and policy, will be developed in consultation with key interested parties. ❑ A Public relations strategy, running alongside the provision of information, will be developed to bolster public confidence in, and support for, the ways the NHS uses information. ❑ The phasing of information provision, and particularly information about rights, will reflect the developing capacity of the NHS to respond effectively to patient preferences.	❑ A code of practice, agreed by all key stakeholders, dealing with the handling of confidential patient information by NHS staff, will be developed to replace DoH guidance on confidentiality. ❑ All staff in the NHS, including contractors, should be subject to strict confidentiality clauses in their contracts. The current situation will be reviewed and remedial action taken if necessary. ❑ Computer based learning and awareness raising packages, tailored to organisational type and circumstances will be urgently developed and provided to all NHS organisations. ❑ All NHS staff who have access to confidential patient information will receive appropriately tailored training in confidentiality issues.	❑ Proposals for identifying and dismantling barriers to the adoption of the NHS Number will be developed and action taken. ❑ Options for increasing the presence of the NHS Number in key information flows will be developed and action taken. ❑ Proposals for pseudonymisation of patient information utilising an encrypted NHS Number will be agreed with relevant interests and implemented. ❑ Options for pseudonymising historical data sets will be considered. ❑ Guidance on the structure and functionality of electronic records in respect of the rights of patients will be developed and issued. ❑ Guidance on database design and inference control will be developed and issued. ❑ Requirements for audit, access controls and capacity to reflect patient preferences will be included within primary care system requirements and clarified generally for systems suppliers. ❑ Options for respecting absolute demands or requirements for privacy will be developed.	❑ Proposals for Information Governance will be developed for the National Information Policy Board. This includes the development of a coherent framework for initiatives that set standards for holding, obtaining, recording, using and sharing information. ❑ The work currently underway to implement the Caldicott recommendations will be reviewed and if necessary augmented or given higher priority. ❑ External agencies that need access to confidential NHS information, such as social services, will be encouraged to adopt Caldicott standards. ❑ Exemplar protocols governing all routine and other key information sharing with external agencies will be developed. ❑ National and local work, building on the work conducted by the Caldicott Committee in 1997, will identify uses of confidential information that should cease or should switch to anonymised or pseudonymised data.

2. BACKGROUND

2.1 Understanding the need for change

2.1.1 Awareness of the importance of confidentiality in the immediate environment of clinical care remains strong and is well supported by professional codes and guidance. However, information provided in confidence has, as technology has evolved to support this, increasingly been exploited as a valuable resource. Undoubtedly much good has resulted. The small percentage of patients who have been both aware of how information is used and concerned enough to raise their voices, have had little opportunity to influence systems and processes.

2.1.2 The introduction of new Data Protection and Human Rights legislation has irrevocably changed this situation with the introduction of enforceable rights. Some of these rights are not new, but the right of patients to exert a degree of control over how the information they provide in confidence is used has not been well respected by the NHS. This has not, largely, been a matter of conscious decision. The perceived benefits to the many, the perceived lack of detriment to the largely unaware individual, and sometimes the needs of efficiency and expediency, have shaped a culture that has proven to be demonstrably out of step with the expectations of modern society.

2.2 Understanding the context

2.2.1 The following sections outline the historical context and begin to define the problems that must be solved if appropriate change is to be delivered. Appendix A illustrates some of the myriad ways in which confidential information is currently used.

2.2.2 Government policy on informed consent has crystallised in response to Alder Hey and Bristol, and this applies as much to use of confidential information as to decisions about treatment, post mortem procedures and use of organs and tissue. However, consent to use of confidential patient information presents rather different problems to these other areas of activity. For the majority of patients, the ways that information is used are opaque and non-threatening – whereas treatment and organ retention are readily understandable and have a quality of significance and immediacy that use of information generally lacks.

2.2.3 Nevertheless, there is a sizeable and growing minority of patients who are concerned about potential abuse of the trust they place in the NHS. Concerns may be matters of general principle or may reflect the circumstances of the individual concerned. Studies have consistently shown that concern about how information may be used increases as understanding of how it may be used itself increases. This creates a significant challenge for the NHS to strengthen and build on the trust that still exists.

2.3 Historical overview

2.3.1 Issues of confidentiality and privacy have been central to the provision of healthcare since the time of Hippocrates. More recently the challenges of the Information Age have led to concerns at home and abroad over the protection of health information and in many countries increasingly restrictive regulatory legislation. Personal health information is now used not only for the provision of direct care, but also for a myriad of purposes ranging from management to medical research.

2.3.2 Since the mid 1980s there have been a plethora of publications and legislation in the UK relating to the use and protection of personal information. Below is a timeline showing the key publications and legislation relating to healthcare information from 1984 to the present day.

2.3.3 The work programme that resulted from the Caldicott Review of how the NHS uses confidential patient information has begun to raise standards and develop awareness of issues around the NHS. In particular, the requirement for each organisation to have a Caldicott Guardian, generally Board level representatives of wider teams working on related issues, has helped drive change, but progress has been patchy across the service as a whole.

2.3.4 In the last year, confidentiality issues have risen to the top of the professional and health agenda in response to stakeholder concerns and the enactment of the Data Protection Act 1998 ("DPA 98") and the Human Rights Act 1998 ("HRA 98"). Even more recently, the issue of informed consent has risen to prominence as government policy has crystallised in response to the events at Bristol and Alder Hey.

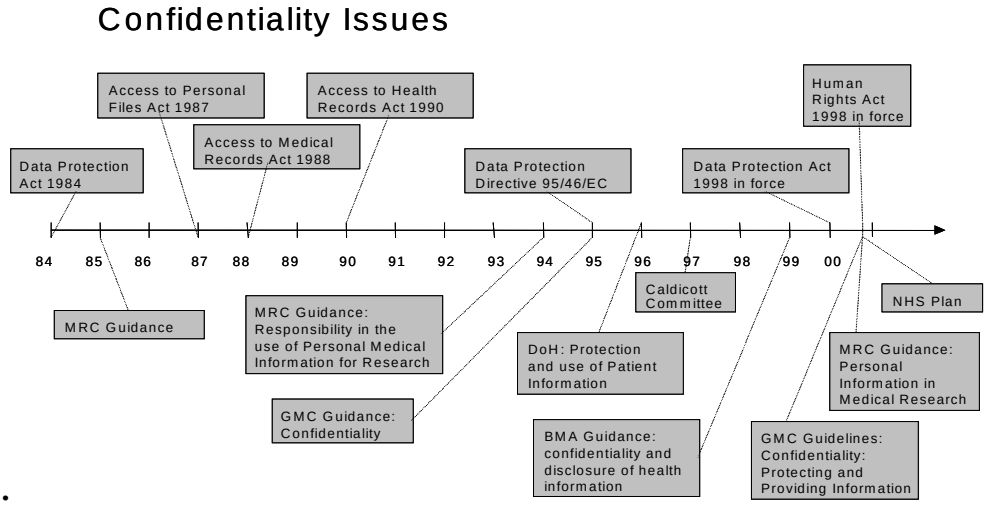


Figure 3 - Confidentiality Issues Timeline

2.4 Rights to privacy vs. Benefits to society

2.4.1 There is a potential conflict between protecting the privacy and confidentiality of individual patients and realising benefits to society from allowing access to such information – for example, to medical researchers investigating the cause of disease. The Human Rights Act 1998, with its emphasis on respect for private life, strengthens the hand of those advocating increased privacy. Modern IT compounds the potential problem by facilitating easy transfer of data, but may also allow closer control and auditing and other privacy enhancing mechanisms.

2.4.2 The tension between individual rights and public good in this area is complex and difficult to resolve conclusively in terms of purely legal requirements that are, in many cases, open to interpretation and difficult to enforce. However, there is an additional ethical dimension that relates to the evolving relationship between the NHS and patients.

2.5 Government Policy: Informed Consent

2.5.1 The Government has made a very public stand on the issue of informed consent. The Secretary of State for Health has, in the context of Alder Hey, made it clear that

> *"The traditional, paternalistic attitude of the NHS that the benefits of science, medicine or research are somehow self-evident regardless of the wishes of patients or their families is no longer acceptable."*

2.5.2 The Minister for Health, speaking to a House of Commons Committee on the issue of using confidential patient information has said:

> *"Informed consent is crucial to the Government's view of how a modern NHS should work. We simply cannot move to a patient centred service if patients are not informed and consenting participants in the services they receive.*
>
> *But as we all know too well this is not the way the NHS operates at the moment. Much of what is done in the NHS relies upon implied consent. In some cases this is appropriate, for example sharing information within a hospital to ensure a patient receives appropriate care, but in other cases the definition of implied consent is pushed much too far.*
>
> *We are determined to address this. It is no small task, and the culture of the NHS will have to change radically as we move away from our comfortable habits and into practice based on real consent."*

2.5.3 Although the NHS Plan did not address the issue of informed consent to the use of confidential patient information directly, the strategic direction set by the Plan is clear and the confidentiality strategy outlined in the following pages should be seen as a logical development. Two of the NHS core principles set out in the NHS Plan are directly relevant to the issues of patient choice, privacy and confidentiality:

- The NHS will shape its services around the needs and preferences of

individual patients, their families and their carers; and

- The NHS will respect the confidentiality of individual patients and provide open access to information about services, treatment and performance.

2.5.4 The NHS Plan did however squarely address the issue of informed consent to treatment and called for improvements across the NHS to ensure that the central importance of the rights of each patient are recognised. Whilst it might be argued that there are significant differences between treatment and use of information, the relationship with patients should essentially be the same.

2.5.5 Whilst the approach adopted in respect of seeking and recording patient consent to treatment is unlikely to reflect the approach needed in respect of consent to use of information, where it can it should.

2.6 The Requirements

2.6.1 Prior to Government policy on informed consent firming up from an ethical and patients' rights perspective, the problem facing the NHS over confidentiality was essentially one of risk management. The NHS had to balance the risk of challenge to its data processing activities with the cost of reducing that risk. Eliminating risk of challenge entirely is probably impossible. Even if every member of the UK population were to sign a consent form covering every possible use and disclosure of data by the NHS, the risk of challenge would still exist. Individuals could always claim that the consent information was not clear or did not cover a particular circumstance.

2.6.2 The cost of such an undertaking is also likely to be out of all proportion to the risk from challenge. It has been estimated that the cost of consenting the whole UK population to be over £400 million[1] yet the number of challenges to the NHS over its use of data remains small. A survey of NHS Eastern Region Acute Trusts only found evidence of one challenge to a hospital's use of confidential data though clearly it is difficult for people to challenge activity that they are unaware of.

2.6.3 However, the issue is no longer entirely one of managing risk, though an element of this persists as there will be a need to prioritise change. Moreover, deciding to bear risk and not change traditional practices that disregard the need for transparency is no longer an option.

2.7 Legal Issues

2.7.1 The Information Commissioner has made clear her view that the NHS is not fully complying with the laws of confidentiality, primarily the DPA 98 and Common Law. Also, professional groups within the NHS currently breach guidance relating to confidentiality from their own regulatory bodies in the course of carrying out their

[1] Estimate derived from a study into consent issues carried out by Cambridge Health Informatics on behalf of the NHS Executive. The figure is derived as follows: 60m members of the public, £1 cost of letter and form to patients; 50p cost of return, probability of only 30% response so multiple follow-ups required, and assumed 50p cost of data-entry and validation: 60m x ((1.00 + 0.50)/30% + 0.50) = £330m plus follow-up every 5 years, £66m

NHS duties. The most significant regulatory body is the General Medical Council, which issued new guidance on confidentiality in September 2000. Other regulatory and stakeholder groups such as those representing patients and medical researchers have recently issued new guidance and are actively involved in the confidentiality debate.

2.7.2 Essentially, where information that identifies a patient is concerned, the relevant law requires:

- DPA 98: Processing must be for a medical purpose and be carried out by an organisation that has a legitimate interest in processing health information unless the patient consents to other purposes or circumstances.
- DPA 98: Processing must be transparent and must meet 'fair processing' requirements (essentially, patients should be told in general terms who will use information about them and for what purposes).
- Common Law: Processing requires consent or must be required by law (exceptionally the public interest may justify overriding the need for consent).

2.8 Transparency

2.8.1 The Information Commissioner (previously Data Protection Commissioner) is concerned that NHS use of patient information is not transparent and that data subjects appear to be told very little about what happens. There is an apparent gap between patients' expectations about how information they provide in confidence will be used and what happens in reality. In fact, little research has been carried out into patients' expectations.

2.8.2 It is, however, reasonable to suggest that the provision of information to patients by the NHS falls short of what is required by the fair processing requirements, especially if patients are expected to understand what is happening to their data. Attempts to provide information to patients have been made but their implementation has been haphazard and ineffective, relying on passive communication through posters on NHS premises. This centrally led initiative to inform patients through notices and posters was left to local NHS bodies to implement, and has had little impact. A key question, as yet unresolved, is how the NHS should communicate fair processing information in such a way that patients understand what happens to their personal data.

2.8.3 Many commercial organisations probably consider that their registration with the Office of the Information Commissioner constitutes sufficient 'informing' of the public of their use of data – this was generally the interpretation under previous Data Protection legislation. Larger commercial organisations also seek to inform the public on forms that gather information from customers – usually with a 'tick-box' to limit further distribution.

2.8.4 These methods would not be accepted as sufficient 'fair processing information' for a large Government agency such as the NHS. Health information is too sensitive and the risk of detriment to patients too great. However, even at this level it is obvious that individual Trusts have widely varying registrations with the

Commissioner, leading to inconsistency (they cannot all be right) and confusion to any member of the public who might seek to gather information via this route. This is largely due to a lack of understanding within Trusts about how they use information and insufficient priority being given to these issues in the past.

2.8.5 However, the requirements of a relationship with patients based on informed consent, are likely to prove far more demanding that the minimum standard required by law.

2.8.6 A solution to the problems of transparency and fair processing needs to address the following points:

- How should information be communicated to patients?
- What information should be given in order to meet the fair processing provisions?
- How can public understanding be enhanced and how can the trust patients have in the NHS be strengthened?

2.9 Consent

2.9.1 The current situation is that NHS relies, by default, on the 'implied consent' of patients to disclosure of confidential information in the vast majority of cases. This consent is implied on the assumption that patients understand all the uses to which the NHS puts their personal information. Patients however do not understand these uses due to the current lack of transparency that exists in the NHS. As a result, implied consent is unlikely to be valid for all uses of confidential information at present. Issues of NHS transparency and the provision of fair processing information are, therefore, intimately connected with issues of consent.

2.9.2 The legal view underpinning the guidelines published by the General Medical Council, which the Department of Health accepts as essentially correct, is that implied consent can be a valid form of consent for the NHS for certain uses of patient information, provided that patients are given fair processing information, are aware of the right to object or opt-out and are given the opportunity to exercise that right. The NHS falls short of this 'legitimacy' by not providing fair processing information, not informing patients of their rights to object, and not having mechanisms in place to support opt-out.

2.9.3 For certain data uses, such as those beyond immediate clinical care but which may affect the patient as a result of the data flow, implied consent is unlikely to be appropriate, even if valid. In these circumstances express consent should be sought. The possibility of adopting procedures for obtaining express consent which mirror those being developed for consent to treatment needs to be considered.

2.9.4 Consent implies that there is some choice. If there is no choice, then there can be no valid consent. The validity of consent is also dependent on the quality of information given. The more explicit the information given to data subjects about how their information is used, the less likely the validity of any consent given will be open

to challenge.

2.9.5 A solution to the problem of consent needs to address the following points:

- Which data flows should implied consent cover?
- Which data flows need to be covered by express consent?
- What information needs to be given to the data subject for consent to be valid?
- How is consent/withdrawal of consent to be recorded and acted upon?

2.10 Anonymisation/Pseudonymisation

2.10.1 Although the need for transparency must always be addressed, once information no longer identifies individual patients there are no existing legal restrictions on its use. The NHS should still act responsibly as in some circumstances there will be a small risk of a patient's identity being determined, inadvertently or deliberately, by combining data from multiple sources.

2.10.2 Anonymisation may be irreversible, so that there can be no means of re-establishing identity, or reversible (termed pseudonymised) where some form of code or tag remains attached to a particular item of information. Although pseudonymised data requires careful handling and safeguards to be in place, either form of anonymisation can be sufficient to render information no longer confidential.

2.10.3 The attractions of anonymising information are clear. It safeguards privacy and confidentiality whilst removing most of the legal obstacles to its use. Uses of information other than for the direct provision of healthcare to the individual rarely require the individual to be identified. However, the need to link episodes of care and prevent duplication of data means that information must be matchable/linkable.

2.10.4 This need has required that information flowing into databases contains personal identifiers including name, address, and date of birth, even though there has been (usually) no intention to use these details to identify an individual. The NHS Number is also used as a unique identifier to allow matching/linking but is not always available when an information flow dataset is generated. Dependence upon a single identifier may also prove problematic if mis-entry rates are found to be high (though the risk of mis-entry of the NHS Number is alleviated through the inclusion of a check digit). These problems should be addressed over the next few years.

2.10.5 A solution to the problem of encouraging wider use of anonymisation techniques needs to determine:

- Where should the NHS be required to use anonymisation or pseudonymisation now?
- What are the barriers to the use of anonymisation and pseudonymisation?
- What technical solutions can be developed to support greater reliance on anonymisation and pseudonymisation?

2.11 Introducing New Statutory Requirements

2.11.1 Where there is a legal requirement to disclose information it is lawful to do so without consent, though the issue of transparency must still be addressed. However, legislation that sets aside the need for consent cannot and should not be undertaken lightly and must be subject to strict safeguards. If it is to comply with the expectations of society and the rights-based thrust of European Union law, then any intrusion into the private lives of individuals needs to be robustly justified.

2.11.2 The basis for laying regulations that require and regulate the use of confidential patient information is provided by the Health and Social Care Act 2001. This incorporates a range of safeguards that will, where the power is invoked, need to be tailored and enhanced to fit the specific circumstances.

2.11.3 Health Ministers have stressed in Parliament that this is a largely transitional measure intended to support important activity during a difficult period of change. It does not signal any move away from the principle of informed consent forming the basis of NHS use of confidential patient information. There is a requirement built in to this legislation for the Secretary of State to review annually whether the support of this power continues to be warranted.

2.11.4 A solution to the issue of where it is appropriate to introduce new legal requirements needs:

- To identify which purposes should be supported, at least temporarily, by law
- To determine, in each case, what safeguards need to be put in place.

2.12 Public Interest

2.12.1 It has long been accepted in law and by professional regulatory bodies that the public interest can, in exceptional cases, override the need to obtain consent prior to disclosing or using information for a particular purpose. The need to consider each such case individually and to apply a rigorous but indeterminate test means that the public interest is little understood and almost certainly used either too frequently or insufficiently to justify disclosure by different parts of the NHS, e.g. to the police.

2.12.2 A solution to the problem of encouraging appropriate reliance on the public interest requires:

- An exploration of public interest justifications for disclosure of information without consent, and, possibly, the development of appropriate guidance.

2.13 Culture Change

2.13.1 Many of the confidentiality issues within the NHS are not complex. Simple measures may go a long way to improving patient confidentiality and reducing the risk of breaches and subsequent complaints and litigation. A general enhancement of the duty of confidentiality and awareness of confidentiality issues by NHS staff, including

senior managers, would help prevent inadvertent disclosures. Examples of these include:

- Staff discussing patients in public areas such as elevators or canteens
- Poorly designed wards and cubicles hindering privacy
- Inadvertent disclosure of patient information over the telephone, especially from the practice of 'blagging' (fraudulent enquiries).

2.13.2 At the same time, there is a need to ensure that staff understand the requirements of law and ethics, that they appreciate the need for changes to systems and processes and that they are able to deal with patients in partnership, respecting preferences and addressing concerns.

2.13.3 A solution to the issues of changing NHS culture requires:

- The development of guidance for the NHS on required practice
- The provision of training and distribution of educational material
- Effective management of a standards-based approach to improvement.

2.14 Risk Management

2.14.1 It is impossible to eliminate the risk of challenge in respect of any use made of confidential patient information, though this strategy aims to minimise that risk. At the same time, it is unlikely that sufficient resources will be available to change all traditional practices and update all existing systems at the same time. There is clearly a risk that resources that might otherwise be used to improve the quality of services in other ways are used inefficiently or inappropriately.

2.14.2 An element of risk management will therefore be required both nationally and locally when setting priorities and considering different options for change.

2.14.3 A solution to the management of risk requires:

- Work to identify which uses of information are most likely to generate concern
- Work to identify the options for change
- Prioritisation of change in line with available resources and risk.

3. BUILDING THE STRATEGIC APPROACH

3.1 Developing a Strategic Approach

3.1.1 The section on problem definition identified a range of issues that need to be addressed. Some of these issues are closely linked to others, for example the information that must be provided to patients to support transparency and that which must be provided to support consent. These linked issues can sensibly be grouped thematically with an eye to the work that will be required to resolve them. The resulting groupings are the component elements of the wider strategy. They are:

- Preparing the ground;
- Communications with the Public;
- Change Management;
- Securing Confidential Patient Information; and
- Information Governance.

3.1.2 The following sections outline the actions that are required to address the issues associated with each of the component elements of the strategy for Protecting and Using Confidential Patient Information.

3.2 Next Steps

3.2.1 The final section outlines the next steps and starts to flesh out the possible timetable for delivering the actions identified. It is extremely important that all interested parties accept and agree the timetable for delivering the change that is needed. Change of the scale required is rarely achieved without a degree of disruption and in an area such as healthcare it is vital that disruption is planned for, managed sensitively and effectively and, wherever possible, kept to a minimum.

4. PREPARING THE GROUND

4.1 Issues to be addressed

4.1.1 The issues previously identified that need to be addressed in order to prepare the ground for the changes that are required are:

- What is meant by confidential, consent, anonymisation, pseudonymisation and public interest?
- What are the options for change?
- When does the public interest justify disclosure without consent?
- Which activities should be supported, at least temporarily, by legislation?

4.2 Clarifying Definitions

4.2.1 There is much confusion over the concepts of consent, anonymisation and pseudonymisation in both legal and healthcare circles. Part of this arises from confusion over definitions. This is evidenced in the differing nomenclature used by different stakeholders. Consent has been referred to as *explicit*, *express*, *implicit*, *implied*, *necessary implied*, *specific* and *informed*. Often these terms are used interchangeably and without prior definition. The term *explicit consent* in particular causes confusion because it is used to describe both the manner in which a subject gives consent, and the quality of the information given to obtain that consent.

4.2.2 What is required is a set of definitions onto which stakeholders can map their own definitions and uses of terms. The following table provides a set of such definitions that may need to be refined through discussion and consultation.

Confidential	Information is confidential where it reasonable for an individual who provides it to believe that it will be held in confidence and it has been neither anonymised nor pseudonymised
Consent	Agreement, by someone with the capacity to make a valid decision, either express or implied, to an action based on knowledge of what the action involves, its likely consequences and the option of saying no
Express Consent	Consent which is expressed orally or in writing (except where patients cannot write or speak, when other forms of communication may be sufficient) (GMC)
Implied Consent	Consent which is inferred from a person's conduct in the light of facts and matters which they are aware of, or ought reasonably to be aware of, including the option of saying no
Anonymisation	Information from which individuals cannot be identified, or where the probability of an individual being identified is minimal (e.g. one in a million)
Pseudonymisation	A form of anonymisation where a key to the identity of the individuals concerned exists but is not available to organisations that wish to process the information

4.3 Potential Solutions

4.3.1 In the section on problem definition it was made clear that transparency is a given requirement, where the only flexibility relates to method. Beyond the requirement for transparency, there are only four robust options for satisfying the requirements of law, ethics and policy when dealing with patients who have the capacity to provide a valid form of consent. Each option represents an important component of a possible combined solution rather than a self-contained solution in its own right. Whilst, for example, gaining express consent for all uses of confidential information could theoretically be achieved, the cost would likely be prohibitive and the gains for patients minimal.

	Options
1.	Restructuring of NHS data flows to rely on anonymised or pseudonymised data
2.	Gain express consent from patients for data uses and support patient objections
3.	Gain implied consent from patients for data uses and support patient objections
4.	Introduce new statutory requirements

4.3.2 The public interest was considered as a potential fifth option, but the need to look at circumstances of individual cases and the difficulty of establishing a robust position on the public interest outside of Court relegates this to a marginal role. There may be scope for developing guidance that promotes consistency of interpretation across the health sector, but there is nothing to suggest that this will make the public interest a more, rather than a less, attractive option.

4.3.3 Some individuals lack the capacity to consent, whether through immaturity, illness or mental incapacity. In these circumstances, information may be used in the best interests of the individual concerned. Guidance on dealing with those who lack the capacity to consent is available from the Department of Health and the General Medical Council, and is beyond the scope of this strategy document.

4.3.4 In thinking about the appropriate balance between the four options outlined above, there are a number of principles that fall out of legal, ethical and policy requirements, namely that:

a) The issue of transparency **must** be effectively addressed. There are clearly links between the need to do this and the need to provide the information that necessarily underpins valid consent.

b) Unless it can be demonstrated that there is a strong case for using confidential information about patients, anonymised or pseudonymised information should be used.

- Anonymisation should be the first option considered. Only where it cannot provide an acceptable solution, should other options be considered;
- Pseudonymisation should be the second option considered. Technology and techniques are still evolving however, so complexity is introduced in that whilst peseudonymisation may not be an option now, it may be at some future date.

c) If, given the state of current technology and techniques, there are robust reasons why confidential information about identifiable patients must be used, consent should be the first option considered. This might be implied or expressed, but validity of consent will depend crucially on the information made available to patients and on the fact that they have a choice being clearly flagged.

d) Only where it is either impracticable to gain consent, or it can be demonstrated that it would not be the right thing to do, should the final option of introducing new statutory requirements be considered:

4.3.5 The following diagram illustrates how this hierarchy of options should determine the decision making process.

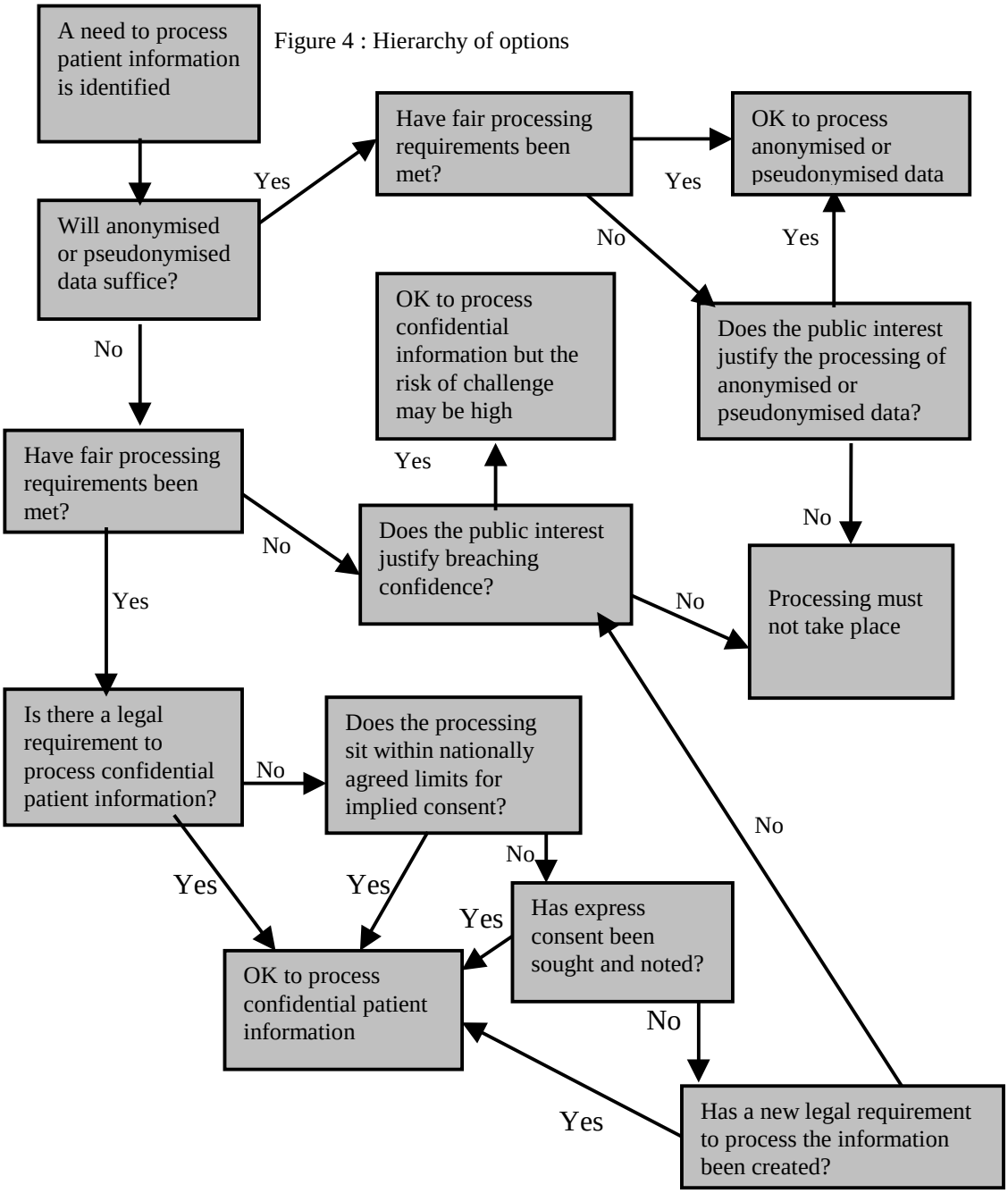


Figure 4 : Hierarchy of options

4.4 Determining which activities should be supported by legislation

4.4.1 Section 60 of the Health and Social Care Act 2001 provides scope for introducing requirements to process confidential patient information without patient consent. The process by which this power is used needs to be open and transparent and must be designed with the interests of patients demonstrably to the fore.

4.4.2 A range of constraints on the use of the power have been built in to the legislation, but these need to be developed and where appropriate, enhanced. An expert advisory group was assembled to design and document this process – patient

organisations, GMC, BMA, Academy of Medical Royal Colleges, research and public health communities etc, all were represented. Section 60 itself provides that the power may only be invoked:

- For a medical purpose;
- Either to improve the care and treatment of patients or in the public interest;
- Where the purpose is not to determine the care and treatment given to particular individuals; and
- Where there is no reasonably practicable alternative way of achieving the purpose.

4.4.3 Section 60 also makes it clear that it will be necessary to demonstrate that wherever the power is invoked to support a specific activity, the Data Protection Act 1998 and Human Rights Act 1998 are complied with.

4.4.4 Although these requirements will necessarily form the backbone of any process of determining whether the power should be invoked, these need to be fleshed out and added to. The following aspects will almost certainly need to be considered:

- An assessment of the value and quality of the activity, with appropriate standards being required;
- Reasoned arguments why patient consent cannot or should not be sought, e.g.
  - Why it is impracticable to gain consent
  - Why it is inappropriate to seek consent
  - Why seeking consent would undermine results to the extent that the value and quality standard referred to above cannot be met
- An assessment of any other potential or actual practicable alternative ways of conducting the activity without access to confidential information, including an assessment of barriers and costs

4.4.5 The possibility that the criteria used to establish need and justification for use of Section 60 might be progressively tightened also needs to be explored. Applications for Section 60 support should utilise an agreed template ensuring that all aspects of the testing process are effectively addressed.

4.4.6 Applications will need to be considered by an expert standing committee – the Patient information Advisory Group. This committee will advise the Secretary of State as to whether applications for Section 60 support should be taken before Parliament.

4.4.7 The Patient Information Advisory Group will also develop a much broader role in respect of advising on confidentiality and security issues.

Actions

- The NHS Executive Information Policy Unit will ensure that all key professional and patient groups are aware of and understand the Strategy on Protecting and Using Confidential Patient Information.
- A new Patient Information Advisory Group – a statutory standing committee - will be created to steer implementation of the strategy, agree standards and advise on the use of new legal powers to support certain uses of confidential patient information.
- The definitions and terms relevant to work on confidentiality will be agreed with all key parties.
- The possibility of developing guidance on public interest justification for disclosing confidential patient information will be explored

5. COMMUNICATIONS WITH THE PUBLIC

5.1 Communications Issues

5.1.1 The issues previously identified that need to be addressed by a communications strategy are:

- How can public understanding be enhanced?
- How can patients trust in the NHS be strengthened?
- How should information be communicated to patients?
- What information should be given in order to meet transparency and fair processing requirements?
- What information needs to be given to patients for consent to be valid?

5.1.2 Informing the public and patients about how the NHS uses patient identifiable information will require specialist communication planning including design of messages and selection of appropriate media. The communication campaign must bring about a major increase in transparency about how the NHS uses personal information. However, it must also strike a balance between informing patients and raising unnecessary alarm. Confidentiality is a potentially sensitive issue. Patients must be reassured that the NHS does protect their confidentiality so that they feel able to share sensitive information with the healthcare professionals who are caring for them.

5.1.3 An information campaign that aims to increase transparency may benefit from a theme that builds patient confidence in the NHS and its staff (*'you can tell your doctor anything'*). It may also appeal to public sense of altruism, informing them how their information helps improve the health of everybody (e.g. through helping research). Any information campaign, which will be expensive, should have a higher level aim in addition to just ensuring compliance with the law.

5.2 Local and National aspects

5.2.1 A large percentage of the UK population interact with the NHS in any one year and providing information to patients as they interact with the NHS will be one way of communicating with patients. For example, 78% of the population of England and Wales attended a GP during 1991/1992 (*Morbidity Survey From General Practice in England & Wales 1991/1992*). 16% of the UK population attended a GP in a two-week period (*General Household Survey 1996*). Significant percentages of the UK population also attend NHS hospitals in any one year, either as an in-patient (9%), or as an outpatient (15*%) (General Household Survey 1996*).

5.2.2 However, relying on communication through patient interaction with the NHS will not be sufficient to inform all NHS patients because the proportion of the population interacting with the NHS is not representative of the whole population, with the very young and the elderly heavily represented. Adults of working age are less likely to interact with their GP or NHS hospital in any one year, although they are still NHS data subjects and will need to be informed of NHS uses of their personal information.

5.2.3 It will therefore be necessary to undertake some form of national campaign, in addition to communication through the NHS at point of interaction. Such a campaign may include a national mail shot from the NHS and also media campaigns, perhaps including television and radio.

5.3 What needs to be communicated

5.3.1 In order to comply with the DPA 98 the information communicated to data subjects must include:

- 'Fair Processing Information'

5.3.2 If the ultimate aim is to gain implied consent from patients the information must also include:

- The concept that the patient has a choice over allowing disclosures
- How the patient may go about exercising that choice

5.3.3 Not all information needs to be provided in each form of communication. Indeed, to do so may overload the message and defeat the primary purpose of increasing transparency. An effective campaign will therefore consist of several levels of information provision, provided through different messages and media.

5.3.4 At its broadest level the NHS needs to communicate four or five concepts to patients. Further, more detailed information, can be provided through subsequent messages or upon request by the patient.

Broad level concepts:

i. Information provided to the NHS is kept highly confidential
ii. Confidential information is used for purposes in addition to those for direct care
iii. Such information is extremely valuable to improve everybody's healthcare and healthcare services
iv. Patients can find out more about NHS uses of their information
v. Patients can object to how the NHS uses their information

5.3.5 Subsequent messages provided to patients, either through mail shot, leaflets or upon request can include more detailed information with more comprehensive explanations of NHS uses of confidential information, the rights of patients and how preferences can be registered.

5.3.6 The concept of social responsibility also needs to be explored. Patients clearly have a right to treatment and to confidentiality, but should the relationship with patients be all one way? Whilst there is no intention to develop a specific social contract with patients, the tone and content of communications might raise awareness of the needs of society and the greater public good.

5.3.7 Once the content and design of the message (or more likely *messages*) has been decided, appropriate media must be selected to facilitate communication. Broad-level communication will best be achieved through visual and audio media such as posters, television and radio. More detailed information will best be achieved through letters, leaflets/booklets etc. Multi-media and web-based communications are increasingly accessible to many patients. A combination of media is most likely to be required to communicate such complex information. Enquiries and requests for further information may best be handled through NHS Direct and the National Electronic Library for Health, as well as through primary and secondary care.

Actions

- A communication strategy, with both national and local components, that will effectively inform patients of how confidential information is used and will satisfy the requirements of law, ethics and policy, will be developed in consultation with key interested parties.
- A Public relations strategy, running alongside the provision of information, will be developed to bolster public confidence in, and support for, the ways the NHS uses information.
- The phasing of information provision, and particularly information about rights, will reflect the developing capacity of the NHS to respond effectively to patient preferences.

6. CULTURAL CHANGE

6.1 Cultural Change Issues

6.1.1 The issues previously identified that need to be addressed through Cultural Change are:

- What guidance does the NHS need on required/best practice?
- What are the training and educational resources required and how should they be delivered?

6.2 Development of policy and guidance

6.2.1 NHS policies over the use and disclosure of confidential information should be developed under the direction of the Expert Advisory Committee and should, as far as is practicable, reflect the guidance of other bodies such as the General Medical Council and Medical Research Council.

6.2.2 An early requirement is the development of a code of practice for NHS staff who have access to confidential patient information. Guidance should also be developed on the role of the public interest in justifying disclosures of confidential patient information without consent.

6.3 Raising awareness

6.3.1 All NHS staff, regardless of their role, need to be reminded of the importance of confidentiality within the NHS. An internal campaign aimed at the whole NHS workforce should be run at regular periods. These should be timed to coincide or precede national campaigns aimed at the general public and patients, helping to create reinforcement.

6.3.2 The internal campaign will need proper project planning and execution. It is critical that staff are made aware of the public campaign, and that NHS organisations are able to handle the subsequent enquiries from the public, media, and other interested bodies. To some degree the public campaign itself will help to inform staff.

6.3.3 The NHS can do much to improve the confidentiality of the information that it holds. Such improvements can help reduce the occurrence of inadvertent or unauthorised disclosure and therefore reduce the NHS' risk of challenge.

6.4 Local Management of Confidentiality Issues

6.4.1 There is little consistency across the NHS in respect of the priority currently given to the issues addressed by this strategy. Management arrangements consequently vary enormously. Caldicott Guardians, Data Protection Officers, IM&T Security Managers and Records Managers are but a few of the roles and individuals that may be involved. Posts have been established in response to particular initiatives and there has been little joined up thinking either locally or nationally.

6.4.2 We now need to look beyond the requirements of individual information initiatives, important as they undoubtedly are, to establish a coherent, transparent and managed framework that provides staff with a clear and practicable model for working. Section 8 of this document explores this further.

6.5 Training and Education

6.5.1 Any campaign to inform the UK population about how their confidential information is used, and their rights to exert a degree of control over this, must be preceded by thorough training of staff likely to be asked questions and deal with concerns generated by the campaign.

6.5.2 NHS staff training will require proper planning and execution. It is important that the training is rapidly replicated through the NHS.

6.5.3 In particular, all NHS frontline administrative staff need to be trained to provide patients with appropriate leaflets, to understand the reasoning for providing patients with information and to be able to tell the patient what to do if they want to receive more information or wish to make their preferences known.

6.5.4 Target staff to be trained are:

i. Primary care reception staff (34,000 in England, *Statistics for General Medical Practitioners in England*)
ii. Secondary care reception staff (estimated as 50,000 in UK)

6.5.5 Beyond this basic training, within every NHS organisation there will need to be staff trained to deal specifically with patient concerns. These staff will need a more detailed understanding of NHS policy and procedures, especially how to effect patient objections to certain data uses.

6.5.6 Training of the large number of frontline clinical staff in the NHS could be a very expensive and time consuming exercise. All such staff already operate under a strict duty of confidentiality so the aim of training would be to make them aware, in general terms, of the ways the NHS uses patient information, to remind them to take every opportunity to make patients aware of the disclosures that are taking place and enable them to deal with patient objections.

6.5.7 The curricula of the medical and nursing schools also need to be modified to enhance future clinical staff awareness of confidentiality issues within the NHS. The education and training of other professions and staff groups will need similar modification.

Actions

- A code of practice, agreed by all key stakeholders, dealing with the handling of confidential patient information by NHS staff, will be developed.
- All staff in the NHS, including contractors, should be subject to strict confidentiality clauses in their contracts. The current situation will be reviewed and remedial action taken if necessary**.**
- Computer based learning and awareness raising packages, tailored to organastional type and circumstances will be urgently developed and provided to all NHS organisations.
- All NHS staff who have access to confidential patient information will receive appropriately tailored training in confidentiality issues.
- The curricula of the medical and nursing schools will be modified to enhance future clinical staff awareness of confidentiality issues within the NHS.

7. SECURING CONFIDENTIAL PATIENT INFORMATION

7.1 Securing Confidential Patient Information

7.1.1 The issues previously identified that need to be addressed by work to secure confidential patient information are:

- What are the barriers to use of anonymisation and pseudonymisation?
- What technical solutions can be developed to support greater reliance on anonymisation and pseudonymisation?
- Which data flows need to be covered by express consent?
- Which data flows should/can implied consent cover?
- How is consent/withdrawal of consent to be recorded and acted upon?

7.1.2 As well as increasing transparency and informing patients that they have a right to express preferences, it will be vital to develop systems that enable staff to respect any reasonable preferences expressed. This may cause problems for a range of activities where complete and high quality information is important. The NHS can minimise these problems by reconfiguring as many flows as possible to contain only anonymised or pseudonymised data. Many NHS data flows contain patient identifiable data purely to allow matching and linking of data over time and space, not because there is any need to identify any individual. Using encryption, enhanced by the use of the NHS number, many of these dataflows may become pseudonymised.

7.2 The NHS Number as the Unique Patient Identifier

7.2.1 The availability of a Unique Patient Identifier is essential for future confidentiality enhancing technology. The new NHS number is already in widespread use throughout the NHS and will fulfil the function of the Unique Patient Identifier. Use of the NHS number will allow other personal details such as name, address and date of birth to be removed from many information flows as these will no longer be necessary to link and match data over time and space. Removing all personal information other than the NHS number does not render a record de-identified, but it does prevent it from being readily identified – perhaps by accident.

7.2.2 However, the NHS number can also be used as the basis to pseudonymise information by encrypting it through a tightly held algorithm. The encrypted NHS number will still serve to uniquely identify information for matching over time and space but will not allow the identification of the individual due to the unavailability of the algorithm to decrypt the number.

7.2.3 It is unlikely that every NHS record or information flow will be able to contain the NHS number. It may sometimes not be possible to trace the NHS number for homeless people and foreign visitors will not have one. A mechanism will need to be developed to deal with information flows generated from such records.

7.2.4 The use of the NHS Number was promoted by the Caldicott Committee in 1997, but progress has not been as rapid as hoped. A project to investigate the barriers

to the adoption of the NHS Number is imperative, as this is an essential building block of a major confidentiality-enhancing measure. The NHS Number project should be given the status of the Y2K initiative, not only for the confidentiality issues, but also the data integrity and systems benefits that it would bring.

7.3 Using Local NHS Organisation Identifiers for Traceability

7.3.1 Records that have been pseudonymised through encryption of the NHS number can still be made traceable if required (for example to follow up on a research project) by including the organisation code of the institution generating an information flow and the local identifier code of the patient within that organisation.

7.4 Inference control

7.4.1 Centralised databases will need careful design to minimise the risk that individual patients can be identified through inference. Generally, the more information that is known about an individual, the greater the risk that someone will be able to identify that individual. The risks of inferability are well described, as are mechanisms and strategies to reduce the risk. Such strategies include vetting search requests, refusing searches that produce a small number of hits and removing outliers, such as extremes of age.

7.5 Implied/Express Consent

7.5.1 Certain data flows or uses will require express patient consent, either verbal or written. Gaining, recording and maintaining express consent for multiple NHS information flows is likely to be hugely expensive and time consuming, with little or no net benefit to the majority of patients. Express consent should be reserved for specific types of flow, especially where there is disclosure beyond the control of the NHS or where disclosures may adversely affect the patient.

7.5.2 Within the NHS, work is required to establish the limits of implied consent. The potential for maximising what it is reasonable to expect patients to be aware of and to comprehend needs to be considered within the communications component of this strategy as described in section 6.

7.5.3 There is a risk that information disclosed by the NHS to external agencies may subsequently be accessed by other government departments or the police. Whilst patients could be informed of this risk it may be preferable to prevent it occurring, e.g. by prohibiting confidential patient information disclosed by the NHS from being entered onto non-NHS computer systems. Work is needed to agree policy in this area.

7.5.4 Express consent for disclosure will best be recorded at the point of disclosure in the relevant record. Introducing a central registry for consent to certain disclosures will introduce another level of complexity into NHS operations and will require staff who need to disclose information having to consult the register which may be out of date. It would be better to develop a culture of staff asking the data subject for consent to disclose information whenever practicable during episodes of care and treatment.

7.6 Future primary and secondary care systems

7.6.1 Future computer systems must support patient objections to disclosure. This requires manufacturers to be responsive to NHS requirements through centrally mandated design requirements such as the RFA specifications for primary care systems.

7.6.2 Electronic records have the potential to undermine the commitment to informed consent unless appropriate access controls and the capacity to reflect and to respect patient preferences are built in from the outset. It is very unlikely that even a sizeable minority of patients will choose to opt-out of any of the uses that their information might support, especially if the NHS is open and transparent and presents a convincing case for such uses, e.g. by highlighting the importance of research.

7.6.3 Patients are most likely to be concerned about disclosures in their local environment, e.g. concerned that the next door neighbour who works in their GP practice as a receptionist has access to their medical records. Such concerns are best addressed at a local level, on a case by case basis. This is especially true for patient objections to disclosures within healthcare teams. These should be dealt with by sensitive discussion and negotiation to reach a satisfactory arrangement for the patient.

7.7 Supporting and recording patient objections

7.7.1 Initially this will best be managed within existing business processes. Future changes including electronic health records will require a fundamental appraisal of how to support patient objections at the design stage of such systems.

7.7.2 A simple sticker or wrapper for notes can enable paper records to support patient objections to disclosure, both within and outside the healthcare team. This can warn staff that only certain personnel, identified either individually or by role, may access the notes or that access, e.g. for research, may only take place with express consent or if information is anonymised by a member of the healthcare team. This can be effected by any NHS organisation, including primary care and secondary care.

7.7.3 Much information in both primary and secondary care is held on computer. It is from such systems that most disclosures outside the healthcare team are generated, e.g. to the local health authority through the Exeter System in the case of primary care, and to the NHS Wide Clearing Service in the case of secondary care. Most, if not all, existing systems do not provide a way of flagging records or blocking automated reports. Systems also need to include audit trails for accessing systems (current RFA requirements only detail audit trails for updates) as well as instigating effective monitoring procedures on such trails, otherwise they will be pointless.

7.7.4 Some patients may have very strong privacy concerns. These subjects could be those in public life or otherwise at risk of unauthorised intrusion into their records. Such patients may not trust the NHS with any of their information and consideration needs to be given to whether/how they may be provided with both high quality care and absolute privacy.

Actions

- Proposals for identifying and dismantling barriers to the adoption of the NHS Number will be developed and appropriate action taken.
- Options for increasing the presence of the NHS Number in key information flows will be developed and appropriate action taken.
- Proposals for pseudonymisation of patient information utilising an encrypted NHS Number will be agreed with relevant interests and implemented.
- Options for pseudonymising historical data sets will be considered.
- Guidance on the structure and functionality of electronic records in respect of the rights of patients will be developed and issued.
- Guidance on database design and inference control will be developed and issued.
- Requirements for audit, access controls and capacity to reflect patient preferences will be included within primary care RFA and clarified more generally for systems suppliers.
- Options for respecting absolute demands or requirements for privacy will be developed.

8. INFORMATION GOVERNANCE AND CALDICOTT

8.1 Issues to be addressed

8.1.1 The issue previously identified that needs to be addressed by work on information governance is:

- How should appropriate standards be set and enforced across the NHS and beyond?

8.2 Current situation

8.2.1 *Information for Health* and the *NHS Plan* are the most recent strategic documents to highlight the importance of information within the NHS, with specific reference to the challenging modernisation agenda. Like their predecessors however, they have not served to bring coherence to the complex, confusing and occasionally redundant or conflicting requirements that are placed upon NHS staff by a wide range of information initiatives. In the absence of an integrated approach progress on a range of linked initiatives will be constrained. There is potential not just for continued confusion but for a dangerous fragmentation of approach that, in the longer term, will result in frustration, delay, expense and risk. The 'do nothing' option is likely to result in:

- Excess work for staff resulting from failure to handle information safely and in coping with system deficiencies;
- Litigation and expense resulting from failure to handle information correctly;
- Inability to set up robust information flows between multiple systems e.g. pathology report for GP's, flows for cancer services;
- Difficulties in integrating departmental systems into a seamless whole and transferring information between systems;
- Inability to produce reliable indicators of organisational and individual performance.

8.3 A standards based approach

8.3.1 We now need to look beyond the requirements of individual information initiatives, important as they undoubtedly are, to establish a coherent and transparent framework that provides staff with a clear and practicable model for working. System and process management, records management, data quality, data protection and the controls needed to enable information sharing to be secure, confidential and responsive to patient rights and preferences, present issues that are inextricably linked. The term that we have coined for this new strategic framework is, perhaps inevitably, Information Governance.

8.3.2 Broadly speaking, the intention is to identify the essential components of all initiatives whose prime purpose is to set standards or impose requirements in respect of how the NHS works with patient information. Integrating these within a unified framework can then serve as the vehicle for meaningful performance assessment, year on year improvement and gradual cultural change. Information Governance aims to

improve outcomes by ensuring that information processing is subject to continuous improvement.

8.3.3 Integration of standards can enable superficially conflicting requirements to be understood as a positive tension, providing organisations' with an opportunity to question, monitor and assess, system, process and practice in accordance with known and clear standards and through clinical and managerial leadership.

8.4 Integrating standards

8.4.1 There are a number of ways that this can be addressed. An important step is to take a practical look at just what each requires in terms of action at a local level. However, this can only paint part of the picture. It will not, for example, reveal any of the interdependencies between initiatives, nor will it readily identify gaps or weaknesses in the various approaches. Information governance provides a means of addressing these issues by focussing on information processing standards.

8.4.2 Information processing has five broad aspects. These encompass how information is *Held, Obtained, Recorded, Used* and *Shared* (HORUS). Whenever the delivery of policy involves any form of information processing, then the information processing – HORUS – will, at least in part, determine the outcome.

8.4.3 These five broad aspects of processing can be fleshed out a little by reference to the standards of processing that apply in each case. We would suggest that information should be:

Held securely and confidentially
Obtained fairly and efficiently
Recorded accurately and reliably
Used effectively and ethically
Shared appropriately and lawfully

8.4.4 Thinking of information processing in terms of a set of standards helps to highlight interdependencies between initiatives because the dependencies between different standards are easier to grasp. How information is used or shared is dependent upon how it is obtained, recorded and held. If the information was obtained unfairly, it will not meet the requirements of Data Protection legislation. If it is inaccurate or unreliable, its use will be severely constrained and if patient identifiable information is not held securely and confidentially it will probably fall foul of Data Protection, Human Rights and common law.

8.5 The scope of information governance

8.5.1 Initiatives that impact on information processing standards tend to fall into two, more or less distinct, groups. The first group is concerned only with raising standards, with each initiative typically aimed at different aspects of information processing. This narrow focus can make it difficult to effectively prioritise between

the demands of different initiatives. Caldicott, Data Protection, IM&T Security, Data Accreditation, Controls Assurance etc are examples of this type of initiative. These are the initiatives that should be integrated within an information governance framework.

8.5.2 The second group is more concerned with outcomes and impacts on information processing standards only where this is needed to achieve the desired outcome, a means to an end rather than the end itself. This latter group tends to focus on the most obviously outcome oriented standards i.e. obtaining information efficiently, using it effectively and sharing it appropriately, and policy leads are often unaware of broader information processing standards. The pursuit of improvements to one or two processing standards without reference to the others can result in conflicting and confusing messages and may severely undermine outcomes. These initiatives need to take account of information governance standards to ensure that policy development is effectively informed.

8.5.3 The following table lists a number of initiatives that might form the information governance core. Each is mapped against the ten information processing standards associated with the HORUS model of information processing, to indicate which initiative attempts, in any meaningful way, to set standards relating to each area of processing

Aspects of Information Processing →	**Holding**		**Obtaining**		**Recording**		**Using**		**Sharing**	
Standards → / **Initiative**	**Sec**	**Conf**	**Fair**	**Effic**	**Acc**	**Rel**	**Effec**	**Ethic**	**Appr**	**Lawf**
Caldicott	✔	✔	✔					✔	✔	
Confidentiality		✔	✔					✔		✔
GMC guidance		✔	✔					✔	✔	✔
IM&T Security	✔								✔	
Data Protection	✔	✔	✔		✔					✔
Risk Management	✔	✔		✔		✔	✔		✔	
Data Quality Indicator					✔	✔				
Data Accreditation	✔			✔	✔	✔	✔			
PRIMIS	✔			✔	✔	✔	✔			
NHS Number prog.				✔	✔	✔			✔	
Controls Assurance	✔	✔			✔	✔				
Records Management					✔	✔				

8.6 Why Information Governance?

8.6.1 First, the integrated approach supported by Information Governance will facilitate greater awareness of all information processing standards by drawing them together and presenting them in a transparent way as a coherent package. This will be an extremely valuable resource for both the centre and the NHS, eliminating repetitive reporting and clarifying priorities.

8.6.2 Second, the standards can be broken down into levels of achievement, as

already done within Caldicott and Controls assurance, which establish a clear direction of travel for those needing to make improvements and makes appropriate targets clear to those developing new initiatives.

8.6.3 Third, these levels of achievement can be combined in various ways for performance assessment purposes, weighted appropriately, enabling comparative assessment of overall information governance performance, or more focussed assessment of performance against individual or multiple standards.

8.7 The Caldicott work programme

8.7.1 The Caldicott work programme underpins much of the strategic approach to protecting and using confidential patient information and also provides a model developing information governance. Although many NHS organisations have used the Caldicott programme to make considerable improvements to their current systems and working practices, progress has not been uniform across the service and in many areas competing priorities have resulted in Caldicott work being neglected. There is a need therefore to establish requirements for revitalising work on Caldicott and to ensure that the benefits of information governance are realised.

8.8 Caldicott and Partner Organisations

8.8.1 It is extremely important that, as far as is practicable, the standards that apply within the NHS should be consistent and equally, that similar standards apply in those organisations with whom confidential patient information is sometimes shared.

8.8.2 This needs to be addressed both nationally by agreement that partner organisations acknowledge the importance of agreeing a similar and locally through the introduction of information sharing protocols. Whilst these are already a Caldicott requirement, local organisations have found it extremely difficult to develop protocols and have argued convincingly that a central lead is required.

8.9 Reviewing Current uses of Confidential Patient Information

8.9.1 Caldicott work to map current uses of confidential patient information has led to a growing appreciation, both nationally and locally, of the complexity and volume of information usage. However, there has been little progress to date in reducing the use of confidential information. A process needs to be developed for determining whether each particular activity that currently utilises confidential information actually needs to do so, and if so whether this will change as technology for anonymising/pseudonymising information comes available. This will build upon related work conducted by the Caldicott Committee in 1997, but will also need to identify and plan ways of overcoming barriers and delivering change.

Actions

- Proposals for *Information Governance* will be developed and will include a coherent framework for initiatives that set standards for holding, obtaining, recording, using and sharing information.
- The work currently underway to implement the Caldicott recommendations will be reviewed and if necessary augmented or given greater priority.
- External agencies that need access to confidential NHS information, such as social services, will be encouraged to adopt Caldicott standards.
- Exemplar protocols governing all routine and other key information sharing with external agencies will be developed.
- National and local work, building on the work conducted by the Caldicott Committee in 1997, will identify uses of confidential information that should cease or should switch to anonymised or pseudonymised data.

9. NEXT STEPS

9.1 Required Action

9.1.1 A range of actions have been identified in this document under the headings of:

- Preparing the Ground
- Communications With The Public
- Cultural Change
- Securing the Confidentiality of Patient Information
- Information Governance and Caldicott

9.1.2 These actions are drawn together in the table on the following page.

9.2 Managing Change

9.2.1 Change of the scale envisaged will require careful and sensitive management. It will be essential that, as far as is practicable, all key stakeholders are agreed on both the actions required and the timetable for delivering outcomes. The formation of a Standing Advisory Body that is able to effectively represent the views of stakeholders and to provide advice to the Department on issues and details that will inevitably arise, is key to the development of this necessary consensus.

9.3 Benefits for Patients

9.3.1 The changes that are required will result in better informed patients who are aware of their rights and who are better able to engage with the NHS as partners in the provision of care and wider NHS work. Awareness of the importance of NHS work and of social responsibilities should also be enhanced.

9.3.2 Access to the level of information desired by individual patients must be supported and the process of exercising rights must be transparent and straightforward. However, there is a need to balance pressures so that empowerment does not evolve into a burden for patients and efforts to safeguard confidentiality do not inadvertently undermine care processes.

9.4 Benefits for those needing to process information about patients

9.4.1 Although there will inevitably be a degree of upheaval as changes are made to systems and working practices, the aim is to ensure that important activity is able to continue with increased effectiveness where possible and with a secure basis in law. The development of pseudonymisation solutions will enable researchers, managers and public health workers to have access to richer data than ever before whilst minimising the risk of any detriment to patients.

Preparing The Ground	Communications with the Public	Cultural Change	Securing Confidential Information	Information Governance & Caldicott
❑ The NHS Executive Information Policy Unit will ensure that all key patient and professional groups are aware of and understand the Strategy on Protecting and Using Confidential Patient Information. ❑ A new Standing Advisory Committee will be created to steer implementation of the strategy, agree standards and advise on the use of new legal powers to support certain uses of confidential patient information. ❑ The definitions and terms relevant to work on confidentiality will be agreed with all key parties. ❑ The possibility of developing guidance on public interest justification for disclosing confidential patient information will be explored	❑ A communication strategy, with both national and local components, that will effectively inform patients of how confidential information is used and will satisfy the requirements of law, ethics and policy, will be developed in consultation with key interested parties. ❑ A Public relations strategy, running alongside the provision of information, will be developed to bolster public confidence in, and support for, the ways the NHS uses information. ❑ The phasing of information provision, and particularly information about rights, will reflect the developing capacity of the NHS to respond effectively to patient preferences.	❑ A code of practice, agreed by all key stakeholders, dealing with the handling of confidential patient information by NHS staff, will be developed. ❑ All staff in the NHS, including contractors, should be subject to strict confidentiality clauses in their contracts. The current situation will be reviewed and remedial action taken if necessary. ❑ Computer based learning and awareness raising packages, tailored to organisational type and circumstances, will be urgently developed and provided to all NHS organisations. ❑ All NHS staff who have access to confidential patient information will receive appropriately tailored training in confidentiality issues.	❑ Proposals for identifying and dismantling barriers to the adoption of the NHS Number will be developed and appropriate action taken. ❑ Options for increasing the presence of the NHS Number in key information flows will be developed and appropriate action taken. ❑ Proposals for pseudonymisation of patient information utilising an encrypted NHS Number will be agreed with relevant interests and implemented. ❑ Options for pseudonymising historical data sets will be considered. ❑ Guidance on the structure and functionality of electronic records in respect of the rights of patients will be developed and issued. ❑ Guidance on database design and inference control will be developed and issued. ❑ Requirements for audit, access controls and capacity to reflect patient preferences will be included within primary care systems requirements and clarified for systems suppliers. ❑ Options for respecting absolute demands or requirements for privacy will be developed.	❑ Proposals for Information Governance will be developed and will include a coherent framework for initiatives that set standards for holding, obtaining, recording, using and sharing information. ❑ The work currently underway to implement the Caldicott recommendations will be reviewed and if necessary augmented or given greater priority. ❑ External agencies that need access to confidential NHS information, such as social services, will be encouraged to adopt Caldicott standards. ❑ Exemplar protocols governing all routine and other key information sharing with external agencies will be developed. ❑ National and local work, building on the work conducted by the Caldicott Committee in 1997, will identify uses of confidential information that should cease or should switch to anonymised or pseudonymised data.

APPENDIX A: NHS USES OF CONFIDENTIAL PATIENT INFORMATION

A.1 How the NHS uses confidential patient information

A.1.1 The NHS uses confidential patient information for many different purposes in addition to those directly concerned with the provision of healthcare to individual patients. This is not surprising, considering that the primary function of the NHS is to provide the UK population with high quality healthcare and that the information necessary to run this organisation will, largely, be generated from its primary business activity (treating patients). NHS uses of such information can be classified as:

- **Direct Clinical Care**
  - Informing clinical staff providing care *e.g. doctors and nurses accessing records*
  - Administration of care provision *e.g. medical secretaries typing letters*
  - Managing screening programmes *e.g. breast screening*
  - Informing non-NHS agencies providing care *e.g. Social Services, nursing homes*
  - Monitoring and improving the quality of clinical care provided and staff performance *e.g. clinical audit*
  - Education and training of clinical staff
  - Dealing with complaints and medico-legal issues

- **NHS Operational Management**
  - Registration of patients with organisations *e.g. registration of new GP patients*
  - Maintenance of NHS central register *e.g. updating births and deaths*
  - Paying for services and resource management *e.g. capitation and IOS payments to GPs, paying hospitals*
  - Financial audit of services *e.g. auditing GP IOS payments to counter fraud*

- **Public Health Activity & Medical Research**
  - Health of Populations - *e.g epidemiological studies into disease e.g. BSE*
    - *e.g. surveillance of communicable diseases e.g. meningitis*
  - Clinical Research *e.g. trials of new drugs*
  - Fulfilling statutory reporting duties *e.g. certain communicable diseases*

- **Planning**
  - Understanding national and regional patterns of health utilisation
  - Ensuring efficient and fair distribution of health care resources
  - Understanding how healthcare needs are changing
  - Projecting future costs and resource requirements
  - Planning new services *e.g. new hospitals*

A.1.2 The following page provides a diagram representing major NHS uses of confidential patient information. Although this provides a useful overview, it does not bring out the complexities associated with the provision of modern healthcare, nor does it illustrate the issues that can arise in specific areas of activity.

A.1.3 Information derived from clinical activity is used, in addition to providing care, to monitor and audit the quality of healthcare, monitor demand of services to plan for the future, to determine healthcare costs, to manage the provision of healthcare in a timely and efficient fashion and to conduct research. Research includes public health activities such as epidemiological enquiry into disease (e.g. cancer registries, New Variant CJD, Sellafield) and Health Services Research (for example to monitor and correct inequalities in healthcare provision).

A.2 Illustrating how information is used

A.2.1 This complexity and diversity, often driven by local needs and interests, contributes greatly to the lack of transparency that currently exists and makes analysis difficult. It is also a moving, not static, picture. Information is an enormously valuable resource and proposals for exploiting it, along with new technologies for manipulating it emerge with increasing rapidity.

A.2.2 It is neither possible therefore, nor particularly appropriate within the confines of a strategy document, to attempt to provide even a snapshot of how information is used by the loose association of many thousands of organisations that form the NHS. It is appropriate and possible however, to illustrate at least some of the complexities and issues through examples and case studies. The following pages provide two examples of how confidential information supports clinical activity and begin to suggest some of the limits to transparency at the present time. Three case studies that explore non-clinical uses of information and the issues that can arise follow these examples.

i. Examples of how confidential information supports clinical activity:

   Example 1: Primary Care
   Example 2: Secondary Care

ii. Case studies of how confidential information is used to support non-clinical activity:

   Case Study 1: Public health research, and in particular the work of cancer registries;
   Case Study 2: Disclosures to external agencies; and
   Case Study 3: Items of Service claims made by General Practitioners in order to receive payment for work done.

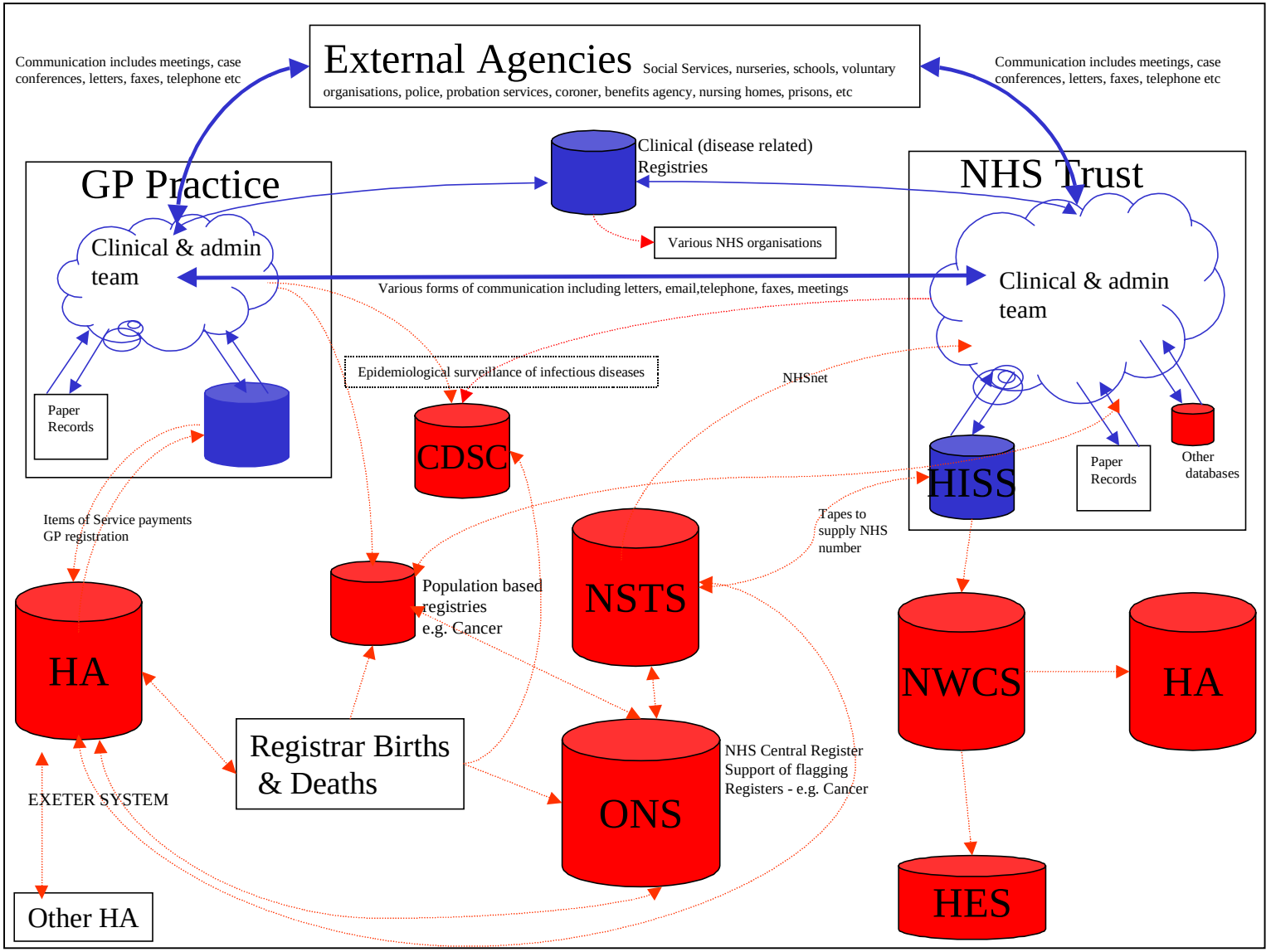


Figure 3 - NHS uses of Patient-Identifiable Information

A.3 Example 1: Primary Care

Example 1: Primary Care	*Patient aware of activity?*
Relatives of an elderly patient call out the GP during a visit to the patient because she appears to be unwell.	
GP makes out-of-hours call to patient and diagnoses a urinary tract infection. Gives patient a first dose of an antibiotic and gives the relatives a prescription to take to the pharmacy the following morning. Takes urine sample to be sent to local hospital.	Yes
Urine sample sent to hospital laboratory.	?
GP discusses patient with relatives who are concerned that she is not coping.	?
GP enters details of visit into practice computer system along with a code indicating an Item of Service claim for a night visit.	
Practice Manager reviews all IOS claims waiting to be sent. Then sends them electronically through the Racal network to the Health Authority.	No
Health Authority reviews IOS claim and makes payment	No
Relatives take prescription to pharmacist.	Yes
Pharmacist sends prescription to Prescription Pricing Authority. Information used to compile statistics and to reimburse pharmacist.	No
GP asks district nurse to visit patient to make sure that she is taking the antibiotics and is coping.	?
District nurse makes visit and takes a blood sample.	Yes
Blood sample and forms sent to local hospital.	?
District nurse agrees with relatives and GP that patient is not coping at home and appears moderately confused.	
Hospital sends back urine test results confirming urinary tract infection.	?
Hospital sends back blood test results which are normal.	?
GP sends referral to Consultant Psychogeriatrician to assess patient. Informs patient and relatives of this.	Yes
Psychogeriatrician makes domicillary visit to patient and makes diagnosis of early Alzheimers disease.	?
Psychogeriatrician writes to GP about diagnosis.	?
GP tells social worker about patient's condition and asks social worker to assess patient for help including meals-on-wheels, and possible re-housing in a residential home. The social worker creates a Care Plan for the patient and makes an application to a residential home with any relevant medical information.	Yes (if GP informs patient and relatives)
Health Authority audit team selects IOS claim for financial audit. Write to patient asking for permission to access the patient's notes to conduct audit.	Relatives read letter but do not respond.
Health Authority do not receive response to letter from patient therefore do not ask to access the patient's notes for the audit.	

A.4 Example 2: Secondary Care

Example 2: Secondary Care	*Patient aware of activity*
A 33 year old diabetic man is admitted to an Acute Trust through it's A&E, acutely unwell with a severe infection. He is stabilised and during admission is diagnosed with AIDS.	
Hospital laboratory that conducted the HIV diagnostic test sends an electronic report to the Communicable Disease Surveillance Centre about the HIV diagnosis. The report includes patient's name (soundex code), full address, postcode and date of birth. The report also includes risk factors such as sexual orientation.	No
The medical team that made the diagnosis refer the patient to the HIV Medicine Team who take over his care. They tell patient about this referral.	Yes
During the admission the patient, or information about the patient, is seen by the following people: Doctors from several teams and specialities (A&E, ITU, General Medicine, Infectious Diseases, HIV Medicine, Endocrinology, Ophthalmology) Nurses in each of A&E, ITU, general medical ward and the HIV Medicine ward. Specialist diabetes nurse Pharmacists Health care assistants Radiographers Radiologists Laboratory staff (microbiology, haematology, biochemistry) Ward clerks Secretarial staff Porters Dieticians Physiotherapists HIV Team Social Worker	?
The HIV Medicine Consultant fills in confidential voluntary reporting forms, one reporting the new diagnosis of HIV infection, the other reporting a new diagnosis of AIDS. Both report forms contain patient identifiable information. These are sent to the Communicable Disease Surveillance Centre (CDSC) of the Public Health Laboratory Service.	No
CDSC enters data into a confidential database to compile public health statistics on HIV infection rates and the incidence of AIDS.	No
The patient is seen during the admission by the Consultant Diabetologist who normally looks after his diabetes. The patient had been informed that the team were going to ask the diabetologist to advise on the patient's glycaemic control whilst he is unwell.	Yes

Consultant Diabetologist enters the patients diagnosis of HIV and AIDS on to the local diabetes registry which is used to coordinate and guide diabetes care between the hospital, the GP, diabetes nurses, podiatrists, and ophthalmologists (who will also be able to monitor for HIV related retinopathy).	?
The hospital microbiology laboratory grows a bacteria in culture from the patient's blood taken on admission. An electronic report is generated from the laboratory to the Communicable Disease Surveillance Centre which includes patient identifiers (soundex code of name, sex, date of birth, address and postcode).	No
Specialist Registrar from the medical team that admitted the patient wants to bring some medical students to examine the patient. The registrar asks the patient for permission.	Yes
Patient concerned that he will not be able to work after he is discharged and is concerned about the poor condition of the flat where he lives. He discusses this with a nurse on the ward who arranges for the hospital to contact Housing.	Yes
The patient is visited by the HIV Team Social Worker who helps the patient fill in claim forms for incapacity benefit and to apply for new housing. The social worker will be involved as part of discharge and ongoing community care.	Yes
Patient requires a medical report to be filled in by a doctor in order to claim certain benefits. The patient signs a consent form authorising the registrar to release the patient's [limited] medical details to the Benefits Agency and to a local Housing Association.	Yes
The patient is discharged from hospital. The Senior House Officer completes a 'TTO' form that goes to the GP. This includes the diagnosis and list of procedures that the patient underwent during the admission and the drugs on discharge.	?
Specialist Registrar dictates a full discharge summary letter on the patient. This is typed out by a medical secretary and sent to the GP.	?
Patient's notes and a carbon copy of the TTO form go to the clinical coding clerks who code the diagnoses and procedures according to ICD codes and enter these into the hospital HISS system.	?
HISS system generates Minimum Data Sets on each admission. Patient identifying details including NHS Number or name, address, date of birth, sex and post code are sent electronically to the NHS Wide Clearing Service (NWCS). From NWCS, information flows to the appropriate Health Authority and also to the Department of Health's Hospital Episodes Statistics Database maintained by IBM.	No

A.5 Case study 1: Public Health Research

A.5.1 Public health research includes epidemiology (the study of incidence, distribution and determinants of disease) and health services research which is concerned with maximising the health benefit from utilisation of health resources. Arguably some of the greatest advances in healthcare have come from public health research. A classic example is the discovery by John

Snow of the link between contaminated water and cholera in the 19th Century. The eradication of diseases such as smallpox and polio has only been possible due to the combination of effective vaccines and public health surveillance.

A.5.2 Modern day examples of such advances include linking smoking to lung cancer (Doll and Hill, 1950) and current research into the risks between mobile phones and brain tumours. Public health research often relies on gathering data about large numbers of patients over many years (longitudinal studies). For this reason, the research sometimes requires access to patient information without being able to seek consent.

A.5.3 This can be for many reasons, including huge sample sizes making the gathering of consent impracticable or the length of time since the research-relevant event. Sometimes the gathering of consent from patients to access information about events can be very intrusive. Sometimes the patient may have died and the seeking of consent may cause distress to relatives.

A.5.4 A good example of the benefit of public health research and the potential conflict between such research and the privacy is provided by UK Cancer Registries.

Cancer registries

The discovery in the early 1990s that the UK was falling behind many other developed and developing nations in its treatment of cancer was made by the cancer registries. All cancer diagnoses are registered which allows registries to determine disease incidence and survival rates and likely causative factors. Subsequent government-led initiatives to improve cancer care such as the National Cancer Plan will rely on the cancer registries' research to monitor progress. In particular, the registry data will help the NHS reach targets for saving the lives of cancer patients, improving the quality of cancer care, and decreasing inequalities between the survival of rich and poor and improving equity of access to treatment. The existence of such inequalities in cancer survival was a key finding of cancer research. Cancer registries will also enable the NHS to plan cancer services and build for the future.
Cancer registries currently rely on the registration of personal patient information from patients diagnosed with cancer.

A registration is made from several data sources when a cancer is diagnosed, for example, pathology departments, death certificates and hospital outpatient departments. The data includes patient name, sex and date of birth as well as information on tumour type and stage. Personal details are necessary to allow matching of patients to subsequent data flows into the registry, for example, from a death certificate on death of the cancer patient (vital to determine survival rates). Using a unique identifier, such as the NHS number, instead of personal details, is currently not possible due to incomplete penetration of the NHS number and non-inclusion of NHS numbers on death certificates. Further information such as full postcodes are necessary to monitor inequalities in healthcare due to social class through the matching with census data. Completeness of information is ensured by data entry clerks from the registries who go out to physically search medical

records.

Senior members of the cancer and public health community are opposed to changing the cancer registration process to include the requirement for patient consent or to anonymise (including pseudonymise) the data. Their arguments against seeking consent are:

1. Incompleteness of data collection causing skewed, biased data with poor generalisability

   a) Even a small proportion of patients declining disclosure would prevent the sample being representative. (e.g. Particular social groups may be more likely to withhold consent).
   b) Process of gaining consent likely to be incomplete and haphazard due to time and clinical constraints, itself becoming a source of bias.
   c) Cancer registries in countries requiring express consent have collapsed and have subsequently have been found to hold poor quality data (e.g. Germany).

2. Process of gaining and recording consent likely to be impracticable or unethical

   a) Doctor may be reluctant to add to the pressures on an already vulnerable group of patients.
   b) Consent that has been recorded must then be acted upon – difficult to ensure that multiple organisations involved in supplying data aware of an individual's consent (or lack of), especially over many years.

Their arguments against relying upon anonymised information are:

1. Anonymisation not practicable since studies are longitudinal and patients must be linkable.
2. Pseudonymisation possible but question the practicability of using NHS number as the means to ensure linkability (NHS number not universal).
3. Matching requires personal information, including name, date of birth and sex, to ensure accuracy.
4. Full post code necessary to monitor inequalities in healthcare due to social class through the matching of census data.

Those representing cancer registries see legislation, making reporting into cancer registries a statutory obligation, as the solution.

A.6 Case Study 2: Disclosures to External Agencies

A.6.1 The NHS does not work in isolation and the care that it provides must be co-ordinated

with other agencies such as social services, nursing homes and voluntary organisations. Government plans for 'joined up care' place an emphasis on the seamless integration of NHS activities with those of other bodies providing care and services to patients. Provision of such care will require increased sharing of confidential information between the NHS and these external organisations.

A.6.2 However, disclosure of confidential information outside the NHS carries risks. Firstly, staff of these external agencies may not be under the same professional or contractual duty of confidentiality as NHS staff, or an equivalent culture of confidentiality may not exist. Once information has been disclosed outside the NHS, the NHS is no longer able to control what happens to it.

A.6.3 There is also the risk that information disclosed to another government body may be misused against the patient. This is possible due to the existence of Strategic Gateways which facilitate the bulk transfer of data between organisations such as Local Authorities or Social Services and the police. These gateways exist principally to combat fraud. NHS data that ends up in the hands of employees of organisations such as Social Services or Local Authorities is at risk of automatic disclosure to the police or other government bodies unless steps are taken to prevent this.

A.6.4 A case study of South London and Maudsley (SLAM) NHS Trust is provided below. SLAM is the largest mental health trust in the UK and the case study demonstrates how NHS staff work in integrated teams with social workers.

South London and Maudsley NHS Trust

The South London and Maudsley NHS Trust is the largest mental health trust in the UK, employing over 4300 staff on 98 sites. It covers 7 Local Authorities and 2 Health Authorities. Its catchment area includes some of the poorest boroughs in the nation. The Trust receives numerous requests for disclosure of patient information from different organisations such as the Police, Social Services, Department of Social Security, solicitors, researchers and patients/clients themselves.

The Trust recognises the importance of maintaining the confidentiality of its patients in the face of numerous demands for access to information and has reorganised its IM&T and medical records department accordingly. The Trust appointed a Data Protection Officer who oversees all Subject Access requests and provides ongoing confidentiality training and briefings for all staff in the Trust. The Data Protection Officer has access to the Trust IM&T Manager, the Caldicott Guardian and a Trust in-house legal advisor.

The Trust has included Social Services records within its medical records, reflecting the move towards Integrated Community Mental Health Teams. This has been driven by the Mental Health Strategy and the National Service Framework for Mental Health. There is now just one record for each patient (client). This can be accessed by medical and nursing staff, community psychiatric nurses (CPNs), therapists and social workers. Information is shared with social workers according to locally agreed information sharing policies and protocols. The Trust records are currently mainly paper-based but it also has an Electronic Patient Record (EPR) system called CCS. This system will be accessed by the integrated mental health team, including social

workers and is currently in operation by integrated teams in Lewisham. While this means that named non-NHS staff access NHS computerised information, there is no actual electronic link between the EPR system and non-NHS computer systems, and therefore no potential for bulk transfer of data.

The CCS system is essentially a clinical register of patients. It currently only holds the details of patients who have been assessed and placed on an Enhanced Care Programme Approach (CPA), as opposed to Standard CPA patients who do not have to go on to a Trust CPA register. The CPA register aims to keep track of patients, ensuring that they are attending clinics, receiving appropriate care and not 'getting lost in the system'. In the future the Trust plans to move all patients, including those on Standard CPA, on to the CCS system from the Trust's three PAS systems. The CCS system has been designed to support restricted levels of access to information, down to individual data fields. The Trust has not yet decided how such confidentiality-enhancing facilities will be deployed. However, any record access automatically generates an email to that patient's Case Manager. The Trust is also working on protocols for allowing Primary and Acute Care to access the record.

The CCS system is available to psychiatric staff at four A&E departments in the Trust's area. This is particularly useful as the CPA record holds the 'crisis plan' for each patient. The CCS system holds the NHS number for each patient who has been an in-patient. In the future the system will become NSTS compliant and will hold the NHS number for all patients, including those who have not been in-patients. This process will be complicated by the common use of aliases and street names by many of the clients that may prevent all records being matched to the NHS number.

Central data flows from the Trust include individual in-patient submissions to NWCS (and hence the Health Authority) and batched activity reports for contractual purposes to both Health Authorities and PCGs. As the majority of mental health services are provided in the community, in-patient HES data (extracted from the NWCS database) provides only a partial picture of mental health activity. Unlike Acute Secondary Care, outpatient activities do not generate reports to NWCS, (though it is intended that out-patient data will be collected from 1 October 2001). The Trust is preparing to supply the Minimum Data Set (MDS) for Mental Health and is looking at ways of sharing its knowledge and EPR expertise with the rest of the NHS. It is a Beacon Site for development of the Mental Health EHR/EPR**.**

The Trust is aware of major issues over patient/client consent over disclosure of confidential information, especially as care is delivered through integrated care teams with routine information sharing between NHS clinical staff and social workers. The Trust does not yet have clear plans about how to support patient objections to disclosure and opt-out. It is trying to resolve these issues, although it is looking for central guidance on policy.

A.7 Case Study 3: Items of service claims

A.7.1 Information flows between the GP and the local Health Authority to enable GPs to claim items of service payments for clinical services, such as providing contraceptive services.

GPs must disclose confidential patient information in order to receive payment. Claims are also subjected to financial audit, with the Health Authority typically choosing around a hundred IOS claims and writing to the relevant patients for express consent to access their GP medical records.

A.7.2 These data flows have been a long-standing source of concern for professional groups and cover, amongst other things, minor surgery and the provision of contraceptive services. However, whilst the process could be anonymised with relative ease, the issues of probity and financial audit are difficult to resolve. Similar, though arguably less sensitive patient identifiable information also flows to the Health Authority from dentists and optometrists for relevant payment purposes. Pharmacists are required to send prescription forms which include patient details to the Prescription Pricing Authority (PPA) and the PPA may release this information to other bodies for research purposes etc.