DEPARTMENT OF HEALTH

The Caldicott Committee

# Report on the Review of Patient-Identifiable Information

December 1997

DEPARTMENT OF HEALTH

The Caldicott Committee

# Report on the Review of Patient-Identifiable Information

December 1997

# Foreword

This Review was commissioned by the Chief Medical Officer of England owing to increasing concern about the ways in which patient information is used in the NHS in England and Wales and the need to ensure that confidentiality is not undermined.

Such concern was largely due to the development of information technology in the service, and its capacity to disseminate information about patients rapidly and extensively.

In 1996 guidance on *"The Protection and Use of Patient Information"* was promulgated. We need to promote awareness of it at all levels in the NHS.

It is a truism that confidentiality is an essential component of the clinical consultation in the provision of health care. The clinical professions have stringent requirements with regard to confidentiality in their codes of ethics.

However, information about patients, not directly associated with their clinical care, underpins the efficient operation of the NHS, and its importance cannot be overstated. Recent outbreaks of Escherichia infection and geographical variation in the prevalence of particular forms of cancer both illustrate how information about disease, suffered by individual patients in particular locations, provides knowledge which contributes not only to their effective treatment, but also potentially to the prevention of further cases occurring.

It is clearly important that confidentiality does not impede the provision of prompt and effective patient care. But at times there is a tension between the needs of the service for patient information and the expectation of patients that information about them will be kept confidential. It is not uncommon for the NHS to have to balance conflicting needs of this kind; this can be done by adhering to explicit and transparent principles of good practice which we have outlined.

Increasing adherence to the principles will reassure patients and those treating them that confidentiality is safeguarded. Such progress should be monitored and appropriately identified, and individuals held to account wherever patient-identifiable data is present in the Service. We believe that the principles outlined here should also be applied to information identifiable to individual patients concerned with their clinical care, and medical research. It is clear that patients expect nothing less.

I should like to thank the members of my Committee, its Working Groups and the secretariat for their contributions to this Review - not easy deliberations but pursued with much commitment and good humour.

Dame Fiona Caldicott

# Executive Summary

i) In the light of the requirements in *The Protection and Use of Patient Information* and taking into account work undertaken by a joint Department of Health (DH) and British Medical Association (BMA) Working Group which has been considering NHS Information Management and Technology (IM&T) security and confidentiality, the Chief Medical Officer established the Caldicott Committee to review all patient-identifiable information which passes from National Health Service (NHS) organisations in England to other NHS or non-NHS bodies for purposes other than direct care, medical research, or where there is a statutory requirement for information.

ii) The purpose was to ensure that patient-identifiable information is only transferred for justified purposes and that only the minimum necessary information is transferred in each case. Where appropriate, the Committee was asked to advise whether action to minimise risks of breach of confidentiality would be desirable.

iii) The work of the Committee was carried out in an open and consultative manner. Written submissions were sought from many organisations to identify existing concerns, and members of the Committee have met with representatives of a number of key bodies. Working groups containing a wide range of health professionals and managers were established to consider related groups of information flows and to take soundings on emerging findings.

iv) Some 86 flows of patient-identifiable information were mapped relating to a wide range of planning, operational or monitoring purposes. Some of these flows were exemplars, representing locally diverse information flows with broadly similar characteristics and purposes.

v) The Committee was greatly encouraged to discover that, within the context of current policy, all of the flows identified were for justifiable purposes. However, a number of the flows currently use more patient-identifiable information than is required to satisfy their purposes. Also many of the patient-identifiers currently used (eg name and address) could be omitted if a reliable, but suitably controlled, coded identifier could be used to support identification.

vi) It was recognised that some flows of information were likely to be missed and that flows commence, evolve or are discontinued with such frequency that specific recommendations could soon date. Although specific recommendations have been included where appropriate, in general the recommendations reflect this evolving picture by developing a direction of travel, outlining good practice principles and calling for regular reviews of activity within a clear framework of responsibility.

## vii) Summary of Recommendations

**Recommendation 1:** Every dataflow, current or proposed, should be tested against basic principles of good practice. Continuing flows should be re-tested regularly.

**Recommendation 2**: A programme of work should be established to reinforce awareness of confidentiality and information security requirements amongst all staff within the NHS.

**Recommendation 3**: A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.

**Recommendation 4:** Clear guidance should be provided for those individuals/bodies responsible for approving uses of patient-identifiable information.

**Recommendation 5:** Protocols should be developed to protect the exchange of patient-identifiable information between NHS and non-NHS bodies.

**Recommendation 6**: The identity of those responsible for monitoring the sharing and transfer of information within agreed local protocols should be clearly communicated.

**Recommendation 7:** An accreditation system which recognises those organisations following good practice with respect to confidentiality should be considered.

**Recommendation 8:** The NHS number should replace other identifiers wherever practicable, taking account of the consequences of errors and particular requirements for other specific identifiers.

**Recommendation 9**: Strict protocols should define who is authorised to gain access to patient identity where the NHS number or other coded identifier is used.

**Recommendation 10:** Where particularly sensitive information is transferred, privacy enhancing technologies (e.g. encrypting identifiers or "patient identifying information") must be explored.

**Recommendation 11:** Those involved in developing health information systems should ensure that best practice principles are incorporated during the design stage.

**Recommendation 12:** Where practicable, the internal structure and administration of databases holding patient-identifiable information should reflect the principles developed in this report.

**Recommendation 13:** The NHS number should replace the patient's name on Items of Service Claims made by General Practitioners as soon as practically possible.

**Recommendation 14**: The design of new systems for the transfer of prescription data should incorporate the principles developed in this report.

**Recommendation 15:** Future negotiations on pay and conditions for General Practitioners should, where possible, avoid systems of payment which require patient-identifying details to be transmitted.

**Recommendation 16**: Consideration should be given to procedures for General Practice claims and payments which do not require patient-identifying information to be transferred, which can then be piloted.

# Contents

# 1. Introduction

## 1.1 The Caldicott Committee

1.1.1 In March 1996, guidance on *The Protection and Use of Patient Information* was published by the Department of Health. This guidance required that when the use of patient information was justified, only the minimum necessary information should be used and it should be anonymised wherever possible. In the light of that requirement, and of the deliberations of a joint DH/BMA working group looking at NHS Information Management and Technology (IM&T) security and confidentiality, the Chief Medical Officer established the Caldicott Committee to review the transfer of all patient-identifiable information from NHS organisations to other NHS or non-NHS bodies for purposes other than direct care, medical research or where there is a statutory requirement, to ensure that current practice complies with the Departmental guidance.

1.1.2 It is important that this Report, and its conclusions and recommendations, are viewed against this remit. It is not a comprehensive inquiry into the whole area of confidentiality of patient information. We were asked to examine particular flows of patient information, albeit defined in a broad manner, and to make recommendations following their review and this is what we have done.

1.1.3 Our precise terms of reference were:-

**Figure 1 - Caldicott Committee Terms of Reference**

"To review all patient-identifiable information which passes from NHS organisations to other NHS or non-NHS bodies for purposes other than direct care, medical research or where there is a statutory requirement for information.

The Committee will consider each flow of patient-identifiable information and will advise the NHS Executive:-

- Whether patient-identification is justified by the purpose;
- whether action to minimise risks of breach of confidentiality is desirable, e.g. reduction, elimination, or separate storage of items of information".

***Scope of the remit***

1.1.4 As the work progressed, and the concerns of Committee members and those they consulted became apparent, we thought it necessary to comment on wider issues and to recommend other aspects for further work or study. The core of the Committee's work, however, has been to consider whether the current transfer of patient- identifiable information is justified for the purposes which it is intended to meet, and whether changes should be made or additional protection is needed.

1.1.5 In tackling this work we have been conscious that we were unlikely to capture every information flow that existed and fell within our remit. We acknowledge that fact explicitly in a number of areas, where exemplar flows have been used to demonstrate the nature of a wide number of similar flows that are known to exist. In particular, it is important to note that the flows which we have examined have all related to the NHS in England. It is likely that other flows exist which we should have examined but which have not been identified here.

1.1.6 In recognition of this we provide a set of general principles which can be applied to information flows that have not been identified during our work, and to any new flows which may arise in the future.

1.1.7 We have not attempted to review the use of aggregated information, though we recognise that it may be possible in certain circumstances to infer the identity of an individual, eg where rare conditions are involved. During the course of our work, particular concerns relating to the transfers of commercially valuable aggregated prescribing information have been noted. We note that the Department of Health is considering the need for additional guidance on the use of aggregated information *(The Protection and Use of Patient Information, para 4.6)* and hope that our recommendations will provide a supportive framework.

1.1.8 An important issue which we have not addressed, but which was clearly of great concern to many of those who were consulted during the course of our work, is that of patient consent to the routine but important use of information about them by the NHS. In particular we note that the General Medical Council (GMC) is considering this issue in preparation for revising its guidance to doctors on confidentiality. We hope that the Department of Health will be encouraged to work with the GMC and other organisations to address concerns whilst ensuring that the NHS can continue to respond effectively to the needs of the population.

1.1.9 The EC Data Protection Directive, which must be implemented in this country by October 1998, is a further important concern for the NHS and the Department of Health. The Department of Health is considering what the likely impact of the Directive will be. It intends to revise its guidance once legislation, shortly to be introduced, has been enacted. The impact of this Directive was clearly outside our remit, though some reference to its content is included in the Appendices (Appendix 2 and Appendix 5).

## 1.2 What is patient - identifiable information?

1.2.1 One of our first tasks was to attempt to determine what we meant by patient-identifiable information, and the Working Groups which were established to support the Committee collectively identified a number of items by which a person's identity may be established. These are listed in Appendix 7.

1.2.2 In almost all of the flows reviewed there are items of information present which would enable a person's identity to be established by one means or another.

1.2.3 We felt that no single item - with perhaps the exception of the new NHS Number in certain circumstances - can be relied upon to identify an individual with certainty, and even where this exception applies, corroborating information is likely to be sought. The degree to which other items might identify an individual will depend on the context - for example an unusual surname may be a stronger pointer to a specific individual than a more common surname.

1.2.4 However, it was clear to us that there are many items of information which could be used to identify individual patients. Although particular items may not in themselves uniquely identify an individual patient, taken together they may permit identity to be inferred. Different combinations of items may require different degrees of effort (and use of other information sources) to allow individuals to be identified.

1.2.5 We concluded that **all** items of information which related to an attribute of an individual should to be treated as potentially capable of identifying patients to a greater or lesser extent, and appropriately protected to safeguard confidentiality. Note should be taken of the degree of difficulty involved in actually identifying a specific individual, and this should be balanced against the purpose and usefulness of the specific items of information.

1.2.6 Our conclusion was that we were required to take a broad view of what is patient- identifiable information, and not limit our work to only those items which seek to clearly identify an individual, but take into account other identifying characteristics.

# 2. Background and Context

## 2.1 The Information Explosion

2.1.1 The need to safeguard the confidentiality of the information that patients give to clinicians about their condition, their personal circumstances, their family and their way of life, is fundamental to the relationship between patients and health care professionals.

2.1.2 In the past, unauthorised and inappropriate access to such information was inhibited as it was often held in a variety of locations and in paper format. Whilst this had the by-product of providing a measure of protection of confidentiality, it has not supported effective record keeping and has acted as a barrier to the appropriate sharing of patient information between health professionals.

2.1.3 In the last few years the information explosion has significantly changed the ways in which the National Health Service handles and exchanges information about patients; both between health service organisations and with other agencies involved in providing, managing or researching into health.

2.1.4 The introduction of new technologies is aimed at improving the effectiveness and efficiency with which care can be given to patients, providing support to health care workers and making the most effective use of health information to plan and monitor the services provided. However, the opportunity brings with it new risks, and concerns over the confidentiality of patient information have been raised in the last few years as a result of the increasing use of information technology within the health service, and the possibility that unauthorised or inappropriate access to personal information may become more likely as a result.

### *Developments in the Health Service*

2.1.5 It has always been important to exchange and retain patient-identifiable information, not just for direct patient care but also for the efficient and effective operation of the NHS, for planning, operational and monitoring purposes. (See paragraph 3.5). However, changes in the way the Health Service operates have created specific and extensive demands for information. In particular three major policy developments have contributed:

- Seamless Care - Seamless care for patients, particularly seamless community based care, requires detailed liaison between the NHS, Social Services and other agencies. Referral to hospital by the GP, hospital treatment followed by early discharge, and support in the community, all require the exchange of essential information about the patient as efficiently as possible if effective care is to be delivered.

- Evidence Based Medicine - Improving the practice of evidence based medicine requires clinical audit and evaluation of treatment and outcomes for patients. Information technology and appropriately designed clinical information systems permit the collection and analysis of considerable amounts of information about patients in computerised databases so that patients' conditions and progress can be checked and evaluated, as well as supporting the further development of an evidence base.

- Organisational Change - The organisation and management of the NHS in recent years has been based on the concept of an internal market. Managing and monitoring contracts has required the transfer of information about patients treated to enable the system to operate. Whatever the exact form of the new Government's measures to replace the internal market, there will still be a need to provide information about activity, for example for planning and accountability purposes.

### 2.2 Principles of Confidentiality and Security

2.2.1 Maintaining the confidentiality of patient information is fundamental to the relationship between patients and healthcare professionals and is an integral part of the ethics of the healthcare professions. Furthermore, both common law and statute impose relevant obligations of confidentiality or require the protection of information (see Appendix 2).

2.2.2 In addition to the Department of Health guidance, with which all NHS bodies must comply, professional and regulatory bodies have also produced guidance. Appendix 5 contains examples drawn from relevant legislation and published guidance, including guidance provided by the Department of Health, the GMC, and the ICC, plus principles drawn from the Data Protection Act 1984 (DAP) and the EC Directive on Data Protection (ECAD).

# 3. Methodology and Findings

## 3.1. Methodology

3.1.1 The starting point for the Committee was a scoping study commissioned by the NHS Executive which identified four areas where flows of information would need to be examined.

3.1.2 To examine and review the information flows in detail, the Committee established four Working Groups - one for each area - representative of a wide range of professions and other organisations. Membership of the Working Groups is shown at Appendix 1. Their task was to undertake a detailed review of the information flows, to identify further flows which had not been located in the initial scoping study, and to make recommendations to the main Committee.

3.1.3 The Working Groups were:

- **Primary Care** - chaired by Dr Philip Leech of the NHS Executive Primary Care Division, which examined information flows supporting primary care.

- **Operational Management -** chaired by Professor Alastair Bellingham, immediate past President of the Royal College of Pathologists and Chairman of the NHS-Wide Clearing Service Security and Confidentiality Advisory Group, which examined information flows supporting the day-to-day running of the NHS, particularly in the secondary care sector, with emphasis on contracting and the collection of certain performance monitoring and management data.

- **Health of Populations -** chaired by Dr Jeremy Metters, Deputy Chief Medical Officer of the Department of Health, which examined those information flows which support the provision of population-based services and statistics; and

- **Multi-Agency Working** - chaired by Mr Sandy Taylor, Chief Executive of the Dorset Community NHS Trust, which examined the exchange of information with non-NHS organisations.

3.1.4 The Working Groups approached their task by:-

- identifying the information flows which they would address;

- collecting the basic information about each flow such as the purpose, source and recipient of the flow, the items of information which are actually exchanged and any existing security measures which protect the data;

- establishing a framework of questions against which to test the inclusion of items in the information flows;
- consulting with appropriate colleagues to gather input from as wide a range of views as practical on the issues and the information flow mapping;
- considering the justification of each information flow in the light of their findings.

3.1.5 A number of organisations were invited to submit comments on the general aspects of the work, and have done so. These are listed at Appendix 9.

3.1.6 Figure 2 lists the criteria which were used to review the information flows.

**Figure 2 - Review Criteria**

- What are the purposes of the information flow?
- Are these purposes justifiable?
- At which point(s) does the information need to identify the patient to meet its purpose(s)?
- Are individual identifying details such as patient names, addresses, postcodes, dates of birth, sex and NHS number needed for the information flow to meet its purpose(s)?
- What are the implications if any particular information items or group of information items are removed?
- Is the information retained in a patient-identifiable form after its purpose(s) have been met? If so, why?
- What practical alternatives can be suggested to replace existing practice?
- Are there any particular concerns about confidentiality /security?

## 3.2 Mapping the Information Flows

3.2.1 Appendix 3 to this Report sets out all the flows in summary form. Appendix 8 shows a sample of a fully detailed information flow mapping. A copy of all the detailed mapping can be obtained from: Richard Walker, Quality & Consumers Branch, NHS Executive, Quarry House, Leeds LS2 7UE.

3.2.2 The data flows are described in terms of:-

- FLOW TITLE A description of the information flow
- PURPOSE The reasons why the information is transferred.
- FROM: TO Showing the parties or organisations between whom the information flows.
- SECURITY A description of measures taken to protect the information from unauthorised disclosure.
- COMMENTS Other relevant information about the flow
- FLOW ASSESSMENT The Committee's opinion as to the justification of the flow or otherwise

3.2.3 We are conscious that there will be some information flows which have not been mapped and examined in the course of our work. Indeed, new flows are constantly being established, and existing flows discontinued. **Nevertheless, we believe that the majority of flows within our remit have been mapped.**

### 3.3 Exemplar Flows

3.3.1 In a number of instances we found information flows which existed in many different circumstances, but with broadly similar purposes and characteristics. Disease Management Registers are a good example, as there are many in existence, their purposes are similar, the information which they capture, hold and analyse has common characteristics (albeit that the clinical details vary), and the parties between whom information is transferred are usually clinicians or professional carers.

3.3.2 In these cases we did not attempt to locate and describe every flow which could be found. Instead we identified one information flow as an exemplar flow, typical of a large number of those in existence.

### 3.4 Definitions

3.4.1 The Committee discussed in detail the precise meaning of a number of the phrases used in the Terms of Reference, including the meanings of direct care, medical research and statutory requirement.

3.4.2 We concluded that whenever there was doubt about the inclusion of a particular information flow or issue, we should take an inclusive rather than an exclusive view of the Terms of Reference. Thus, Appendix 3 to this report includes a number of information flows which might be omitted if the Terms of Reference were more strictly applied.

### 3.5 Purposes of the information flows

3.5.1 We believe that, within the parameters of our terms of reference, the transfer of patient-identifiable information can be classified as being for either planning, operational or monitoring purposes. This analysis is not exhaustive and there will be other factors which require the presence of patient-identifiable items in some of the flows e.g. to detect duplication.

3.5.2 Planning purposes typically include:

- **Public Health and epidemiological investigation,** research or survey work which may require linking episodes of care. The ability to establish such links is dependent on the existence in the data set of some identifying features, usually related to individuals in a population;

- **collection of statistical information** where, although the output is aggregated, information is collected and possibly held in patient-identifiable form either to provide flexibility of analysis or to enable linkage between different events occurring to the same person.

- **adverse drug reaction reporting** and **planning for new, dangerous or unusual diseases, like HIV infection or CJD**, relies on having patient-identifiable data items so that duplicate records may be eliminated. This may require holding multiple identifiers or apparently redundant data items to ensure accurate elimination of duplicates;

- **planning certain services** on a small area or locality basis may require the analysis of activity information down to postcode level, and particularly need more than just the first part of postcodes.

3.5.3 Operational purposes include:

- **registration services** to note that an organisation or individual is responsible for the care of that patient;

- **exchange of NHS contract information** - to support NHS contracts for the provision of services, and ensure that the service is paid for. For example contract minimum data sets currently include name and address so that Health Authorities and Fundholding Practices can be satisfied that the patient's treatment is their responsibility;

- **determining patients' rights** to, for instance, free prescriptions or free dental services which are dependent on ability to prove identity or eligibility;

- **management of disease registers** which require the ability to link the appropriate patient on the register to that person's medical record.

3.5.4 Monitoring purposes include:

- the need to support **probity** and ensure that claims for payment by service providers can be authenticated or audited. General medical practitioner claims for items of service are, in most cases, linked to the patient's identity for authentication against the patients registered with that practice;

- **public accountability** - although information is not required at an individual level, the need to be able to account to Parliament for the use of public resources requires the collection and analysis of statistical data which is based on aggregation of individual details, and sometimes requires aggregating by certain personal characteristics, e.g. age, sex, location, etc.

- **local performance management** - as for public accountability, monitoring performance against local plans may require the use of statistical data based on aggregations of person-based datasets.

3.5.5 The need for existing service requirements (e.g. contracting) is rarely the subject of unanimous agreement, but consideration of alternative ways of meeting service requirements is clearly outside the scope of this work. Therefore, when evaluating the purposes for which patient-identifiable information is transferred, our approach was to establish whether the continued use of patient-identifiable information is justifiable in the context of *existing* service requirements.

### 3.6 Justification of information flows

3.6.1 We agreed to consider flows and form a view as to the justification of each information flow in terms of one of the following categories:

- Full justification - where we thought that the existing transfer of patient-identifiable information was fully justified, e.g. screening programmes and NHS central register maintenance - 55 examples;

- Unjustified - where we thought that there were no grounds to support the exchange of any patient-identifiable information - no examples were found;

- Partially justifiable - where there was justification for the exchange of patient-identifiable information, but we thought that less patient-identifiable information should be transferred or that there is a need to make patients less easily identifiable e.g. General Practice items of service claims, contracting & commissioning and AIDS/HIV flows - 31 examples.

3.6.2 We were conscious that our review could only capture flows of patient-identifiable information at a particular point in time and that the purposes and their justification were likely to change over time in response to service requirements and government policies.

### 3.7 Access to information

3.7.1 Having considered the purposes to which patient-identifiable information may justifiably be put, and formed a view as to whether current practice is justified, we then considered issues relating to the access to such information.

3.7.2 A wide range of staff, some involved in direct care, others not, may have access to the information for the purposes listed above. For example, a referral letter from a general practitioner to a consultant has, as its primary purpose, the direct care of the patient. However the letter, or information extracted from it, may be handled by non-clinical staff in support of legitimate processes concerned with the operation of the NHS. Whilst this is clearly not a new development in the NHS, it is increasingly of concern as the use of information technology increases.

3.7.3 Information flows will be anonymised to a varying degree. In some cases, as with the Hospital Episode Statistics (HES) data, access to those items which might permit identification is strictly controlled. In other cases, such as the collection of data from general practice, a unique identifying number known only to the practice is allocated to the data set and only partial post codes are included.

3.7.4 We thought that in some cases, while some staff might require access to all the patient-identifiable data items, others did not need such access or only needed access to part of the information to fulfil their functions.

3.7.5 We were also concerned that once information is provided to a non-NHS organisation, even for a legitimate purpose, it becomes more difficult to police its subsequent use. This is an area in which we believe that very clear protocols are needed to ensure that the recipients of such information work in accordance with the standards expected of staff within the NHS.

### 3.8 Options for reducing the amount of identifiable information

3.8.1 We thought it important to consider the methods by which the risk of inappropriate disclosure could be reduced.

3.8.2 The first question we asked was whether it is practical to remove all identifiable items from flows and still meet the specific purpose(s). If the function can be carried out without the need for any such personal information, then it should be.

3.8.3 Reducing the number of identifiable items might also be possible in some flows. Whilst not guaranteeing anonymity, such action could help to reduce the risk of deliberate or inadvertent disclosure.

3.8.4 Where there is a clearly justifiable need for some form of personal identifying information to form part of a flow, then every effort should be made to protect the confidentiality of that information within systems and whilst in transfer.

3.8.5 There are a number of techniques which can be used in computer-based information systems to protect the confidentiality of data - these techniques are referred to as privacy enhancing technologies by the Data Protection Registrar[1] and others.[2]

3.8.6 One way of reducing the potential for risk of access is through the use of a coded reference identifier (for example the new NHS Number or a random number generated by a clinical system) as the main patient identifier, and reducing, if not altogether removing, other identifying items which are used within information flows. However, although the use of a coded identifier may enable other patient-identifiable items such as name and address to be removed, it is essential to prevent any unauthorised access to systems which allow the related patient information to be accessed using that coded reference identifier.

3.8.7 Encrypting both identifying and non-identifiable information in transfer and storage may be a means of ensuring greater safeguarding of confidentiality and help to reduce the risk of disclosure. Whilst no system of encryption might be regarded as totally secure, the motivation to break the system or the resource needed to crack the code would have to be substantial in order to achieve identification and encryption in an appropriate form may be considered secure for all practical purposes.

3.8.8 Holding identifying information separately from other information about the patient might also be possible in some cases and particularly in those circumstances where the information may serve more than one purpose, or where some individuals do not need to use all of the patient information.

3.8.9 There are many other systems techniques which can be used to control access to information, to audit such access, and to manage the exchange of information in a secure manner. Many of these are detailed in the NHS IM&T Security Handbook and a short summary of some of the relevant technical issues is contained within Appendix 6.

## 3.9 NHS Number

3.9.1 The NHS Number is a unique personal identifier for use within the NHS for healthcare purposes. All patients have had a number in the past, but a new number has recently been issued to overcome the problem caused by having different formats in use which were not very machine-friendly. The new NHS Number has already been widely implemented within primary care and is now in the process of being increasingly used within the secondary care sector.

[1] Data privacy in medicine : a perspective offered by the Data Protection Registrar, British Journal of Healthcare Computing 1997 Vol 14 Number 2 pp 20:22

[2] ”Privacy Enhancing Technologies - The Path to Anonymity”: Report from the Information and Privacy Commissioner of Ontario, Canada and the Dutch Data Protection Authority (Registratiekamer)

3.9.2 The new NHS Number is a ten-digit number in which the tenth digit acts as a “modulus 11” check digit - a means of minimising the risk of accidentally transposing or mis-typing the other nine digits. It is important to appreciate that the check digit system only works when numbers are entered on a computer or terminal which automatically carries out the validation calculation. Thus use of the check digits is of no value in detecting transcription errors in hand written entries. A second category of errors that will not be detected is the entry of a valid NHS number referring to the wrong patient.

3.9.3 Although unique, because of the risk of transposition error in recording the NHS number, additional items such as sex, or date of birth may be used as corroboration.

3.9.4 In addition to the use of the new NHS Number within the NHS, an NHS Number Tracing Service has been established to provide a means by which an individual’s NHS number may be traced.

# 4. Conclusions & Recommendations

## 4.1 Conclusions

4.1.1 We concluded that all items of information which relate to an attribute of an individual ought to be treated as potentially capable of identifying patients, to a greater or lesser extent, and should be appropriately protected to safeguard confidentiality. Note should be taken of the degree of difficulty involved in actually identifying a specific individual, and this should be balanced against the purpose and usefulness of the specific items of information.

4.1.2 We concluded that all the purposes which we identified are, *in the context of current policy*, justifiable and valid service requirements - for planning, for managing the NHS, and for supporting accountability. As an illustration of the method by which we arrived at our conclusions, Appendix 8 presents an example of a detailed dataflow mapping - contracting information - together with a cross-reference for each item of patient-identifiable information against its purpose.

4.1.3 We were conscious however that our conclusions about the justification of the purposes for which patient information flows, could only relate to the particular point in time at which we conducted our review. It would, therefore, be misleading to place too much emphasis upon our conclusions in this area given changes in government policies and service requirements. We have therefore concentrated on establishing good practice principles which we think are of more lasting value, and on calling for regular and routine testing of information flows against these principles.

4.1.4 We concluded that whilst there was no significant evidence of unjustified use of patient-identifiable information, there was a general lack of awareness throughout the NHS at all levels of existing guidance on confidentiality and security, increasing the risk of error or misuse**.** Problems posed by poor access controls were identified. The Recommendations proposed in this Report are designed to focus attention on the procedures and systems where we identified a weakness, and to propose solutions.

4.1.5 A small number of information items included within existing primary care flows were considered to be redundant by the Committee. These information items do not render patients appreciably more identifiable and there would be significant costs incurred by precipitate action. Therefore these findings have been fed into the forthcoming review of the current GMS forms and do not feature in the recommendations.

## 4.2 Recommendations

### 4.2.1 General Principles

4.2.1 From our consideration of existing information, we identified a number of general principles, which can be applied to other current flows and any new flows which may be proposed in the future. These principles are set out in Figure 3 below.

4.2.2 These principles provide a framework of good practice which should be adopted by all organisations which have access to patient information.

**Recommendation 1:** Every flow of information, current or proposed, should be tested against these principles as a matter of course. Continuing flows should be re-tested regularly and routinely.

4.2.3 Although the precise method of testing a specific use of patient-identifiable information will necessarily be a matter for judgement, the test should be rigorous, explicit and open to external scrutiny. A suggested methodology is outlined in Appendix 12**.** This detailed approach supports consideration of the information requirements of each specified purpose.

4.2.4 When establishing the purpose(s) for which patient-identifiable information is to be used, or when monitoring an existing use, it is important to consider the extent to which each purpose can be, or is being, effectively achieved. A purpose which cannot realistically be satisfied, whether because of poor quality information or another reason, should not justify the collection and use of patient-identifiable information.

## 4.3 Building Awareness

4.3.1 It was apparent that although the Department of Health guidance on *The Protection and Use of Patient Information* and on *IM&T security* had been available to the NHS for more than twelve months, the impact of the specific arrangements it sought to promote had been limited.

4.3.2 We thought that many of the concerns about confidentiality which exist might be addressed by the implementation of guidance amongst all levels of the NHS. Effectiveness in this context however requires more than a wider distribution of written material. It requires the establishment of a new culture for handling information - not a quick and easy task!

**Figure 3 - General Principles**

- **Principle 1 -** ***Justify the purpose(s)***

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

- **Principle 2 -** ***Don't use patient-identifiable information unless it is absolutely necessary***

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

- **Principle 3 -** ***Use the minimum necessary patient-identifiable information***

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

- **Principle 4 -** ***Access to patient-identifiable information should be on a strict need-to-know basis***

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

- **Principle 5 -** ***Everyone with access to patient-identifiable information should be aware of their responsibilities***

Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- **Principle 6 -** ***Understand and comply with the law***

Every use of patient-identifiable information must be lawful. Someone in each organisation[3] handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

[3] For example NHS Trust, Health Authority, Fund-holding practice, PHLSB or other body carrying out work on behalf of the NHS.

4.3.3 We were particularly concerned that patients are not adequately informed of the uses to which information about them might be put. The Department's guidance includes a model notice for patients and there are examples of good practice in existence which could be built upon, for example the GP Practice leaflet devised by Dr Alan Hassey of the Fisher Medical Centre, Skipton. (Appendix 10). However, whilst this problem should be addressed in part by the effective dissemination and implementation of existing guidance as recommended in this report, we believe that more detailed work is required in this area.

**Recommendation 2**: It is recommended that a programme of work, led by the NHS Executive, be established to reinforce confidentiality and IM&T security requirements amongst all staff within the NHS, with senior managers being specifically targeted to remind them of their responsibilities for maintaining security and confidentiality within their organisations. This programme should include:

- effective dissemination of existing guidance;
- the establishment of local codes of conduct aimed at safeguarding patients' rights in this respect;
- appropriate awareness training to ensure that all staff who have access to patient-identifiable information are fully aware of their obligations to respect and protect the confidentiality of that information;
- a duty of confidence requirement in staff contracts and induction processes that ensure newly recruited staff are informed of policies and procedures as part of standard induction processes;
- undertaking work in conjunction with the clinical professions and patient groups, to produce readily accessible material for patients which will clearly inform them about the uses to which information about them may be put, and to establish the most effective ways of disseminating this information;
- ensuring that, in all cases where access to patient-identifiable information held electronically is necessary, computer systems must adhere to the requirements set out in the NHS Executive's IM&T Security Manual, implement appropriate security controls and provide audit trails of access to such information.

## 4.4 A Framework of Responsibility

4.4.1 Whilst it is essential that action is taken to raise awareness of confidentiality and security requirements, we recognise that progress will be slow and variable. We suggest that a degree of performance management is also required where there are particular concerns about the protection and use of patient information. To support a performance management framework, responsibility for safeguarding confidentiality of data flows needs to be attributable to a named individual within each organisation.

4.4.2 This individual would be responsible for ensuring that where there is scope for local flexibility, the purposes for which patient information is used within an organisation are robustly justified, that the minimum necessary information is used in each case and that good practice and security principles are adhered to.

**Recommendation 3**: A senior person should be nominated in each NHS organisation, including the Department of Health and associated agencies, to act as a "guardian". The "guardian" should normally be a senior health professional or be closely supported by such a person. The NHS IM&T Security Manual (Section 18.4) requires each organisation to designate a senior medical officer to oversee all procedures affecting access to person-identifiable health data. This role and that of the "guardian" may be combined, providing there is no conflict of interest. The Department of Health should take the development of this role forward in partnership with interested parties.

4.4.3 Individuals and other bodies with the responsibility of safeguarding the confidentiality of patient information will require clear guidance.

**Recommendation 4:** Guidance must be provided for those individuals/bodies responsible for approving uses of patient-identifiable information (for example. the "guardian" or research ethics committees) to enable them to critically appraise new proposals and continuing practice.

4.4.4 Nationally prescribed flows of patient-identifiable information, for example the core component of minimum data sets, should be subject to rigorous review to ensure that the principles in this Report are adhered to. The Department of Health should consider whether existing committees, for example The Review of Central Returns (ROCR) or the Committee for the Regulation of Information Requirements (CRIR), are able effectively to discharge these responsibilities.

4.4.5 A relevant example of an area where the "guardian" should play an active part is the transfer of patient information to support interprofessional warnings, for example where an individual represents a significant threat to the safety of others. This caused the Committee concern as it was not clear that warnings were always justified, nor effectively targeted geographically. Interprofessional warnings about particular patients should be authorised by the "guardian" taking account of the principles laid down in *The Protection and Use of Patient Information* and in this report. Where there are serious concerns about public and/or health service staff safety, it is clearly important that authorisation be given swiftly.

### 4.5 Development of protocols for the exchange of patient-identifiable information

4.5.1 Whilst it is important that the confidentiality of patient information is safeguarded, particularly where information is transferred between the NHS and partner organisations, it is essential that this does not act as a barrier to the provision of care.

4.5.2 There are many situations where we feel that the exchange of patient-identifiable information is necessary for the efficient and effective operation of the NHS and its partner organisations. Information flows supporting shared or transferred care are essential if patients are to receive seamless care. The goal is clearly to ensure that those who *need to know* have ready access to sufficient and appropriate information.

4.5.3 However we believe that it is also essential to ensure that those asked to transfer patient information can be confident that all those involved are fully aware of the basis on which that information is being transferred, and adhere to consistent protocols. There were particular concerns relating to a perceived loss of control of patient information once it had been transferred to other organisations for legitimate purposes ie. that there might be secondary uses of the information which fail to respect patient confidentiality.

4.5.4 Whilst recognising the need for a degree of local flexibility, based on local operating arrangements, we believe that there is a need for consistency of approach throughout the country which could be based upon some common frameworks.

**Recommendation 5:** We wish to see the Department and the NHS, along with partner organisations, jointly identify the key areas in which protocols are required and prepare and publish good practice frameworks for local adoption in these areas. A sample framework, based on existing good practice, is provided in Appendix 11.

**Recommendation 6:** It is further recommended that consistent with the framework of responsibility advocated by this report, each NHS and non-NHS organisation clearly establishes and communicates to partner organisations who is responsible for monitoring the sharing and transfer of information within the agreed local protocol.

4.5.5 Where there is a need to share information about patients, it is important that all organisations contributing to the provision of seamless care are able to inspire mutual confidence in their internal procedures and standards of confidentiality. A form of accreditation, which should be promoted as an opportunity for partner organisations to demonstrate high standards, should be explored.

**Recommendation 7:** The possibility of an accreditation system, which would recognise those organisations which follow good practice with respect to confidentiality, should be explored by the Department of Health in partnership with interested groups.

### 4.6 Minimising Patient-Identifiability

4.6.1 Whilst it may be necessary for a patient to be *identifiable*, we thought that outside of the provision of care it should rarely be necessary for individuals to be *identified*.

4.6.2 For an individual to be *identifiable*, but not *identified*, there must be a mechanism for using the information available to establish identity. For example an individual would be identifiable if NHS number and perhaps postcode (for corroboration) were known, but would not be identified.

4.6.3 As noted earlier in this report, we thought that no single item of information can be relied upon uniquely to identify an individual. It is likely that the NHS number will eventually become sufficiently reliable in some areas where the purpose is other than to provide care, for example where a small but continuing error rate is acceptable, and this is clearly a desirable goal.

4.6.4 In the interim, however, we thought that substitution of the NHS number for patient details (particularly name and address), supported as necessary by other items which would reduce the risk of error to an acceptable level (e.g. date of birth and/or post code), would represent substantial progress. This would remove the risk of immediate recognition of an individual patient by those staff handling the information who did not need to know the patient's identity.

4.6.5 Where particular items of information, such as date of birth or postcode, are required for purposes other than confirmation of identity, there may be sufficient justification, on practical grounds, for these specific items to accompany the NHS number. Such exceptions should be robustly justified.

4.6.6 We recognise however that the use of the new NHS number is only now becoming more widespread. Further work is needed to establish:-

- how quickly it will become a sufficiently robust identifier;
- whether, for an interim period, the new NHS number will need to be accompanied by additional items of information, such as date of birth and/or postcode, to ensure reliability;
- ways of supporting longitudinal uses of patient data eg incorporating individuals who died prior to the introduction of the new NHS number.

**Recommendation 8:** The new NHS number should replace patient-identifiable data, as soon as practically possible, in every data flow where there is a need to distinguish between individuals but where there is no immediate corresponding need to identify those individuals. Continued use of additional patient-identifiable data items for other purposes must be robustly justified. The Department of Health should urgently pilot the use of the NHS number as the main identifier, eg in contracting flows.

4.6.7 The ease with which patients who are identifiable from information can be identified is clearly extremely important, and the mechanism for doing so must be carefully controlled. Replacing more readily patient-identifiable information with a coded identifier will be worthless if access to tracing services is not restricted.

**Recommendation 9:** The NHS Executive, in partnership with professional bodies, should develop strict protocols to define which individuals are authorised to gain access to patient identity, (e.g where the new NHS number is the main identifier, through use of the NHS Number Tracing Service or through access to administrative or other population registers), and under what circumstances access should be authorised.

4.6.8 Although we believe that the recommendations above should safeguard confidentiality for most purposes, there is concern that the new NHS number may not be a sufficiently secure main/sole identifier for information flows of a particularly sensitive nature, for example from clinicians to the Public Health Laboratory Service (PHLS) where HIV/AIDS is involved. In the case of information flows which include such sensitive material, the use of appropriate privacy enhancing technologies, for example encryption of the NHS number, must be explored as a matter of urgency.

**Recommendation 10:** Where particularly sensitive information is to be transferred, the use of privacy enhancing technologies (e.g. encrypting the NHS number) must be urgently explored.

## 4.7 Systems Design

4.7.1 We also thought it essential that the patient-based information systems which are used within the NHS should be built around the principle of protecting the privacy of individuals and should be designed to incorporate appropriate privacy enhancing technologies at the outset.

4.7.2 Furthermore we thought that those staff working on the development and implementation of such systems should be fully aware of the issues relating to confidentiality and the importance and relevance of such technologies.

**Recommendation 11:** We recommend that the appropriate trade and professional associations[4] are encouraged to raise awareness amongst their members, and that institutions providing training in healthcare informatics are encouraged to include privacy enhancing technologies as part of those training programmes.

4.7.3 We were particularly concerned about the capacity, using new technologies, to transfer information easily and from one individual or organisation to another, without effective monitoring or regulation.

**Recommendation 12:** The internal structure, and administration, of databases should reflect the principles developed in this report, e.g. separating patient-identifying details from event, treatment, or condition information with linkage possible only under specific and controlled circumstances. Whilst it is recognised that there may be practical barriers to restructuring existing databases, the practicalities of doing so should be explored.

## 4.8 Primary Care

4.8.1 Although the earlier recommendations apply to primary care, there are a number of specific additional concerns in this area which require separate recognition. We were particularly concerned about the flows of patient information to support registration and claims for payment in primary care, particularly contraceptive claims.

**Recommendation 13:** The new NHS number should replace the patient's name on Items of Service Claims made by General Practitioners as soon as is practically possible. The software used by all General Practitioners, the Dental Practice Board and Health Authorities should be reviewed to determine the resource consequences of specification changes which would be required to support changes in practice as recommended in this report.

4.8.2 Although we recognise that the cost of immediately replacing existing paper forms relating to prescribing would far outweigh any likely benefit, the opportunities provided by the development of electronic means of transferring details should be taken to apply to the principles developed in this report.

**Recommendation 14:** The design of new systems for the electronic transfer of prescription data should incorporate the principles developed in this report.

[4] Such as the association for IM&T professionals in healthcare (ASSIST), the British Computer Society (BCS), the Computer Suppliers and Services Association (CSSA), the Clinical Professions Information Advisory Group (CPIAG), the Nursing Professions Information Group (NPIG), the Academy of Medical Colleges Information Group (ACIG) and the Medical Information Group (MIG).

4.8.3 We also believe that, consistent with the principles outlined in this Report, it is important that transfers of patient information are robustly justified and that alternatives to the transfer of patient information are developed wherever practicable.

**Recommendation 15:** Negotiations on pay and conditions for GPs should have regard to the desirability of avoiding systems of payment which require patient-identifying details to be transmitted (see recommendation 16).

4.8.4 Under the NHS (Primary Care) Act 1997, new arrangements for the provision of personal medical services and personal dental services will be piloted. These pilots will focus attention upon information handling and confidentiality requirements in the primary care setting, in addition to opportunities to test ways of satisfying existing legitimate purposes without requiring the transfer of patient information.

**Recommendation 16:** The practicalities of piloting new procedures for claims and payments which do not require patient-identifiable information to be transferred should be urgently considered, e.g. batched claims with details held in general practice for audit purposes.

# Appendix 1 - Membership

Membership of the main Committee and the four separate Working Groups is given below.

## Main Committee

| | |
|---|---|
| Dame Fiona Caldicott **(Chair)** | Principal of Somerville College, Oxford and Consultant Psychiatrist |
| Dr Philip Leech | Principal Medical Officer, NHS Executive Primary Care Division |
| Dr James Willis | GP Principal, Alton |
| Professor Rod Griffiths | Director of Public Health, NHS Executive West Midlands Region |
| Rosemary Butler | Director of Statistics, Department of Health |
| Ray Rogers | Executive Director, NHS Executive Information Management Group |
| Annette Holbrook | Director of Information, Calderdale & Kirklees Health Authority |
| Dr Jeremy Metters | Deputy Chief Medical Officer, Department of Health |
| Dr Chris McCall | GP Principal, Corfe Mullen, Dorset |
| Dr Barry Tennison | Director of Public Health, West Hertfordshire Health Authority |
| Dr Myriam Lugon | Medical Director, Whipps Cross Hospital |
| Penny Payne | Information Systems Manager, Kent Social Services |
| Martin Staniforth | Head of Corporate Affairs, NHS Executive HQ |
| Tricia Hart | General Manager and Chief Nurse, York Health Services NHS Trust |
| Professor Alastair Bellingham | Royal College of Pathologists |

| | |
|---|---|
| Dr Elaine Gadd | Senior Medical Officer, Department of Health |
| Sandy Taylor | Chief Executive, Dorset Community NHS Trust |
| Julia Neuberger | Chair, Camden & Islington Health Authority |
| Barry Slater | Secretariat |
| Phil Walker | Secretariat |

**Primary Care Working Group**

| | |
|---|---|
| Dr Philip Leech<br>**(Chair)** | Principal Medical Officer, Primary Care Division, Department of Health |
| Dr James Willis | GP Principal, Alton |
| Dr Sarah Baker | Director of Primary & Community Care, Leeds Health Authority |
| Helen Campbell | Health Promotion Division, Department of Health |
| David Sexton | Information Analyst, East Kent Health Authority |
| Dr Robert Scholefield | GP Principal, Ledbury |
| Ruth Walker | GP Practice Manager |
| Chris Parks | FHS Computer Unit |
| Keith Dowthwaite | Audit Commission |
| John Thompson | Primary Care 2 Division, Department of Health |
| Don Mulholland | Secretary of the IOW Local Pharmaceutical Committee |
| Douglas Ball | Prescription Pricing Authority |
| Giles Denham | Primary Care Division, Department of Health |
| Mike Sowerby | Primary Care Division, Department of Health |
| Jerry Read | Primary Care Division, Department of Health |
| Diane Kennard | Primary Care Division, Department of Health |
| Chris Audrey | Primary Care Division, Department of Health |
| Phil Walker | Secretariat |

### Multi-Agency Working Group

| | |
|---|---|
| Sandy Taylor<br>**(Chair)** | Chief Executive, Dorset NHS Community Trust |
| Philip Sands | Director of Contracting, Calderdale & Kirklees Health Authority |
| Dr Gyles Glover | Mental Health Services Division, Department of Health |
| Dr Elaine Gadd | Health Promotion Division, Department of Health |
| Susan Knight | Information Management Group, Department of Health |
| Dr Myriam Lugon | Medical Director, Whipps Cross Hospital |
| Dr Simon Wood | Hull & Holderness Community Health NHS Trust |
| Carl Petrokofsky | NHS Executive Anglia & Oxford |
| Catherine Staite | Mental Health Services Division, Department of Health |
| Catherine Borowy | Social Care Group, Department of Health |
| Robert Lake | Staffordshire County Council, Director of Social Services |
| Raymond Warburton | Social Care Group, Department of Health |
| Carole Jobbins | Public Health, North West Regional Office, Department of Health |
| Louise Silburn | Community Care Division, Department of Health |
| Phil Walker | Secretariat |

### Operational Management Working Group

| | |
|---|---|
| Professor Alastair Bellingham<br>**(Chair)** | Royal College of Pathologists |
| Rosemary Butler | Director of Statistics, Department of Health |
| Paul Eveson | Information Management Group, Department of Health |
| Christine Hatton | Director of Information, Berkshire Health Authority |

| | |
|---|---|
| Dr Chris McCall | GP Principal, Dorset |
| Dr Barry Tennison | Director of Public Health, West Hertfordshire Health Authority |
| Dr John Todd | Leicester Royal Infirmary |
| Phil Walker | Secretariat |

**Health of Populations Working Group**

| | |
|---|---|
| Dr Jeremy Metters **(Chair)** | Deputy Chief Medical Officer, Department of Health |
| Dr Barry Tennison | Director of Public Health, West Hertfordshire Health Authority |
| Annette Holbrook | Director of Information, Calderdale & Kirklees Health Authority |
| Dr Vicky King | Communicable Disease, Health Promotion Division, Department of Health |
| Dr Mike Catchpole | Communicable Disease Surveillance Centre |
| Dr Liz Tebbs | Environment and Food Division, Department of Health |
| Dr Paul Thornton | Coventry Health Authority, GP |
| Dr Edmund Jessup | Director of Public Health, West Surrey Health Authority |
| Dr Graham Copeland | Consultant Surgeon, Warrington General Hospital |
| Dr Jennie Carpenter | Health Care Directorate, Department of Health |
| Dr Patricia Cresswell | Consultant in Public Health Medicine, Northern & Yorkshire, Department of Health |
| Charles Stiller | Cancer Registry |
| Dr John Fox | Director of Census Population and Health Group, Office of National Statistics |
| Phil Walker | Secretariat |

# Appendix 2 - Confidentiality: the legal framework

***General***

1. There is no general statutory right for an individual to sue another person for damages for breach of confidentiality, and the legal position can only be ascertained from a study of the common law. It is generally accepted however that in a healthcare context there is a well-established common law duty of confidence. The courts rarely revisit the principle that personal health information is subject to a duty of confidentiality in the following circumstances:

   - where information is not a matter of public knowledge; *and*

   - information is entrusted by an individual in confidence where there is a general obligation not to disclose the information without consent.

2. The basic principle in relation to patient information is that patient information is confidential to the patient and should generally not be disclosed without consent unless justified for a lawful purpose. The exceptions are set out in detail in the Department's guidance.

3. An example of when disclosure without consent may be necessary for a lawful purpose is where it is required by statute. The term "required by statute" is very difficult to pin down accurately since it is a term used to connote a broad range of disclosures. Loosely, the term is used to cover cases where legislation (whether primary or secondary) imposes an obligation to pass information to another - usually specified - person, regardless of any common law duty of confidentiality which may otherwise exist. The main examples are listed in Figure 4.

4. Injunctions have been used successfully to prevent breaches of confidence, but such civil action is less effective after the event. Civil claims for damages have rarely been brought in medical cases because it is generally considered that damages for mental distress are very difficult to prove (a claim for an account of profit, if demonstrable, might be more likely to succeed).

**Figure 4 - Examples of information "required by statute"**

- **s11, Public Health (Control of Disease) Act 1984** - Duty to notify proper officer of the local authority of the name, age, sex, and address of a person suffering from a notifiable disease or food poisoning;

- **s124, National Health Service Act 1977** - Duty of child's father or person in attendance on mother at a birth to notify the proper authority of the birth or stillbirth;

- **reg 4-5 Abortion Regulations 1991** - Duty of a medical practitioner to notify of abortions carried out and circumstances in which further disclosure of that information may be required or requested;

- **s18, Prevention of Terrorism Act 1989** - Power to require the production of information from any person; also makes it an offence to fail to volunteer that information;

- **Regulations made under the Health and Safety at Work Act 1974**- Notification of industrial accidents and diseases;

- **s172, Road Traffic Act 1988** - Power to require any person to disclose information which may lead to the identification of a person guilty of certain offences.

- **s1, AIDS Control Act 1987 -** Duty of health authority and others to make reports of numbers of persons with AIDS or known to be HIV-antibody -positive.

**Specific Legislation**

5. Wider concerns about the security of data held on computers has led to a body of legislation which criminalises misuse and unauthorised access to computerised information. This legislation currently includes:

- The **Data Protection Act 1984** covers all "personal data" (including patient information) relating to living individuals that are held on a computer system. NHS bodies which use computerised information must register with the Data Protection Registrar the purposes for which they hold personal information, sources and disclosures. It is a criminal offence to hold or disclose information in breach of the registration requirements of the Act.

- The **Computer Misuse Act 1990** provides criminal sanctions against unauthorised access or damage to computerised information. Authorised users have permission to use certain programmes and data. If those users go beyond what is permitted, it is a criminal offence. The Act makes provision for accidentally exceeding permitted activities and also covers fraud, extortion and blackmail.

### *EC Data Protection Directive*

6. The Directive will not become law until legislation has been enacted in this country and consideration of its impact is necessarily somewhat speculative at present. The main provisions of the Directive must be implemented by October 1998, three years after it was adopted by the EC. Although a degree of caution is warranted, there are a number of general points which can be made.

7. The Directive will apply to the processing of certain data by manual means as well as to automatic processing, and in this respect it is wider than our current Data Protection legislation.

8. The Directive prohibits, with some notable exceptions, the processing of personal data concerning health, except in certain limited circumstances. Most, if not all, NHS data processing fall within what can be loosely called the health care exception. The healthcare exception to the prohibition in Article 8 applies if the processing is required *"for the purpose of preventative medicine, medical diagnosis, the provision of care or treatment or management of healthcare services, where that data is processed by health professionals subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy".*

9. The Directive establishes a set of principles with which users of personal information must comply, requires certain information to be provided to individuals whose personal information is processed, gives individuals rights of access to information held about them and provides for a supervisory authority to oversee and enforce the law.

10. The Data Protection Registrar has suggested that the current requirement of confidentiality in the NHS supported by the existing guidance from the Department of Health is, in her opinion, insufficient to meet the requirements of Article 8 of the EC Directive.[5]

11. However, it will not be possible to say what the precise impact of the Directive will be on the NHS until the framework for implementation is established. The main difference may be that what is currently done as a matter of good practice, or in pursuance of common law requirements, will be embodied in legislation.

[5] Data privacy in medicine : a perspective offered by the Data Protection Registrar, British Journal of Healthcare Computing 1997 Vol 14 Number 2 pp 20:22

# Appendix 3 - Summary of data flow mappings

1. The following pages contain a listing of the dataflows considered by the Working Groups. A full detailed dataflow mapping containing details of the specific data items associated with each flow is available on request from Richard Walker, NHS Executive, Quarry House, Leeds LS2 7UE.

2. Where a flow assessment of "partially justified" is given there is an additional comment indicating the specific issue related to that flow.

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

Insert Table here

# Appendix 4 - Reference documentation

The Committee took note of the following documents:

| **Source** | **Title** |
|---|---|
| Office of Statistics | Maintaining the Confidentiality of Data |
| Department of Health | HSG(96)18 "The Protection and Use of Patient Information" |
| NHS Executive Information Management Centre | The NHS IM&T Security Manual |
| | Code of Practice on Access to Government Information |
| Department of Health | Code of Practice on Openness in the NHS |
| Information & Privacy Commissioner of Ontario, Canada and the Dutch Data Protection Authority (Registratiekamer) | Privacy Enhancing Technologies - The Path to Anonymity |
| BMA | Security Principles |
| National Academy of Sciences | For the Record "Protecting Electronic Health Information" |

# Appendix 5 - Existing principles

This Appendix summarises some of the existing relevant guidelines and principles.

**Department of Health Guidance**

1. Guidance was provided for the NHS by HSG(96)18 *"The Protection and Use of Patient Information"* and all NHS organisations, and broadly those providing services to the NHS, are expected to comply with its requirements. Patient information is defined in the guidance as "all personal information about members of the public held in whatever form by or for NHS bodies or staff". This includes personal non-health information e.g. name, address and details of financial or domestic circumstances.

**Basic Principles**

2. The guidance states that information may be passed on for a particular purpose with the patient's consent or on a "need to know" basis in certain circumstances.

3. The guidance states that, in the interests of the NHS being able to respond effectively to the public's needs, patient's specific consent is not required each time information needs to be passed on for a particular purpose but that there is a "need for patients to be fully informed of the uses to which information about them may be put".

4. The "need to know" circumstances outlined in the guidance are:

- for NHS purposes where the recipient needs the information because he or she is or may be concerned with the patient's care and treatment, but also for:

  a) assuring and improving the quality of care and treatment;

  b) monitoring and protecting public health;

  c) co-ordinating NHS care with that of other agencies;

  d) effective health care administration;

  e) teaching;

  f) statistical analysis and medical or health service research to support a)-e)

- the information is required by statute or court order; or

- passing on the information can be justified for other reasons, usually for the protection of the public.

The guidance makes clear that personal information should be anonymised wherever possible but that anonymisation does not, of itself, remove the duty of confidence. It may still be passed on only for a justifiable purpose.

### GMC Guidance for Doctors

The guidance for doctors from the General Medical Council states that:-

"Patients have a right to expect that their doctor will not disclose any personal information which you learn during the course of your personal duties, unless they give permission. Without assurances about confidentiality patients may be reluctant to give doctors the information they need in order to provide good care.

For these reasons:

- when you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is disposed of, stored, transmitted or received.
- when patients give consent to disclosure of information about them, you must make sure they understand what will be disclosed, the reasons for disclosure and the likely consequences.
- you must respect requests by patients that information should not be disclosed to third parties, save in exceptional circumstances (for example, where the health or safety of others would otherwise be at serious risk).
- you must make sure that patients are informed whenever information about them is likely to be disclosed to others involved in their health care and that they have the opportunity to withold permission.
- if you disclose confidential information you should release only as much information as is necessary for the purpose.
- you must make sure that health workers to whom you disclose information understand that it is given to them in confidence which they must respect.
- if you decide to disclose confidential information, you must be prepared to explain and justify your decision."

**UKCC Guidance for Nurses**

The guidance for nurses from the UKCC states that:

- a patient or client has the right to expect that information given in confidence will be used only for the purpose for which it is given and will not be released to others without their permission;
- you should recognise each patient's or client's right to have information about themselves kept secure and private;
- if it is appropriate to share information gained in the course of your work with other health or social work practitioners, you must make sure that as far as is reasonable, the information will be kept in strict professional confidence and be used only for the purpose for which the information was given;
- you are responsible for any decision which you make to release confidential information because you think this is in the public's best interest;
- if you choose to break confidentiality because you believe this is in the public's best interest, you must have considered the situation carefully enough to justify that decision; and
- you should not deliberately break confidentiality other than in exceptional circumstances.

**Data Protection Act: the eight principles**

The Data Protection Act contains eight key principles, namely:-

- the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
- personal data shall be held only for one or more specified and lawful purposes.
- personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or purposes.
- personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
- personal data shall be accurate and, where necessary, kept up to date.
- personal data held for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
- an individual shall be entitled, at reasonable intervals and without undue delay or expense, to be informed by any data user whether he holds personal data of which the individual is the subject and to have access to any such data held by a data user and where appropriate, to have such data corrected or erased.
- appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

**NHS IM&T Security Policy principles**

- A management structure should be established within each organisation to ensure information security within the NHS.
- IM&T security officers should be designated in each organisation within the NHS.
- Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during employment.
- Equipment should be physically protected from security threats and environmental hazards.
- Responsibilities and procedures for the management and operation of all computers and networks should be established.
- Exchange of data and software between organisations should be controlled and carried out on the basis of formal agreements.
- Logical access controls should restrict access to application systems and data to authorised users. Where personal health data in a person identifiable form is involved, access controls require particular attention and regular review.
- Wherever possible, patient information should be fully anonymised, but where this is not possible, the number of data items which could aid identification of any individual should be minimised.
- Appropriate security controls, including audit trails, should be designed into application systems.
- All relevant statutory and contractual requirements should be explicitly defined and documented for each system. The controls, countermeasures and individual responsibilities to meet these requirements should be similarly defined and monitored.

## EC Directive on Data Protection : principles relating to data quality

The EC Directive on Data Protection adopted on 24th October 1995 states that:-

"Member States shall provide that personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use."

## The Code of Practice on Access to Government Information

1. The Code of Practice on Access to Government Information came into force in April 1994. A slightly revised edition of the Code came into force on 1 February 1995 (Rev 1997).

2. Under the Code, there is a presumption that Government departments will release information unless there is good reason for it to be withheld under one or more of 15 exemptions in Part II of the Code. If the Department decides to turn down a request for information, in full or in part, an explanation of which exemption applies must be given. The person requesting information must also be informed of the review arrangements, which consist of an internal review, followed by recourse to the Ombudsman.

### *The Exemptions*

3. There are fifteen exemptions in Part II of the Code. The most relevant to Department of Health staff include the following:

- exemption 2 protects from disclosure internal policy advice or opinion which has been given to Ministers leading up to a policy decision;

- exemption 7(b) is relevant when the release of information might undermine the efficient running of the Department or some other public body or authority, such as an NHS organisation;

- exemption 11 may apply to certain information which relates to research or is held for surveillance for health and safety purposes;

- exemption 14 could apply where a request is received for information which was supplied in confidence or where disclosure would harm the individual's physical or mental health.

4. In judging whether any particular exemption might apply staff are required to consider whether the public interest in releasing the information outweighs any possible risk from disclosure.

### *Protection Offered by the Open Government Codes of Practice*

5. The confidentiality of the doctor-patient relationship is, arguably, implicit in exemption 14 of the Code on access to Government Information, "Information given in confidence", although the Code itself does not specifically refer to the common law duty of confidentiality.

6. A Code of Practice on Openness in the NHS, complementing the central government Code, came into force from 1 June 1995. The guidance to the NHS is somewhat clearer on this point. Section 9 of the Code of Practice on Openness in the NHS outlines what information may be withheld. Paragraph (vii) reads as follows: *Information given in confidence. The NHS has a common law duty to respect confidences except when it is clearly outweighed by the public interest.*

# Appendix 6 - Technical issues

**Introduction**

1. Levels of concern over the confidentiality of patient data have been raised in the last few years as a result of the increasing use of information technology within the health service and the possibility that unauthorised or inappropriate access to personal data may become more likely as a result.

2. In the past unauthorised and inappropriate access to such data was inhibited as it was often held in a variety of locations and in paper format, which made it difficult to first locate specific personal data and then share it. While providing a measure of protection of privacy, this also made the job of healthcare professionals harder. The introduction of new technologies is aimed at providing support to healthcare workers, and improving the effectiveness and efficiency with which care can be given to patients.

3. Although the focus of the work of the Review Group has been on issues surrounding confidentiality, some consideration has been given to the technical issues which may offer means of enhancing confidentiality within information systems. This Appendix presents a brief summary of some of the terms and techniques relating to the means by which privacy may be enhanced.

**Privacy Enhancing Technologies**

4. Privacy enhancing technologies is the name given to a range of approaches to ensuring the privacy of data.[6] [7] At one extreme this may involve simple password protection at point of access, through to sophisticated data encryption and access control mechanisms.

5. The Data Protection Registrar is supportive of the notion that privacy enhancing technologies (PETs) should be used to help minimise the risk of unnecessary or unlawful disclosure of personal information.

6. PETs provide the means by which security of data can be enhanced, but depend crucially on establishing sound and widely accepted principles of confidentiality upon which to build. Some examples of different forms of PETs are outlined below.

[6] "Privacy-Enhancing Technologies - The Path to Anonymity" : Report from the Information and Privacy Commissioner of Ontario, Canada & the Dutch Data Protection Authority (Registratiekamer)

[7] Data privacy in medicine : a perspective offered by the Data Protection Registrar, British Journal of Healthcare Computing 1997 Vol 14 Number 2 pp20:22

### Physical Access Control

7. Although not a privacy enhancing technology, one of the most basic security measures is control of access to the physical computer equipment itself. This is normally associated with the physical protection of locations and the siting of equipment. By controlling physical access of individuals to those sites and equipment, an initial level of privacy can be established.

8. As an example, the NHS-wide Clearing Service application operates on equipment located in a purpose-built data centre with controlled access, perimeter security fencing, and 24 hour a day camera surveillance and security cover. Within the data centre the application is physically and electronically isolated from any other computer system or network and within an environment which contains a limited number of secure terminals, access to which is limited to a small number of authorised staff for maintenance purposes only.

### Logical Access Control

9. The next level of security, and one where PETs apply, is in relation to providing control over access to the system. Through the use of passwords, authentications and associated privileges, a range of logical access controls may be implemented whereby only certain users are permitted to use specific terminals to access a system and perform certain specified functions. Furthermore combinations of user identities, terminals and functions can be restricted to specific data records or subsets of those records. For example a user may be granted update rights on the full database when using their own personal terminal in a secure office but may only be permitted to carry out read-only functions on a subset of the database if accessing the system from another terminal.

### Audit trails

10. Audit trails can provide details of systems access, communications into and out of a system and the use of software utilities, which are thought to be particularly sensitive, as well as accesses to a set of records held within a database. Audit trails usually contain details about the user - both the individual users as well as the physical device from which they accessed the system - together with details of the transactions or functions that they carried out on the system. The level of detail of data about the transactions can vary from basic details of the type of access - view, create, amend, delete - to complete copies of a system database before and after the access. This allows for an analysis of not only the type of access, but also the actual changes, which were made to the database.

11. Although they are important tools to protect privacy, audit trails need to be configured and managed carefully. In some instances organisations have been found to have switched off audit trail features to speed up normal processing, which totally negates their value. However, new systems are addressing this by removing all facilities to switch off audit procedures.

12. Furthermore where audit trails are used, there must be appropriate management review and monitoring procedures to identify and investigate instances where there may be cause for concern.

13. As an example, the NHS-wide Clearing Service contains a secure message audit log which records the receipt and transmission of all messages into and out of the application, and a secure database audit log which records all activity on the database itself. The secure audit logs cannot be deleted and are archived whenever the database is archived.

**Pseudonymity**

14. Pseudonymity relates to the concept whereby data is exchanged with some in a format that is not totally anonymised, but the identifying attributes of the data are restricted only to a controlled set of individuals and/or for a defined set of purposes.

**Encryption**

15. Encryption is the process whereby information held in plain-text format - that is characters and codes that are clearly intelligible to the human reader - is converted into a sequence of alternative characters and codes which cannot be readily understood. This involves applying a set of rules - an algorithm - to the plain-text format to generate the encrypted material.

16. The set of rules in the encryption algorithm is always the same, and is used in association with a 'cryptographic key' which is normally different for each different user and often for each different purpose. The result of the encryption depends on both the encryption algorithm chosen and the length of the key used.

*Symmetric encryption*

17. In symmetric encryption algorithms the same key which is used to encode the plain-text message, can also be used to decode the encrypted message. This means that both the sender and the recipient of a message encrypted using a symmetric algorithm need to know the same key.

18. The security of symmetric encryption is critically dependent on both parties protecting the key and not divulging it to others. Symmetric encryption can also be provided by technology, such as link encryptors that operate across fixed links. These devices do not need users to hold keys as the keys are pre-programmed inside the devices and are capable of being reprogrammed automatically by the devices themselves on a routine basis.

*Asymmetric encryption*

19. In asymmetric encryption algorithms - also known as public key cryptography - one key is used to encode the plain-text message while another different key is required to decode the message. This means that if a recipient A publishes their encoding key widely, then anyone wishing to send a confidential message to person A can use A's encoding - or public - key to encode the message. As long as A keeps their decoding - or private - key secret, then they will be the only ones able to decode and hence read the message.

*Cryptographic services*

20. Public key cryptography has the advantage that it allows confidential transmissions of data to be passed to the sender of the encrypted message without the need for the sender's private key. In addition, by using the

private key, it is possible to perform a number of other valuable functions. These include:-

- **digital signing** - applying a signature using the sender's private key, which can be verified by the recipient using the sender's public key. As yet there is no legal status for digital signatures in the UK, although many bodies have indicated to the government that this is an area which needs clarification.

- **authenticating** - authenticating part or all of a message, using the sender's private key to create a 'check sum' over the parts to be authenticated. This check sum can again be verified by the recipient using the sender's public key;

- **time stamping** - time stamping a message, using the private key of someone who is trusted to operate a reliable clock, the time stamp being verified by any party by the use of the time stamper's public key;

- **non-repudiation** - in which the sender of a message which has been signed using the sender's public key cannot subsequently deny that the message was sent by him.

21. It is also possible for message enclosures to have several levels of digital signing and therefore authentication, e.g. composite documents with several different authors, or batching messages and signing with a single digital signature

22. With the possible exception of time-stamping, these services are sometimes referred to collectively as 'cryptographic services' to distinguish them from the basic encryption of a message to preserve its confidentiality.

*Database encryption*

23. Any of the processes which apply to the transmission of data between two separate users can also be applied to the storage of data. Data transmission can be treated as the movement of data between two users separated in space, and data storage as the movement of data between two users (or possibly the same user twice over) separated in time.

24. Encryption is therefore a technique which can be used both to secure the exchange of data, and also as a tool to ensure that only users with knowledge of appropriate keys can access the contents of a data base, or to allow users to sign and authenticate the contents of parts of a data base.

*Encryption strength*

25. The strength of the encryption process is related both to the choice of encryption algorithm used and the length of the key. Short keys are more easily broken by the application of computer technology to simply attempt to try all possible combinations. However the processing power and time required to break keys in this way is exponentially related to the length - and hence number of different combinations - of the key.

26. Although the difficulty of breaking a key increases very rapidly with key length, the computing resources required to use a key in normal operation increases much more slowly as the key length is increased. Use of a larger key does not therefore increase processing time exponentially.

*Key Management - Trusted Third Parties*

27. For a public key system to work, there needs to be a mechanism whereby the public key for an individual or organisation can be readily accessed, and users must have a reliable means of authenticating the public keys. The role of a Trusted Third Party (TTP) in providing key management services would be to provide a trusted source of information about keyholders and holders of public key directories for those keyholders.

28. It is not necessary for a TTP holding public keys to have any knowledge of the corresponding private keys. All but one of the services listed above as 'encryption services' can also be implemented without the need to involve any form of TTP. The single exception is the secure time-stamping service, where it is an essential element of the service that all those involved have trust in the accurate and inviolate running of the clock which is used to time stamp the messages.

29. TTPs can also allocate and change keys as circumstances dictate. Indeed a TTP need not necessarily be an organisation - it might itself be a trusted computer system or service.

30. At the time of writing, the Department of Trade and Industry is in consultation regarding the licensing of TTPs for the provision of encryption services. The proposals under consultation were put forward by the previous government, and the current government has not yet committed itself to progressing these proposals as they currently stand.

**Separated databases**

31. The concept of a separated database is one in which the main data content is kept separate from the data that enables an individual to be identified. Linkage is controlled through the adoption of a PET, such as the encryption of the personal identifying data items or other internal linking mechanisms. By applying an encryption algorithm to a unique identifier contained within the source data and using a public key, an encrypted but still unique identifier can be stored on the secondary database.

32. In this way the data content held in the secondary database may be used for a range of analytical purposes, including the linkage of different data records through use of the encrypted identifier, but for all practical purposes it is not possible to identify any individual patient.

33. Reverse linkage - ie the identification of an individual from the non-identifiable data - can only be undertaken under tightly controlled circumstances and will require use of a controlled private key.

34. Even in these circumstances, other PETs - such as access control lists - should be employed to ensure that any such reverse linkages are only undertaken by authorised persons, and that any such action is recorded and auditable.

35. However even though the separation of databases in this way offers a means of enhancing privacy, it should only be considered in those circumstances where there is a clear justification that there is any need at all for the storage of the identifiable data.

36. The database managed as part of the NHS-wide Clearing Service has been designed in this way, with episode data and patient-identifiable data held in separate databases, and with a very tightly controlled linkage mechanism. In this way events for the same patient can be linked using internal identifiers in such a way that the actual patient identity is not disclosed to the user.

**Layered databases**

37. A layered database - which may reside on one or several different distributed hardware platforms - is one in which the identifying and non-identifiable data remains in one logical database.

38. The database allows access based on user privileges and data sensitive marking, so that it is possible to provide access to a data record, but hide certain parts on a need to know basis.

# Appendix 7 - Patient-identifiable information

1. The Working Groups identified a number of items by which a person's identity may be established. These include:-

    - Surname
    - Forename
    - Initials
    - Address
    - Postcode
    - Date of Birth
    - Other Dates (i.e death, diagnosis)
    - Sex
    - NHS Number
    - N.I. Number
    - Local Identifier (i.e. hospital or GP Practice Number)
    - Ethnic Group
    - Soundex[8] Code
    - Occupation

2. The groups determined that an individual item from this list, taken with another item from a particular flow, may in certain circumstances enable identify to be inferred, e.g.:-

    - Age linked to a diagnosis;
    - Postcode and the medicine prescribed;
    - Address and the item of service provided.

[8] A soundex code is a phonetic coding system which can be applied to a word to help in the task of matching it with similar sounding words eg Johnston, Johnstone, Johnson.

3. These examples are by no means comprehensive and other combinations of items would serve the same purpose. While it may be helpful to consider items of information as falling within a spectrum of identifiability based on the nature of the item and the context, nevertheless all personal information is confidential and deserves the same respect for privacy.

4. No single item - with perhaps the exception of the NHS Number - can be relied upon uniquely to identify an individual, and even corroborating information is likely to be sought. The degree to which other items might identify an individual will depend on the context - for example an unusual surname may be a stronger pointer to an individual than a more common surname.

5. Studies have shown that the items which could be included with the NHS number to eliminate errors include date of birth, sex, address information or part of the real name.However in assessing the use of other identifiers the discrimination and stability of the additional items must be considered, and of those examples, sex and date of birth are both very stable and, in the case of date of birth, relatively discriminating.

6. Nevertheless all such items should be treated as patient-identifiers to a greater or lesser extent and appropriately protected to protect the privacy of patient data.

# Appendix 8 - Example of a full data flow mapping

1. The following pages contain an example of a full dataflow mapping, illustrating the full range of data recorded.

2. For each flow, basic information about the flow is given together with details of the specific data items which are exchanged as part of that flow.

**Example of detailed justification**

**Exemplar flow - 42: Contracting & Commissioning- APC General Episode**

| | | Purposes | | | | |
|---|---|---|---|---|---|---|
| Patient-identifiable data item[9] | | Health needs assessment incl. small area statistics | Health outcome monitoring | Strategic development | Performance management and contracting | HES reporting (documented as separate flow no. 44) |
| Internal ref. number | Description | | | | | |
| 300 | Address | | ✓ | | ✓ | |
| 2 | Date of Birth | ✓ | ✓ | ✓ | ✓ | ✓ |
| 244 | Ethnic Origin | ✓ | ✓ | ✓ | ✓ | |
| 53 | HA of residence | | | ✓ | ✓ | |
| 1 | Name | | ✓ | | ✓ | |
| 3 | NHS Number | | ✓ | | ✓ | |
| 302 | Postcode | ✓ | ✓ | ✓ | ✓ | ✓ |
| 8 | Sex | ✓ | ✓ | ✓ | | ✓ |

[9] See Appendix 7 for details of patient-identifiable data items

Insert Table here

Insert Table here

# Appendix 9 - List of organisations invited to contribute to the review

1. The work of the Committee was carried out in an open and consultative way. The Committee wrote to a large number of organisations seeking views and information, and subsequently the Committee engaged a range of key organisations in more detailed consideration of the emerging findings and recommendations.

2. Working Group members also consulted widely with their peers and with those involved in day to day use of patient information.

Academy of Medical Royal Colleges and their Faculties in the UK
- Information Group
Royal College of General Practitioners
Royal College of Physicians
Royal College of Pathologists
Royal College of Radiologists
Royal College of Anaesthetists
Royal College of Obstetricians & Gynaecologists
Faculty of Public Health Medicine of the Royal College of Physicians of the UK
Royal College of Psychiatrists
Royal College of Surgeons
Royal College of Ophthalmologists
Royal College of Midwives
Royal College of Nursing of the UK
Royal College of Paediatrics and Child Health
College of Speech and Language Therapists
Standing Medical Advisory Committee
Joint Consultants Committee
Medical Protection Society
Medical Defence Union
General Medical Council
The General Dental Council
General Optical Council
The General Council and Register of Osteopaths
United Kingdom Central Council for Nursing, Midwifery & Health Visiting
English National Board for Nursing, Midwifery & Health Visiting
Medical Research Council
British Medical Association
British Dental Association
Health Visitors Association
National Association of Health Authorities and Trusts
Hospital Consultants and Specialists Association
British Association of Occupational Therapists
The Chartered Society of Physiotherapy

Association of Optometrists
The Society of Chiropodists & Podiatrists
Royal Pharmaceutical Society of Great Britain
The British Psychological Society
The Association of the British Pharmaceutical Industry
Public Health Laboratory Service
Centre for Health Informatics (University of Wales)
IMS International Ltd
Advanced Medical Communications
Data Protection Registrar
The Law Society
Association of Community Health Councils for England and Wales
Local Government Management Board
The Health Service Commissioner
Law Commissioner
Scottish Consumer Council
Patient's Association
MENCAP
Action for Victims of Medical Accidents
Association of Medical Research Charities
Brook Advisory Centres
National Council for Civil Liberties
Campaign for Freedom of Information
Guild of Editors
National Consumer Council
Consumers Association
Help for Health
Long Term Medical Conditions Alliance
Terence Higgins Trust
Patient's Forum
Royal National Institute for Deaf People
British Association of Cancer United Patients
MIND
Royal National Institute for the Blind
National Eczema Society
British Heart Foundation
Public Health Alliance
Scottish Association of Health Councils
British Association of Medical Managers
Institute of Health Service Managers
Association of Managers in General Practice
Clinical Systems Group

# Appendix 10 - Informing patients

1. The Department of Health guidelines *"The Protection and Use of Patient Information"* provided a sample notice for informing patients of the use to which this information might be put.

## MODEL NOTICE FOR PATIENTS

We *ask* you for information so that you can receive proper care and treatment.

We *keep* this information, together with details of your care, because it may be needed if we see you again.

We *may use* some of this information for other reasons: for example, to help us protect the health of the public generally and to see that the NHS runs efficiently, plans for the future, trains its staff, pays its bills and can account for its actions. Information may also be needed to help educate tomorrow's clinical staff and to carry out medical and other health research for the benefit of everyone.

Sometimes the law requires us to *pass on* information: for example, to notify a birth.

The NHS Central Register for England & Wales contains basic personal details of all patients registered with a general practitioner. The Register does not contain clinical information.

**You have a right of access to your health records**

**EVERYONE WORKING FOR THE NHS HAS A LEGAL DUTY TO KEEP INFORMATION ABOUT YOU CONFIDENTIAL.**

**You may be receiving care from other people as well as the NHS. So that we can all work together for your benefit we may need to share some information about you.**

**We only ever use or pass on information about you if people have a genuine need for it in your and everyone's interests. Whenever we can we shall remove details which identify you. The sharing of some types of very sensitive personal information is strictly controlled by law.**

**Anyone who receives information from us is also under a legal duty to keep it confidential.**

## THE MAIN REASONS FOR WHICH YOUR INFORMATION MAY BE NEEDED ARE:

- **giving you health care and treatment**
- **looking after the health of the general public**
- **managing and planning the NHS.** For example:
- making sure that our services can meet patient needs in the future
- paying your doctor, nurse, dentist, or other staff, and the hospital which treats you for the care they provide
- auditing accounts
- preparing statistics on NHS performance and activity (where steps will be taken to ensure you cannot be identified)
- investigating complaints or legal claims
- **helping staff to review the care they provide to make sure it is of the highest standard**
- **training and educating staff** (but you can choose whether or not to be involved personally)
- **research** approved by the Local Research Ethics Committee. (If anything to do with the research would involve you personally, you will be contacted to see if you are willing )

**If you agree, your relatives, friends and carers will be kept up to date with the progress of your treatment.**

***If at anytime you would like to know more about how we use your information you can speak to the person in charge of your care or to ......***

2. Local NHS bodies were asked to adapt this notice to suit local circumstances. The following sample leaflet is based upon a leaflet produced by the Fisher Medical Centre, Skipton, which the Committee considered to be an excellent example of a local initiative.

**PRIVACY AND CONFIDENTIALITY OF YOUR MEDICAL RECORDS**

Your medical record is a life-long history of your consultations, illnesses, investigations, prescriptions and other treatments. The doctor-patient relationship sits at the heart of good general practice and is based on mutual trust and confidence. The story of that relationship over the years is your medical record.

Your GP is responsible for the accuracy and safe-keeping of your medical records. You can help us to keep it accurate by informing us of any change in your name, address, marital status and by ensuring that we have full details of your important medical history.

If you move to another area or change GP, we will send your medical records to the local Health Authority to be passed on to your new practice. However, we will keep a copy of all entries into your records whilst you were registered with us.

**YOUR RIGHT TO PRIVACY**

You have a right to keep your personal health information confidential between you and your doctor. This applies to everyone over the age of 16 years and in certain cases to those under sixteen. The law does impose a few exceptions to this rule, but apart from those (listed in detail below), you have a right to know who has access to your medical record.

**WHO ELSE SEES MY RECORDS?**

There is a balance between your privacy and safety, and we will normally share some information about you with others involved in your health care, unless you ask us not to. This could include doctors, nurses, therapists and technicians involved in the treatment or investigation of your medical problems.

[This practice is involved in the teaching of medical students and the training in General Practice of young doctors. If you see a medical student or GP trainee during a consultation, they may be given supervised access to your medical record.]

Our practice nurses, district nurses, midwives and health visitors all have access to the medical records of their patients. It is our policy to try to have a single medical and nursing record for each patient. We firmly believe that this offers the best opportunity for delivering the highest quality of care from a modern primary care team.

Our practice staff have limited access to medical records. They need to notify the health authority of registration and claim details and perform various filing tasks on the medical records.

All our doctors, nurses and staff have a legal, ethical [and contractual] duty to protect your privacy and confidentiality.

**WHERE ELSE DO WE SEND PATIENT INFORMATION**

We are required by law to notify the Government of certain infectious diseases (e.g. meningitis, measles but *not* AIDS) for public health reasons.

The law courts can also insist that GPs disclose medical records to them. Doctors cannot refuse to cooperate with the court without risking serious punishment. We are often asked for medical reports from solicitors. These will *always* be accompanied by the patient's signed consent for us to disclose information. We will not normally release details about other people that are contained in your records (e.g. wife, children, parents etc) unless we also have their consent.

Limited information is shared with health authorities to help them organise national programmes for public health such as childhood immunisations, cervical smear tests and breast screening.

GPs must keep the health authorities up to date with all registration changes, additions and deletions. We also notify the health authority of certain procedures that we carry out on patients (contraceptive and maternity services, minor operations, night visits, booster vaccinations) and other "item-of-service" procedures, where we are paid for performing these procedures.

Social Services, the Benefits Agency and others may require medical reports on you from time to time. These will often be accompanied by your signed consent to disclose information. Failure to cooperate with these agencies can lead to patients' loss of benefit or other support. However, if we have not received your signed consent we will not normally disclose information about you.

Life Assurance companies frequently ask for medical reports on prospective clients from the GP. These are *always* accompanied by your signed consent form. GPs must disclose *all relevant medical conditions* unless you ask us not to do so. In that case, we would have to inform the insurance company that you have instructed us *not to make a full disclosure* to them. You have the right, should you request it, to see reports to insurance companies or employers before they are sent.

**HOW CAN I FIND OUT WHAT'S IN MY MEDICAL RECORDS**

We are required by law to allow you access to your medical records. If you wish to see your records, please contact [the practice manager] for further advice. All requests to view medical records should  be made in writing to the surgery. We are allowed by law to charge a small fee to cover our administration and costs.

We have a duty to keep your medical records accurate and up to date. Please feel free to correct any errors of fact which may have crept into your medical records over the years.

**WHAT WE WILL NOT DO**

To protect your privacy and confidentiality, we will not normally disclose any medical information over the telephone or fax unless we are sure that we are talking to you. This means that we will not disclose information to your family, friends, colleagues about any medical matters at all, unless we know that we have your consent to do so.

This also means that we will not normally disclose test results over the phone and may wish to call you back to ensure that we are talking to the right person.

Our staff will not disclose any details *at all* about patients over the telephone. Please do not ask them to - they are instructed to protect your privacy above all else!

Finally, if you have any further queries, comments or complaints about privacy and your medical records, then please contact [the practice manager] or talk to your own GP.

# Appendix 11 - Sample protocol

## SAMPLE FRAMEWORK FOR THE SHARING OF PERSONAL INFORMATION BETWEEN NHS AND NON-NHS BODIES THROUGH ORAL REPORTS, WRITTEN RECORDS AND COMPUTER SYSTEMS

### 1. Outline

1.1 This framework document contains six sections:

- Objectives of a locally agreed protocol
- General Principles governing the sharing of personal information
- Setting Parameters for sharing personal information
- Defining Purposes for which personal information is required
- Holding personal information, access and security
- Ownership of information and the rights of individuals

### 2. Objectives

2.1 To set parameters for the sharing of information between agencies which contribute to the health or social care of an individual.

2.2 To define the purposes for holding personal information within each agency.

2.3 To define how personal information should be held within each agency and who should have access to this information.

2.4 To define which information is designated as health services information and which is designated as social services information and to specify the rights of access to each for individuals as required by legislation.

### 3. General Principles

3.1 Whilst it is vital for the proper care of individuals that those concerned with that care have ready access to the information that they need, it is also important that service users and their carers can trust that personal information will be kept confidential and that their privacy is respected.

3.2 All staff have an obligation to safeguard the confidentiality of personal information. This is governed by law, their contracts of employment, and in many cases by professional codes of conduct. All staff should be made aware that breach of confidentiality could be a matter for disciplinary action and provides grounds for complaint against them.

3.3 Although it is neither practicable nor necessary to seek an individual's specific consent each time that information needs to be passed on for a particular purpose **that has been defined within this protocol**, this is contingent on individuals having been fully informed of the uses to which information about them may be put. All agencies concerned with the care of individuals should satisfy themselves that this requirement is met.

3.4 Clarity about the purposes to which personal information is to be put is essential, and only the minimum identifiable information necessary to satisfy that purpose should be made available. Access to personal information should be on a strict **need to know** basis.

3.5 If an individual wants information about themselves to be withheld from someone, or some agency, which might otherwise have received it, the individual's wishes should be respected unless there are exceptional circumstances. Every effort should be made to explain to the individual the consequences for care and planning, but the final decision should rest with the individual.

3.6 The exceptional circumstances which override an individual's wishes arise when the information is required by statute or court order, where there is a serious public health risk or risk of harm to other individuals, or for the prevention, detection or prosecution of *serious* crime. The decision to release information in these circumstances, where judgement is required, should be made by a nominated senior professional within the agency, and it may be necessary to take legal or other specialist advice.

3.7 There are also some statutory restrictions on the disclosure of information relating to HIV and AIDS, other sexually transmitted diseases, assisted conception and abortion.

3.8 Where information on individuals has been aggregated or anonymised, it should still only be used for justified purposes, but is not governed by this protocol. Care should be taken to ensure that individuals cannot be identified from this type of information, as it is frequently possible to identify individuals from limited data e.g. age and post code may be sufficient.

## 4. **Setting Parameters**

4.1 There should be a nominated senior professional, within each agency covered by this protocol, responsible for agreeing amendments to the protocol, monitoring its operation, and ensuring compliance.

4.2 Personal information should be transferred freely between the agencies who have agreed and are complying with this protocol, for the purposes it defines. A regularly updated register of individuals who need access to personal information, and the defined purpose for which they need this access, shall be made available to each agency concerned.

4.3 If appropriate, service level agreements can be used to establish standards for sharing information, e.g. speed of response.

4.4 Specific consent is required prior to personal information being transferred for purposes other than those defined in this protocol, unless there are exceptional circumstances as outlined above.

4.5 Where individuals are unable to give consent, the decision should be made on the individual's behalf by those responsible for providing care, taking into account the views of patients and carers, with the individual's best interests being paramount. Where practicable, advice should be sought from the nominated senior professional and the reasons for the final decision should be clearly recorded.

## 5. Defining Purposes

5.1 There will be a range of justifiable purposes to be locally agreed. The following list is not exhaustive and covers internal NHS purposes only:

- delivering personal care and treatment
- assuring and improving the quality of care and treatment
- monitoring and protecting public health
- managing and planning services
- contracting for NHS services
- auditing NHS accounts and accounting for NHS performance
- risk management
- investigating complaints and notified or potential legal claims
- teaching
- statistical analysis
- medical or health services research

## 6. Holding information, access and security

6.1 Staff should only have access to personal information on a need-to-know basis, in order to perform their duties in connection with one or more of the purposes defined above. Clinical and professional details should be available to all those, but only those, involved in the care of the individual.

6.2 Each agency will ensure that they have mechanisms in place to enable them to address the issues of physical security, security awareness and training, security management, systems development, site specific information systems security policies, and systems specific security policies.

6.3 Each agency will take all reasonable care and safeguards to protect both the physical security of information technology and the data contained within it.

6.4 All information systems will be effectively password protected and users will not divulge their password nor leave systems active whilst absent.

6.5 All personal files and confidential information must be kept in secure, environmentally controlled locations when unattended, e.g. in locked storage cabinets, security protected computer systems etc.

6.6 Keys to lockable storage cabinets should be held only be staff who require regular access to the information they contain. Keys must be held in a secure place.

## 7. Ownership of information and the rights of individuals

7.1 Whilst written and computerised records will be regarded as shared between the agencies, an individual's right of access to the information contained in the records differs when it has been provided by a health professional from when it has been provided by Social Services staff.

7.2 Any health professional contribution to records maintained by Social Services staff, whether a letter, a case record or a report, must be clearly marked as such, and where practicable, kept in a closed part of the file. Social Services staff cannot grant access to this information without written authorization.

7.3 The reverse also applies. NHS staff cannot grant access to Social Services information without written authorization.

# Appendix 12 - Methodology for considering dataflows

1. The majority of data flows summarised in this report have been mapped in a detailed form which lists the data items included and provides a brief overview of purpose(s). However, the Multi-Agency Working Group developed a more complex form of data flow mapping to facilitate consideration of what information was required for each identified purpose. This was thought to be needed by the Working Group because some of the flows they considered were more complex than most.

2. Essentially this data mapping identifies in detail those data items in a flow which are used for each particular purpose. This analysis can be done at a number of levels, thus:

   - Table 1 looks at flows of information in a Child Protection case where the mother has mental health problems. Each broad purpose for which patient information is needed is displayed down one side of the table and each item of patient information required to satisfy that purpose can be seen at a glance.

   - Table 2 provides a more detailed analysis based on one service for elderly mentally ill people drawn from the Mental Health Minimum Data Set pilot work (see table 3 for a list of the data items in this Data Set). This table is too large to comfortably follow the format of this report and as printed it is three sheets wide by four high.

3. The Committee felt that its recommendations for the future critical examination of data flows would be usefully supported by this kind of detailed analysis and that it would prove particularly helpful to those charged with considering the justification for using patient information where flows are multi-directional and complex.

4. The Committee would like to thank Dr Gyles Glover, Senior Medical Officer with the Department of Health, for the detailed analysis drawn from his work on the Mental Health Minimum Data Set. Any questions about the detail of this work should be addressed to Dr Glover.

**Table 1: Business Process: Child Protection where Mother has Mental Health Problems**

| | **From:** Health Visitor, CPN Consultant Psychiatrist and GP, Nursing Staff, Midwife Consultant Obstetrician | **To:** Social Services, Housing Dept or Association Support Services, eg. Nursery or Drop in Centre, Voluntary Organisations, Police Probation Service, Coroner | **Child's Diagnosis** | **Child's and Mother's Address** | **Child's current name and Mothers current and previous names** | **Sex - Child's** | **Birth Date - Child's** | **Marital Status - Mother** | **Ethnic Group - Mother** | **Child's Health History** | **Child's previous name(s)** | **Ethnic Group - Child** | **Other family members - eg. father, mothers partner, siblings etc.** | **Previous history of mother's and/or child's contacts with health services** | **Professional opinion eg. of health visitor, CPN, Child Psychiatrist, GP** | **Name(s) of health worker's involved** | **Details of previous communications with mother/child** | **Details of professionals' observations of mother and child** | **Details of previous communications between professionals involved** | **Treatment regimes for mother/child and outcomes** | **Prognosis for mother/child** | **Housing Status** | **Home Conditions** | **Mother's and child's family and social history** | **Summary report of mother's condition and impact on child** | **Other household members** | **GP's Name** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **PURPOSE** | **COMMENT** | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | To assess the need for safe guarding the child's welfare | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | |
| 2 | To provide support for the mother | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | | |
| 3 | To improve physical conditions for both mother and child | | | 0 | | 0 | 0 | | | | | | | | | | | | | | | 0 | 0 | | 0 | | 0 |
| 4 | To ascertain whether a more formal assessment of the mother's mental health is necessary | | | 0 | 0 | 0 | 0 | 0 | 0 | | | | 0 | 0 | 0 | | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | 0 | |
| 5 | To safeguard the child and promote the child's health and development | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 |

## Table 1: Business Process: Child Protection where Mother has Mental Health Problems

| | **From:** Health Visitor, CPN Consultant Psychiatrist and GP, Nursing Staff, Midwife Consultant Obstetrician | **To:** Social Services, Housing Dept or Association Support Services, eg. Nursery or Drop in Centre, Voluntary Organisations, Police Probation Service, Coroner | **Child's Diagnosis** | **Child's and Mother's Address** | **Child's current name and Mothers current and previous names** | **Sex - Child's** | **Birth Date - Child's** | **Marital Status - Mother** | **Ethnic Group - Mother** | **Child's Health History** | **Child's previous name(s)** | **Ethnic Group - Child** | **Other family members - eg. father, mothers partner, siblings etc.** | **Previous history of mother's and/or child's contacts with health services** | **Professional opinion eg. of health visitor, CPN, Child Psychiatrist, GP** | **Name(s) of health worker's involved** | **Details of previous communications with mother/child** | **Details of professionals' observations of mother and child** | **Details of previous communications between professionals involved** | **Treatment regimes for mother/child and outcomes** | **Prognosis for mother/child** | **Housing Status** | **Home Conditions** | **Mother's and child's family and social history** | **Summary report of mother's condition and impact on child** | **Other household members** | **GP's Name** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **PURPOSE** | **COMMENT** | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | To monitor child's welfare and monitor mother's health state, and to provide continuing support | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | 0 |
| 7 | To request, provide and monitor direct support services and their effectiveness eg. day nursery | | | 0 | 0 | 0 | 0 | 0 | 0 | | | 0 | | | 0 | | | | | | | | 0 | | 0 | | 0 |
| 8 | To review the management of the case by the various agencies and to learn lessons for improving service delivery for the future where there has been the death of a child on the child protection register | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Table 2**

| ITEM | COMMENTS | PATIENT: | Sex | Birth Date | Marital status | Ethnic group | Year of first psychiatric care | Local patient ID | NHS number | ADMINISTRATIVE: | Health authority | Electoral ward | GP practice number | GPFH code | GP referral number | Contract identifier | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | | * | * | | * | * | * | * | | * | * | * | * | * | * | |
| DH | | | * | * | | * | * | | * | | * | * | | | | | |
| | | | | | | | | | | | | | | | | | |
| 1 Documenting care | | | | | | | | | | | | | | | | | |
| 1.1 Commissioning currencies: | | | | | | | | | | | | | | | | | |
| Finished Consultant Episodes (FCEs) | From HES data | | | | | | | | | | | | | | | | |
| Contacts with staff | | | | | | | | | | | | | | | | | |
| Patient-days on caseload – | | | | | | | | | | | | | | | | | |
| - by severity | | | 1 | 1 | | | 1 | | | | 1 | | | 1 | 1 | | |
| - by level of input,eg CPA level | | | 1 | 1 | | | | | | | 1 | | | 1 | 1 | | |
| | | | | | | | | | | | | | | | | | |
| 1.2 Current policy concerns: | | | | | | | | | | | | | | | | | |
| Person days care on Supervision Register | | | 1 | 1 | | 1 | | | | | | | | | | | |
| Proportion of patients covered by CPA | | | 1 | 1 | | | | | | | | | | | | | |
| Proportion of care of MDOs under ECR | From HES locally | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 1.3 Issues of public concern: | | | | | | | | | | | | | | | | | |
| Episodes of compulsory detention, Rx, supervision | Supplements HES data | | 1 | 1 | | 1 | | | | | 1 | 1 | | | | | |
| Amount and distrib of contentious treatments (eg ECT) | | | 1 | 1 | | | | | | | 1 | | | | | | |

**Table 2**

| ITEM | MENTAL HEALTH CARE SPELL: | Specialty code | Start date | Referral code | End date | End code | Spell days in period | Suspended days in period | Days of minimal CPA | Days more complex CPA | Days full multidisciplinary CPA | CPA at end of period | Occupation code of key worker | Last saw key worker | Days on Supervision Register | Supervision Register at end of period | Days liable for detention | Days Supervised Discharge | Legal status at end of period | Most restrictive in period | Care without consent | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | |
| DH | * | * | * | * | * | * | * | * | * | * | * | * | * | | * | * | * | * | * | * | * | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 1 Documenting care | | | | | | | | | | | | | | | | | | | | | | |
| 1.1 Commissioning currencies: | | | | | | | | | | | | | | | | | | | | | | |
| Finished Consultant Episodes (FCEs) | | | | | | | | | | | | | | | | | | | | | | |
| Contacts with staff | | | | | | | | | | | | | | | | | | | | | | |
| Patient-days on caseload – | | | | | | | | | | | | | | | | | | | | | | |
| - by severity | | | 1 | | 1 | | 1 | | | | | | | | | | | | | | | |
| - by level of input,eg CPA level | | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 1.2 Current policy concerns: | | | | | | | | | | | | | | | | | | | | | | |
| Person days care on Supervision Register | | | | | | | 1 | | | | | | | | 1 | 1 | | | | | | |
| Proportion of patients covered by CPA | | | | | | | 1 | | 1 | 1 | 1 | 1 | | | | | | | | | | |
| Proportion of care of MDOs under ECR | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 1.3 Issues of public concern: | | | | | | | | | | | | | | | | | | | | | | |
| Episodes of compulsory detention, Rx, supervision | | | | | | | 1 | | | | | | | | | | 1 | 1 | 1 | 1 | 1 | |
| Amount and distrib of contentious treatments (eg ECT) | | 1 | | | | | | | | | | | | | | | | | | | 1 | |

## Table 2

| ITEM | ASSESSMENT: | Diagnosis | First HoNOS | Latest HoNOS | Best HoNOS in period | Worst HoNOS | MENTAL HEALTH CARE PACKAGE: | In-patient days | NHS Community bed days | Non NHS staffed residential care days | Other supported residential care days | Day hospital attendances | Day centre care | Sheltered work | OP attendances | CPN contacts | Clinical psychology contacts | OT contacts | SW contacts | Domiciliary Care | Mental health treatments | Administrations of ECT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER |  | * | * | * | * | * |  | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
| DH |  | * | * | * | * | * |  | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 Documenting care |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.1 Commissioning currencies: |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Finished Consultant Episodes (FCEs) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Contacts with staff |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 1 | 1 | 1 | 1 |  |  |  |  |
| Patient-days on caseload – |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| - by severity |  | 1 |  | 1 |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| - by level of input,eg CPA level |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 Current policy concerns: |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Person days care on Supervision Register |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Proportion of patients covered by CPA |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Proportion of care of MDOs under ECR |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.3 Issues of public concern: |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Episodes of compulsory detention, Rx, supervision |  | 1 | 1 | 1 |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Amount and distrib of contentious treatments (eg ECT) |  | 1 | 1 | 1 |  | 1 |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  | 1 | 1 |

Uses of the Mental Minimum data set

**Table 2**

| ITEM | COMMENTS | PATIENT: | Sex | Birth Date | Marital status | Ethnic group | Year of first psychiatric care | Local patient ID | NHS number | ADMINISTRATIVE: | Health authority | Electoral ward | GP practice number | GPFH code | GP referral number | Contract identifier | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | | * | * | | * | * | * | * | | * | * | * | * | * | * | |
| DH | | | * | * | | * | * | | * | | * | * | | | | | |
| 2 Assessing care | | | | | | | | | | | | | | | | | |
| 2.1 Access and gatekeeping: | | | | | | | | | | | | | | | | | |
| Ratios and population based rates of patients | | | | | | | | | | | | | | | | | |
| - Assessed /taken on for treatment | | | | | | | | | | | | | | | | | |
| - Clinic visits only/domiciliary care/day care | | | | | | | | | | | | | | | | | |
| - Ambulatory only/in-patient/supp res care | | | | | | | | | | | | | | | | | |
| - Short term interventions/indefinite duration | | | | | | | | | | | | | | | | | |
| Nature/severity of clin probs at each level | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 2.2 Distribution of care resources: | | | | | | | | | | | | | | | | | |
| 2.2.1 Between geographic or GP based sectors: | | | | | | | | | | | | | | | | | |
| Allocation of resources | | | | | | | | | | | | | | | | | |
| - CPNs | | | 1 | 1 | | | 1 | | | | 1 | 1 | | | | | |
| - Observed bed and day hospital use | | | 1 | 1 | | | 1 | | | | 1 | 1 | | | | | |
| Compared with caseload size/severity and MINI score | MINI scores for | | | | | | | | | | | | | | | | |
| | geographic areas | | | | | | | | | | | | | | | | |
| 2.2.2 Between patient within a sector: | | | | | | | | | | | | | | | | | |
| Caseload size/composition vs staff skills/experience | | | 1 | 1 | | 1 | 1 | | | | 1 | 1 | | | | | |
| Use of day care/sup. housing vs pts illness etc | | | 1 | 1 | | 1 | 1 | | | | 1 | 1 | | | | | |

**Table 2**

| ITEM | MENTAL HEALTH CARE SPELL: | Specialty code | Start date | Referral code | End date | End code | Spell days in period | Suspended days in period | Days of minimal CPA | Days more complex CPA | Days full multidisciplinary CPA | CPA at end of period | Occupation code of key worker | Last saw key worker | Days on Supervision Register | Supervision Register at end of period | Days liable for detention | Days Supervised Discharge | Legal status at end of period | Most restrictive in period | Care without consent | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | |
| DH | | * | * | * | * | * | * | * | * | * | * | * | * | | * | * | * | * | * | * | * | |
| 2 Assessing care | | | | | | | | | | | | | | | | | | | | | | |
| 2.1 Access and gatekeeping: | | | | | | | | | | | | | | | | | | | | | | |
| Ratios and population based rates of patients | | | | | | | | | | | | | | | | | | | | | | |
| - Assessed /taken on for treatment | | 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | |
| - Clinic visits only/domiciliary care/day care | | 1 | | | | | 1 | | | | | | | | | | | | | | | |
| - Ambulatory only/in-patient/supp res care | | 1 | | | | | 1 | | | | | | | | | | | | | | | |
| - Short term interventions/indefinite duration | | 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | |
| Nature/severity of clin probs at each level | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.2 Distribution of care resources: | | | | | | | | | | | | | | | | | | | | | | |
| 2.2.1 Between geographic or GP based sectors: | | | | | | | | | | | | | | | | | | | | | | |
| Allocation of resources | | | | | | | | | | | | | | | | | | | | | | |
| - CPNs | | | | | | | 1 | | 1 | 1 | 1 | | 1 | | | | | | | | | |
| - Observed bed and day hospital use | | | | | | | 1 | | 1 | 1 | 1 | | 1 | | | | | | | | | |
| Compared with caseload size/severity and MINI score | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.2.2 Between patient within a sector: | | | | | | | | | | | | | | | | | | | | | | |
| Caseload size/composition vs staff skills/experience | | 1 | | | | | 1 | | | | | | 1 | | 1 | | | 1 | | 1 | 1 | |
| Use of day care/sup. housing vs pts illness etc | | 1 | | | | | 1 | | | 1 | 1 | 1 | | | | | | | | | | |

**Table 2**

| ITEM | ASSESSMENT: | Diagnosis | First HoNOS | Latest HoNOS | Best HoNOS in period | Worst HoNOS | MENTAL HEALTH CARE PACKAGE: | In-patient days | NHS Community bed days | Non NHS staffed residential care days | Other supported residential care days | Day hospital attendances | Day centre care | Sheltered work | OP attendances | CPN contacts | Clinical psychology contacts | OT contacts | SW contacts | Domiciliary Care | Mental health treatments | Administrations of ECT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | * | * | * | * | * | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
| DH | | * | * | * | * | * | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
| 2 Assessing care | | | | | | | | | | | | | | | | | | | | | | |
| 2.1 Access and gatekeeping: | | | | | | | | | | | | | | | | | | | | | | |
| Ratios and population based rates of patients | | | | | | | | | | | | | | | | | | | | | | |
| - Assessed /taken on for treatment | | 1 | 1 | 1 | | 1 | | 1 | 1 | | | 1 | | | 1 | 1 | 1 | 1 | | | | |
| - Clinic visits only/domiciliary care/day care | | 1 | 1 | 1 | | 1 | | 1 | 1 | | | 1 | | | 1 | 1 | 1 | 1 | | | | |
| - Ambulatory only/in-patient/supp res care | | 1 | 1 | 1 | | 1 | | 1 | 1 | | | 1 | | | 1 | 1 | 1 | 1 | | | | |
| - Short term interventions/indefinite duration | | 1 | 1 | 1 | | 1 | | 1 | 1 | | | 1 | | | 1 | 1 | 1 | 1 | | | | |
| Nature/severity of clin probs at each level | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.2 Distribution of care resources: | | | | | | | | | | | | | | | | | | | | | | |
| 2.2.1 Between geographic or GP based sectors: | | | | | | | | | | | | | | | | | | | | | | |
| Allocation of resources | | | | | | | | | | | | | | | | | | | | | | |
| - CPNs | | 1 | | 1 | | 1 | | | | | | | | | | 1 | 1 | | | | | |
| - Observed bed and day hospital use | | 1 | | 1 | | 1 | | 1 | | | | 1 | | | | | | | | | | |
| Compared with caseload size/severity and MINI score | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.2.2 Between patient within a sector: | | | | | | | | | | | | | | | | | | | | | | |
| Caseload size/composition vs staff skills/experience | | 1 | 1 | 1 | | 1 | | | | | | | | | | | | | | | | |
| Use of day care/sup. housing vs pts illness etc | | 1 | 1 | 1 | | 1 | | | 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | |

**Table 2**

| ITEM | COMMENTS | PATIENT: | Sex | Birth Date | Marital status | Ethnic group | Year of first psychiatric care | Local patient ID | NHS number | ADMINISTRATIVE: | Health authority | Electoral ward | GP practice number | GPFH code | GP referral number | Contract identifier | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | | * | * | | * | * | * | * | | * | * | * | * | * | * | |
| DH | | | * | * | | * | * | | * | | * | * | | | | | |
| 2.2.3 Over time: | | | | | | | | | | | | | | | | | |
| By diagnosis and sector: | | | | | | | | | | | | | | | | | |
| - Duration/session nos of OP/DP/domicil Rx | | | 1 | 1 | | | | 1 | 1 | | | 1 | 1 | | | | |
| - Stay lengths in hospital | Derived from HES | | | | | | | | | | | | | | | | |
| - Internal 'queues', (eg bed blocking) | Not currently supported | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 2.3 Outcome | | | | | | | | | | | | | | | | | |
| 2.3.1 'Administrative' | | | | | | | | | | | | | | | | | |
| Hospital readmission curves (vs stay length) | | | | | | | | | | | | | | | | | |
| - By diagnosis and sector | Derived from HES | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 2.3.2'Clinical' | | | | | | | | | | | | | | | | | |
| HoNOS scores by diagnosis: | | | | | | | | | | | | | | | | | |
| - Short term: start comp to finish | | | 1 | 1 | | | 1 | 1 | 1 | | 1 | 1 | 1 | | | | |
| - Long term: best in year to prev year best | | | 1 | 1 | | | 1 | 1 | 1 | | 1 | 1 | 1 | | | | |

**Table 2**

| ITEM | MENTAL HEALTH CARE SPELL: | Specialty code | Start date | Referral code | End date | End code | Spell days in period | Suspended days in period | Days of minimal CPA | Days more complex CPA | Days full multidisciplinary CPA | CPA at end of period | Occupation code of key worker | Last saw key worker | Days on Supervision Register | Supervision Register at end of period | Days liable for detention | Days Supervised Discharge | Legal status at end of period | Most restrictive in period | Care without consent | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | |
| DH | | * | * | * | * | * | * | * | * | * | * | * | * | | * | * | * | * | * | * | * | |
| 2.2.3 Over time: | | | | | | | | | | | | | | | | | | | | | | |
| By diagnosis and sector: | | | | | | | | | | | | | | | | | | | | | | |
| - Duration/session nos of OP/DP/domicil Rx | | | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | |
| - Stay lengths in hospital | | | | | | | | | | | | | | | | | | | | | | |
| - Internal ‘queues’, (eg bed blocking) | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.3 Outcome | | | | | | | | | | | | | | | | | | | | | | |
| 2.3.1 ‘Administrative’ | | | | | | | | | | | | | | | | | | | | | | |
| Hospital readmission curves (vs stay length) | | | | | | | | | | | | | | | | | | | | | | |
| - By diagnosis and sector | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.3.2‘Clinical’ | | | | | | | | | | | | | | | | | | | | | | |
| HoNOS scores by diagnosis: | | | | | | | | | | | | | | | | | | | | | | |
| - Short term: start comp to finish | | | 1 | | 1 | 1 | | | | | | | | | | | | | | 1 | | |
| - Long term: best in year to prev year best | | | 1 | | 1 | | | | | | | | | | | | | | | 1 | | |

**Table 2**

| ITEM | ASSESSMENT: | Diagnosis | First HoNOS | Latest HoNOS | Best HoNOS in period | Worst HoNOS | MENTAL HEALTH CARE PACKAGE: | In-patient days | NHS Community bed days | Non NHS staffed residential care days | Other supported residential care days | Day hospital attendances | Day centre care | Sheltered work | OP attendances | CPN contacts | Clinical psychology contacts | OT contacts | SW contacts | Domiciliary Care | Mental health treatments | Administrations of ECT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | * | * | * | * | * | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
| DH | | * | * | * | * | * | | * | * | * | * | * | * | | * | * | * | * | * | * | * | * |
| 2.2.3 Over time: | | | | | | | | | | | | | | | | | | | | | | |
| By diagnosis and sector: | | | | | | | | | | | | | | | | | | | | | | |
| - Duration/session nos of OP/DP/domicil Rx | | 1 | 1 | 1 | | 1 | | | | | | 1 | | | 1 | 1 | 1 | 1 | | 1 | | |
| - Stay lengths in hospital | | | | | | | | | | | | | | | | | | | | | | |
| - Internal ‘queues’, (eg bed blocking) | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.3 Outcome | | | | | | | | | | | | | | | | | | | | | | |
| 2.3.1 ‘Administrative’ | | | | | | | | | | | | | | | | | | | | | | |
| Hospital readmission curves (vs stay length) | | | | | | | | | | | | | | | | | | | | | | |
| - By diagnosis and sector | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 2.3.2‘Clinical’ | | | | | | | | | | | | | | | | | | | | | | |
| HoNOS scores by diagnosis: | | | | | | | | | | | | | | | | | | | | | | |
| - Short term: start comp to finish | | 1 | 1 | 1 | | | | | | | | | | | | | | | | | | |
| - Long term: best in year to prev year best | | 1 | | | 1 | | | | | | | | | | | | | | | | | |

**Table 2**

| ITEM | COMMENTS | PATIENT: | Sex | Birth Date | Marital status | Ethnic group | Year of first psychiatric care | Local patient ID | NHS number | ADMINISTRATIVE: | Health authority | Electoral ward | GP practice number | GPFH code | GP referral number | Contract identifier | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | | * | * | | * | * | * | * | | * | * | * | * | * | * | |
| DH | | | * | * | | * | * | | * | | * | * | | | | | |
| 2.3.4 Quality of care | | | | | | | | | | | | | | | | | |
| CPN caseload sizes | Numerator only from MHDMS | | 1 | 1 | | | | | | | | | | | | | |
| Proportion of patients seen within last month | | | 1 | 1 | | | | | | | 1 | 1 | | | | | |
| Proportion seen within week of hosp disch | Not supported | | | | | | | | | | | | | | | | |
| Proportion lost to follow up | | | 1 | 1 | | 1 | | | | | 1 | 1 | | | | | |
| Proportions of compulsory admissions on S4 | From HES | | | | | | | | | | | | | | | | |
| Proportions of emergency sections converted | From KH? | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 3. Predicting care requirements | | | | | | | | | | | | | | | | | |
| 3.1 Planning changes in service configuration | | | | | | | | | | | | | | | | | |
| Use of resources by definable patient groups | | | 1 | 1 | | 1 | 1 | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 3.2 Anticipating trends from new Rx or demography | | | | | | | | | | | | | | | | | |
| Service consumption by specific ethnic groups | | | 1 | 1 | | 1 | 1 | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| 3.33 Resource allocation modelling | | | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |
| **Total uses:** | | | **19** | **19** | **1** | **8** | **10** | **3** | **3** | | **12** | **10** | **3** | **2** | **2** | **0** | |

Uses of the Mental Minimum data set

**Table 2**

| ITEM | MENTAL HEALTH CARE SPELL: | Specialty code | Start date | Referral code | End date | End code | Spell days in period | Suspended days in period | Days of minimal CPA | Days more complex CPA | Days full multidisciplinary CPA | CPA at end of period | Occupation code of key worker | Last saw key worker | Days on Supervision Register | Supervision Register at end of period | Days liable for detention | Days Supervised Discharge | Legal status at end of period | Most restrictive in period | Care without consent | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * | |
| DH | | * | * | * | * | * | * | * | * | * | * | * | * | | * | * | * | * | * | * | * | |
| 2.3.4 Quality of care | | | | | | | | | | | | | | | | | | | | | | |
| CPN caseload sizes | | | | | | | 1 | | | | | | | | | | | | | | | |
| Proportion of patients seen within last month | | | 1 | | 1 | 1 | | | | | | | 1 | 1 | | 1 | | | 1 | | | |
| Proportion seen within week of hosp disch | | | | | | | | | | | | | | | | | | | | | | |
| Proportion lost to follow up | | | | 1 | 1 | | 1 | | | | | | 1 | 1 | | 1 | | | 1 | | | |
| Proportions of compulsory admissions on S4 | | | | | | | | | | | | | | | | | | | | | | |
| Proportions of emergency sections converted | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 3. Predicting care requirements | | | | | | | | | | | | | | | | | | | | | | |
| 3.1 Planning changes in service configuration | | | | | | | | | | | | | | | | | | | | | | |
| Use of resources by definable patient groups | | | 1 | 1 | | | 1 | | 1 | 1 | 1 | | | | 1 | | 1 | 1 | 1 | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 3.2 Anticipating trends from new Rx or demography | | | | | | | | | | | | | | | | | | | | | | |
| Service consumption by specific ethnic groups | | | 1 | 1 | | | 1 | | 1 | 1 | 1 | | | | 1 | | 1 | 1 | 1 | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 3.33 Resource allocation modelling | | | 1 | 1 | | | 1 | | 1 | 1 | 1 | | | | 1 | | 1 | 1 | 1 | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| **Total uses:** | | **7** | **12** | **5** | **9** | **6** | **18** | **0** | **8** | **8** | **8** | **2** | **6** | **2** | **5** | **3** | **4** | **5** | **6** | **4** | **3** | |

**Table 2**

| ITEM | ASSESSMENT: | Diagnosis | First HoNOS | Latest HoNOS | Best HoNOS in period | Worst HoNOS | MENTAL HEALTH CARE PACKAGE: | In-patient days | NHS Community bed days | Non NHS staffed residential care days | Other supported residential care days | Day hospital attendances | Day centre care | Sheltered work | OP attendances | CPN contacts | Clinical psychology contacts | OT contacts | SW contacts | Domiciliary Care | Mental health treatments | Administrations of ECT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PURCHASER | | * | * | * | * | * | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
| DH | | * | * | * | * | * | | * | * | * | * | * | * | * | * | * | * | * | * | * | * | * |
| 2.3.4 Quality of care | | | | | | | | | | | | | | | | | | | | | | |
| CPN caseload sizes | | | | | | | | | | | | | | | | | | | | | | |
| Proportion of patients seen within last month | | | | | | | | | | | | | | | | | | | | | | |
| Proportion seen within week of hosp disch | | | | | | | | | | | | | | | | | | | | | | |
| Proportion lost to follow up | | | | | | | | | | | | | | | | | | | | | | |
| Proportions of compulsory admissions on S4 | | | | | | | | | | | | | | | | | | | | | | |
| Proportions of emergency sections converted | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 3. Predicting care requirements | | | | | | | | | | | | | | | | | | | | | | |
| 3.1 Planning changes in service configuration | | | | | | | | | | | | | | | | | | | | | | |
| Use of resources by definable patient groups | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 3.2 Anticipating trends from new Rx or demography | | | | | | | | | | | | | | | | | | | | | | |
| Service consumption by specific ethnic groups | | 1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 3.33 Resource allocation modelling | | 1 | | 1 | | 1 | | 1 | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| **Total uses:** | | **17** | **10** | **16** | **1** | **15** | | **9** | **8** | **4** | **4** | **10** | **4** | **4** | **9** | **10** | **10** | **9** | **3** | **4** | **1** | **1** |

**Table 3. The proposed Mental Health Minimum Data Set**

| **PATIENT:** | **ASSESSMENT:** |
|---|---|
| Sex<br>Birth date<br>Marital status<br>Ethnic group<br>Year of first psych care<br>Local patient ID<br>NHS number | Diagnosis<br>First HoNOS<br>Latest HoNOS<br>Best HoNOS in period<br>Worst HoNOS in period |
| **ADMINISTRATIVE:** | **MENTAL HEALTH CARE PACKAGE:** |
| Health authority<br>Electoral ward<br>GP practice number<br>GPFH code<br>GP ref number<br>Contract identifier | In-patient days<br>NHS community bed days<br>Non NHS staffed res days<br>Oth supported residential care days<br>Day hosp attendances<br>Day centre care<br>Sheltered work<br>OP attendances<br>CPN contacts<br>Clinical psychologist contacts<br>OT contacts<br>Domiciliary care<br>Mental health treatments<br>Administrations of ECT |
| **MENTAL HEALTH CARE SPELL:** | |
| Specialty code<br>Start date<br>Referral code<br>End date<br>End code<br>Spell days in period<br>Suspended days in period<br>Days of minimal CPA<br>Days more complex CPA<br>Days full multidisciplinary CPA<br>CPA at end of period<br>Occup of key worker<br>Last saw key worker<br>Days on Supervision Register<br>Supervision Register at end of Days detention<br>Days Supervised Discharge<br>Legal status at end of period<br>Most restrictive in period<br>Care without consent | |

Produced by Department of Health<br>11934 CA Q 1000 1P Dec 97 (CWP)<br>CHLORINE FREE PAPER