GUIDANCE ON
THE PROTECTION & USE OF CONFIDENTIAL HEALTH INFORMATION IN PRISONS AND INTER-AGENCY INFORMATION SHARING

Information and Practice 1/2002

CONTENTS

1. INTRODUCTION

This document is about the use and protection of confidential health information within the Prison Service and the effective sharing of information between the Prison Service and external agencies.

It draws on currently available guidance on the protection and use of confidential information and is within the framework of professional codes of conduct and current legal requirements.

Maintaining confidentiality is a key aspect of the clinician/patient relationship. When collecting, storing and using confidential health information it is important to adhere to explicit and transparent principles of good practice.

Disclosure of confidential information should normally only take place with the consent of the individual concerned. Individuals should be made aware of the uses to which their information will be put and with whom it will be shared.

Information can be shared without consent if it is required by statute or a court order. Disclosure without consent can also be made in exceptional circumstances if it is considered essential to protect the individual or anyone else from risk of death or serious harm, or for the prevention, detection or prosecution of serious crime. In such circumstances, the benefits of disclosing the information must be considered to outweigh the patient's or the public interest in keeping the information confidential.

Effective information sharing with other agencies, in particular the NHS, is a key aspect of enabling continuity of care for individuals as they pass from the community to prison and back again. Communication with the NHS may be necessary when prisoners first come into custody, when they leave prison and at various points during their sentence.

This document provides a framework for developing inter-agency information sharing. Local agreements or inter-agency information sharing protocols will be important in ensuring that boundary crossing processes work smoothly, are effectively managed and that patient and staff uncertainties about information sharing are reduced.

Overall, it is important for the Prison Service to use confidential health information fairly, lawfully and ethically within a robust and transparent framework.

2. CONFIDENTIALITY & CONSENT

2.1 Confidentiality

Confidentiality is a key part of the clinician/patient relationship. As well as legislation governing the protection and use of personal data, a common law duty of confidentiality applies.

Personal data which is subject to the common law duty of confidentiality has a number of characteristics:

- The information is not in the public domain or readily available from another source;
- The information is of a certain degree of sensitivity, such as medical data;
- The information has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given, or because the relationship between the recipient and the data subject gives rise to an expectation of confidentiality, as arises between a patient and doctor.

This duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to.

Whilst it is essential for the proper care of individuals that those concerned with their care have ready access to the information they need, it is also important that clients can trust that personal information will be kept confidential and their privacy respected. Without such assurances, patients may be unwilling to provide the information necessary to enable professionals to provide appropriate care and treatment.

All staff who handle, store or otherwise come across patient information should be made aware that they have a common law duty of confidentiality to patients and their employer.

The key principle to follow is that information provided in confidence should, in normal circumstances, only be disclosed with the consent of the individual concerned. This principle is not absolute; exceptions are dealt with in Section 2.3.

2.2 Consent

Health information is normally collected from patients in confidence, and the common law duty of confidence prohibits the use and disclosure of such information without consent.

Consent implies both choice and understanding. "Consent" given under duress or coercion is not, in fact consent. "Consent" given without a reasonable understanding of the purposes for which information is to be processed and of the type and purposes of disclosures envisaged is equally invalid.

Health care professionals must work on the presumption that every adult has the capacity to decide whether to consent to an action, unless it is shown that they cannot understand information presented in a clear way. If doctors need to assess a patient's capacity to consent, they should consult the available guidance (for example, the BMA Law Society publication 'Assessment of Mental Capacity: Guidance for Doctors and Lawyers).

In circumstances where it is clear that an individual has been given sufficient information to make an informed decision about whether or not to consent, consent can sometimes be implied, for example when sharing information within the health care team.

There is some confusion regarding the concept of consent and there is no clear legal definition. Consent may be either express (i.e. explicit) or implied. The Department of Health offers the following definitions of consent:

Consent: Agreement, by someone with the capacity to make a valid decision, either express or implied, to an action based on knowledge of what the action involves, its likely consequences and the option of saying no.

Express Consent: Consent which is expressed verbally or in writing (except where patients cannot write or speak, when other forms of communication may suffice).

Implied Consent: Consent which is inferred from a person's conduct in the light of facts and matters which they are aware of, or ought reasonably to be aware of, including the option of saying no. For example, a patient visiting a GP for treatment may be taken to imply consent to the GP consulting his/her medical records to assist diagnosis or prescription.

2.3 Disclosing Information without Consent

There are circumstances in which information may be disclosed without consent.

Exceptional circumstances which override an individual's wishes arise when the information is required by statute or court order, where disclosure is essential to protect the patient, or someone else from risk of death or serious harm, or for the prevention, detection or prosecution of serious crime. The decision to release information in these circumstances should be made by a nominated senior professional and it may be necessary to take legal or other specialist advice.

Where consent to the release of information is withheld, or if a patient is not competent to give consent, personal information may still be disclosed in the public interest where the benefits of disclosure to an individual or society outweigh the patient's and public interest in keeping the information confidential. In such cases, the possible harm of disclosure should be weighed against the benefits which are likely to arise from the release of the information. Again, it may be necessary to take professional advice on such decisions. Ultimately, the 'public interest' is determined by the courts.

3. LEGAL REQUIREMENTS

3.1 Data Protection Act 1998

The key legislation governing the protection and use of identifiable patient information is the Data Protection Act 1998. The DPA is framed around eight 'Principles' which govern how we process personal data and seven rights for individuals in respect of personal data.

3.1.1 Personal and Sensitive Personal Data

'Personal data' means anything that relates to a living, identifiable individual and includes:

- Factual information
- Expressions of opinion
- Indications of intent

'Sensitive personal data' means anything that relates to an individual's:

- Ethnic origin
- Political opinions
- Religious or other beliefs
- Trade union membership
- Physical or mental health
- Sexual life

- Offences
- Criminal proceedings and sentencing

3.1.2 Principles

The Prison Service has a statutory obligation to process all personal data in accordance with the eight principles laid down in the Act. These are that personal data must be:

- processed (e.g. collected, held, disclosed) fairly and lawfully
- obtained and processed only for one or more specified and lawful purposes
- adequate, relevant and not excessive in relation to the specified purpose(s)
- accurate and kept up to date
- kept no longer than is necessary
- processed in accordance with the data subject's rights under the Act
- kept secure and protected against loss or damage
- adequately protected if transferred to countries outside the EU.

Processing of personal data must satisfy one of the conditions in schedule 2 of the Act. Sensitive personal data, e.g. health information, is further protected in that processing must also satisfy at least one of the conditions listed in schedule 3 of the Act (schedules 2 and 3 are reproduced in Appendix 1).

3.1.3 Rights

All individuals on whom personal data are held have seven statutory rights. These are:

- right of subject access
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- rights in relation to automated decision taking
- right to take action for compensation if the individual suffers damage by any contravention of the Act by the 'data controller'
- right to take action to rectify, block or destroy inaccurate data
- right to make a request to the Information Commissioner to assess if any provision of the Act has been contravened.

Under the right of subject access, individuals are allowed access to information held on them. However, the Data Protection (Subject Access Modification) (Health) Order 2000 provides an exemption from subject access rights where permitting access to the data would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person (which may include a health professional).

The Information Commissioner is an independent officer who reports directly to Parliament and provides guidance on general data/information handling practices. The main duties of the Information Commissioner are to:

- promote good practice by organisations in meeting the statutory requirements of the Data Protection Act
- provide information as to an individual's rights under the Act and investigate complaints
- enforce compliance.

Further guidance on the Data Protection Act 1998, and exemptions, can be found in PSO 9020 issued October 2001.

4. USE OF CONFIDENTIAL HEALTH INFORMATION IN PRISONS

4.1 Entering Prison

A discrete Inmate Medical Record must be created for every new prisoner on reception. Efforts should be made to merge this information with records from previous periods in custody.

Efforts should be made to request any information required from the prisoner's GP or other relevant service he/she has recently been in contact with. The prisoner's explicit consent should be obtained before doing this. In exceptional circumstances, information may be requested and disclosed without consent (see Section 2.3)

Delays in requesting or obtaining relevant information when people enter prison, or first present with a health problem, can result in inappropriate diagnoses or treatment.

4.2 Record Keeping and Management

Inmate Medical Records and other confidential health information should be stored and maintained in accordance with the guidance in PSO 9020. Files and records must be reviewed regularly and destroyed when no longer required.

Health professionals should be aware that prisoners have the right of access to their medical records under the Data Protection Act 1998. For further details on subject access rights see PSO 9020.

4.3 Retention Periods

Inmate Medical Records have different retention periods from other prison records. The periods of retention, in accordance with Health Service Circular 1998/217, and as set out in PSO 9020, are as follows:

Personal Health Records	10 years after conclusion of treatment or death.
Mental Disorder treated under The Mental Health Act 1983	20 years after treatment no longer necessary, or 8 years after patient's death if patient died while still receiving treatment.
Maternity Records	25 years.

4.4 Health Information Sharing within Prisons

Patients should be made aware that information about them will be shared within the health care team. From time to time it may also be necessary for information to be shared, with the consent of the individual concerned, with prison staff outside health care.

Mapping information flows within the organisation will be helpful in identifying types of information held, who has access, and the uses to which that information is routinely put. Access to personal information should be on a strictly need to know basis.

Clarity about the purpose 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 to those entitled to receive it.

4.5 Access to Health Records for Visiting Doctors

Inmate Medical Records should be made available to a visiting doctor on a confidential doctor to doctor basis. The Data Protection Act 1998 allows for the 'processing' (i.e. holding, storing or disclosing) of information by a health professional if it is **necessary** for medical purposes.

In the case of a visiting psychiatrist providing an opinion in relation to a possible admission to hospital under the Mental Health Act 1983, the right of access to the prisoner's Inmate Medical Record is specifically referred to in the Mental Health Act Code of Practice (paragraph 3.6b).

4.6 Reports to the Parole Board

The ability of the Local Review Committees and the Parole Board to offer relevant and adequately considered advice to the Secretary of State on the release of prisoners on parole is conditioned by the availability to them of a range of relevant, contemporaneous reports.

In all cases, medical reports will be a valuable contribution to the information on which the Committee and/or Board base their decision – in some cases the medical report will be crucial. For the most part the purpose of the report is an assessment, by the Committee/Board, of the degree of risk, if any, that would be taken were the prisoner to be released ahead of the completion of his sentence, account being taken of any remission which may have been earned.

It is ethically correct for a medical officer to provide a report containing relevant medical information on a prisoner to the Local Review Committee/Board providing the following considerations are observed:

- The prisoner should first be seen by the medical officer and advised that, for the purpose of consideration for parole, a medical report has been requested. For the most part, prisoners are likely to give their consent to this as they will see it to be in their best interest. If the prisoner withholds consent, the medical officer's report should say so and it must not contain any fact or opinion based upon information obtained by the medical officer in the course of his or her privileged doctor/patient relationship with the prisoner.

- In cases where consent is obtained, care must be taken to limit the report to medical fact or opinion which is relevant for the purposes noted above. A comprehensive history would rarely be relevant for these reports.

- Reports should not be accompanied by copies of, or extracts from, papers in the IMR. However, the inclusion of a document, such as a psychiatric report to court, which has been prepared outside the privileged doctor/patient relationship and in the prisoner's knowledge that the information on which it was based was sought for other than directly healthcare reasons, is permissible if, in the medical officer's view, its contents may be of assistance to the Parole Board.

4.7 Adjudication Proceedings

An adjudication panel is entitled to request relevant information from a prison medical officer and in response the prison medical officer may properly provide such information.

Medical reports to adjudication panels should only contain information relevant for the required purpose and not be excessive. Reports should be prepared on the basis of the medical officer's consultation with the prisoner at

the time of the adjudication and relate only to issues relevant for the required purpose.

As with disclosure of confidential information in any other circumstances, medical officers need to be aware of the potential consequences of a disclosure to the prisoner, via an adjudication, of any information or opinion which (in the opinion of the medical officer) would be likely to cause any harm to the prisoner or any other person. In such cases, medical officers must make the panel aware of their concerns and have their views recorded.

4.8 Prisoner Escort Records

PER forms should be completed as detailed in the PER handbook. Confidential health related information should be placed in a sealed envelope, marked “Medical in Confidence” and attached to the PER form. Confidential health information should not be recorded on the PER form itself without the consent of the individual concerned.

4.9 Legal Proceedings

Solicitors’ requests for copies of information contained within medical records should be accompanied by evidence of their client’s consent. Providing this is demonstrated, copies of records, or parts thereof, may be released under the terms of the Data Protection Act. Staff should be aware that a doctor or other senior health professional should first review the records to assess whether any information should be withheld. Staff may wish to seek advice from Information Management Section at Headquarters to assist them with their decision.

Where legal proceedings against the Home Office have begun, or are indicated, copies of Inmate Medical Records may be released to the Treasury Solicitors. The Data Protection Act 1998 part IV (exemptions) allows for disclosure of information under these circumstances. Section 35 (2) states that:

> Personal data are exempt from the non-disclosure provisions where the disclosure is necessary –
>
> (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
> (b) for the purpose of obtaining legal advice,
>
> or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

4.10 Deaths in Prison

Following a death in custody the Area Manager, as the Commissioning Agency (CA) into all deaths in custody, will commission an investigation. The investigation will be led by a Senior Investigating Officer (SIO) from outside the establishment; a health care professional will normally be appointed to assist the investigating team. In order to gain a full understanding the SIO must have full access to all material including medical records and reports. Investigating teams must treat all information in confidence.

In preparation for the inquest, the medical officer must assemble all health records (including dental records) into the IMR. The Coroner must be advised what documents exist and be provided with all documentation requested. A Coroner's Court is a court of record, therefore all data supplied must be both full and accurate.

Further details on action following deaths in prison can be found in PSO 2710 and PSO1301.

4.11 Release from Prison

Upon release from prison it is important that those people with continuing care needs have relevant information about them communicated to their GP or other agency with responsibility for their care. Failure to pass on such information could adversely affect continuity of care and may, particularly for those people with mental health problems, have serious consequences for the health or wellbeing of the individual or others.

The Health Care Standard for Prisoners states that prisons should have in place written and observed guidelines setting out the procedures for reception, transfer and release, including:

- Ensuring information on continuing care is conveyed to other establishments on transfer, to NHS hospitals for outpatient and inpatient appointments, and
- Information to ensure continuity of care is communicated, with the prisoner's consent, to a general practitioner and or other responsible community agencies on discharge.

The following section provides guidance on sharing information with other agencies which includes advice on establishing local arrangements and protocols.

5. INTER-AGENCY INFORMATION SHARING

At various points it will be necessary for prisons to share health information with, and obtain information from, other agencies for example GPs, NHS providers, social care agencies. In all cases, as with internal sharing of information, the information shared should be adequate for the intended purpose, but not be excessive.

Ideally, the sharing of information between agencies should be governed by locally agreed protocols which satisfy the requirements of law and clearly set out procedures for both disclosing and receiving information.

If an individual wants information about them to be withheld from an agency which might otherwise have expected to receive 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.
As outlined in section 2.3, there are exceptional circumstances in which information may be shared without the consent of the individual concerned. In such circumstances it is important to ensure that the information is disclosed in accordance with locally agreed procedures wherever possible.

Improving the arrangements for information sharing is a key component of developing effective relationships between the Prison Service and the NHS, and other relevant agencies, which should ultimately improve the continuity of care for people passing through the prison system.

The development of effective inter-agency information sharing will require senior management support if it is to be successful. It is important that the accountability and management arrangements that govern information sharing are both robust and transparent.

Information sharing protocols will be a key part in the development of effective information sharing and joint working. Clear operational guidelines should be developed to underpin the policy and support staff in the implementation of the policy and any local agreements.

A suggested process for developing inter-agency information sharing and a framework for information sharing protocols is included at Appendix 2.

APPENDIX 1.

CURRENT GUIDANCE

1. The Protection and Use of Patient Information

The Protection and Use of Patient Information was issued by the Department of Health in March 1996 under cover of HSG(96)18. This relates primarily to the common law duty of confidence held by health professionals and is based on:

i. patients' expectation that information about them will be treated as confidential; and

ii. the importance of making patients fully aware that NHS staff and sometimes staff of other agencies need to have strictly controlled access to such information, anonymised wherever possible.

The guidance sets out:

- The basic principle governing the use of patient information
- Informing patients why information is needed, how it is used and their rights of access to it,
- Safeguarding information required for NHS and related purposes
- The circumstances in which information may be passed on for other purposes or as a legal requirement.

Although produced for the NHS, this guidance is a useful source of advice which can be applied in a prison setting.

2. Caldicott

The review of patient-identifiable information (chaired by Dame Fiona Caldicott) was commissioned by the Chief Medical Officer for England as a result of increasing concern about the ways in which patient information is used in the NHS, and the need to ensure that confidentiality is not being undermined when information is passed between NHS organisations or between the NHS and other organisations. The report of the review – the Caldicott Report – was published in December 1997.

The Committee recommended that NHS organisations should be accountable, through clinical governance procedures, for continuously improving confidentiality and security procedures governing access to and storage of personal information.

Following the report there has been a requirement for each NHS organisation to nominate a senior person, preferably a health professional, to act as a

guardian to be responsible for safeguarding the confidentiality of patient information. These guardians have become known as "Caldicott Guardians" and from January 2002 will exist in Local Authorities as well as health organisations.

Caldicott Guardians act as a focus for information sharing issues which relate to patient information that has been provided in confidence. The responsibility for protecting and using patient information continues to lie with the whole organisation. The Caldicott principles which govern the use of confidential information are as follows:

- Justify the purpose(s) for using personally-identifiable information
- Only use when absolutely necessary
- Use the minimum that is required
- Access should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law

Another important recommendation of the Caldicott Committee was that protocols be developed to protect the exchange of patient-identifiable information between NHS and non-NHS bodies (see Appendix 2. for a suggested framework for information sharing protocols)

3. General Medical Council Standards of Practice: Protecting and Providing Information

The General Medical Council (GMC) published guidance on protecting and providing information in September 2000. The GMC advice to doctors on confidentiality states that:-

> Patients have a right to expect that information about them will be held in confidence by their doctors. Confidentiality is central to trust between doctors and patients. Without assurances about confidentiality, patients may be reluctant to give doctors the information they need in order to provide good care. If you are asked to provide information about patients you should:
>
> - Seek patients' consent to disclosure of information wherever possible, whether or not you judge that patients can be identified from disclosure.
> - Anonymise data where unidentifiable data will serve the purpose.
> - Keep disclosures to the minimum necessary.

> You must always be prepared to justify your decisions in accordance with this guidance.

Doctors are further reminded that "Seeking patients' consent to disclosure is part of good communication between doctors and patients, and is an essential part of respect for patients' autonomy and privacy"

The guidance goes on to deal with circumstances in which consent cannot be obtained, or where patients withhold consent "…exceptionally…personal information may be disclosed in the public interest where the benefits to an individual or to society of the disclosure outweigh the public and the patient's interest in keeping the information confidential."

This guidance given to doctors by the GMC is compatible with the obligations placed upon doctors by the Data Protection Act 1998.

4. United Kingdom Central Council for Nursing Midwifery and Health Visiting: Guidelines for Professional Practice

The UKCC Guidelines for Professional Practice includes sections on confidentiality and providing information.

The guidance includes clause 10 of the Code of Professional Conduct which states that:

'As a registered nurse, midwife or health visitor, you are personally accountable for your practice and, in the exercise of your professional accountability, must…

> "protect all confidential information concerning patients and clients obtained in the course of professional practice and make disclosures only with consent, where required by the order of a court, or where you can justify disclosure in the wider public interest".

5. Guidance on Health Act (S31 Partnership Arrangements) 1999

This guidance relates to assisting the development of partnership arrangements under S31 of the Health Act (1999) which allows pooling of budgets between health and social services to improve the delivery of local health services. There is specific guidance on information sharing between the NHS and Local Authorities which could be applied to partnership arrangements between the Prison Service and the NHS.

The guidance offers advice on sharing information in a legally and ethically acceptable way and is broadly based on Caldicott guidelines. Emphasis is placed on the local 'information community' establishing groups to ensure common procedures and inter-agency protocols are agreed.

Recommendations include:-

- Establishing clear leadership for information sharing and confidentiality
- Establishing local “confidentiality groups”
- Reviewing procedures to ensure compliance with legal requirements
- Ensuring that ‘consent’ procedures are in place
- Adopting and disseminating a code of practice to all staff involved in information sharing
- Developing inter-agency protocols.

APPENDIX 2.

PROCESS FOR DEVELOPING INTER-AGENCY INFORMATION SHARING

The following sections outline a process for developing inter-agency information sharing. The principles and processes could equally be applied to improve internal flows of confidential and sensitive information.

1. Mapping Information Flows

An important starting point will be to map flows of information into and out of the organisation. Key staff should be asked to identify what types of patient information they routinely receive, hold and send.

It will be important as part of this process to identify the uses to which the information is put. This will assist in ensuring that information collected/transmitted is adequate for the intended purpose and not excessive or insufficient.

Reviewing the results of the mapping process should identify which processes and data flows should remain unchanged, and which could be changed or discontinued.

As well as information flows to and from the organisation, it would be helpful to apply the same process to internal information flows.

2. Identifying key partners and stakeholders

The mapping process described above will help to identify key partners with whom information sharing arrangements should be formalised or developed.

The NHS has a network of 'Caldicott Guardians', generally board level clinicians, who act as the focus for information sharing issues. It may be useful for Prisons to consider adopting a similar approach and nominating a senior clinician to act as Caldicott Guardian for their service.

The nominated senior professional should link with the local Caldicott Guardian/s to review the identified information flows and develop arrangements for effective information sharing within legal and ethical boundaries, taking account of confidentiality and consent issues as appropriate.

Making links with the key individuals within partner organisations at an early stage will help to overcome operational difficulties and cultural barriers.

Further joint work will be needed to establish information sharing agreements and protocols between organisations.

3. Information sharing protocols

Information sharing protocols are agreements which set parameters and provide a framework for the secure and confidential sharing of information between organisations.

They provide clear guidance on operational procedures to be followed and should also contain instructions on procedure to be followed in the event of difficulties or where the decision to disclose is a matter of professional judgement.

The existence of such protocols should also give patients and service users confidence that information about them will be managed in accordance with their explicit wishes (except in rare circumstances where organisations are compelled by law to disclose information without consent).

A suggested framework for an information sharing protocol is included at Appendix 3.

APPENDIX 3.

FRAMEWORK FOR AN INFORMATION SHARING PROTOCOL

A protocol for sharing information may be drawn up by two or more parties to encompass the common principles and procedures to be adopted whenever those organisations share information.

The exact content and format of the protocols will be determined locally, but will probably include the following (with examples of issues which could be included under each heading):

- **Objectives of the protocol**

  To set out the commitments and obligations on each party

  To provide a framework for the sharing of information between organisations

  To set out agreed arrangements for data holding and exchange

  To define the uses of the information in question

  To provide safeguards for patients and staff

- **Principles governing the sharing of information**

  Compliance with current legislation on rights of access to information

  Data ownership issues

  Being consistent with relevant guidance and professional codes of conduct

  Being consistent with Caldicott principles

- **Purposes for which information will be shared**

  What information is to be collected/transferred and in what circumstances

  Clearly set out the purposes to which the information will be put by each agency

- **Issues of consent and confidentiality**

  General principles of consent and confidentiality

Guidance to staff on obtaining consent

Recording and checking for consent

Disclosing information without consent (define circumstances and procedures for doing this)

- **Issues of access and security**

  Define arrangements for data collection, storage and transfer

  Define security arrangements for information within each organisation

  Senior person from each agency nominated to ensure compliance with procedures

- **Procedures for disclosing information**

  Clearly set out the circumstances and arrangements for information exchange

  Individuals are to be made aware of the information which will be shared and the purposes for which it will be used

  Information is only to be shared on a need-to-know basis

  When disclosing information, professionals should state whether the information is fact, opinion or a combination of the two

  Where professionals request that information supplied by them be kept confidential from the patient, the reasons for taking this decision should be recorded and such decisions should only be taken on statutory grounds

- **Management and review of the protocol**

  Structures and responsibilities

  Staff awareness and training

  Monitoring arrangements

  How to deal with breaches of the protocol

  Process for review/change of the protocol

APPENDIX 4.

DATA PROTECTION ACT 1998

1. Conditions for Processing (Schedule 2 of the Act)

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):-

- The data subject has given their consent to the processing.
- The processing is necessary:-
  a) for the performance of a contract to which the data subject is a party, or
  b) for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary to comply with any legal obligation to which the data controller is subject , other than an obligation imposed by contract.
- The processing is necessary in order to protect the vital interests of the data subject.
- The processing is necessary :-
  a) for the administration of justice,
  b) for the exercise of any functions conferred by or under any enactment,
  c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
  d) for the exercise of any other functions of a public nature exercised in the public interest.
- The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

2. Conditions for Processing Sensitive Data (Schedule 3 of the Act)

At least one of these must be satisfied, in addition to at least one of the conditions for processing (which apply to the processing of all personal data), before processing of sensitive personal data can claim to have been lawful in accordance with the First Principle.

- The data subject has given their explicit consent to the processing of the personal data.
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment. The Secretary of State may by

order specify cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.

- The processing is necessary:-
  a) in order to protect the vital interests of the data subject or another person in a case where:-
     - consent cannot be given by or on behalf of the data subject, or
     - the data controller cannot reasonably be expected to obtain the consent of the data subject, or

     b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
- The processing:-
  a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade-union purposes and which is not established or conducted for profit,
  b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
  c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes, and
  d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
- The processing:-
  a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
  b) is necessary for the purpose of obtaining legal advice, or
  c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- The processing is necessary:-
  a) for the administration of justice,
  b) for the exercise of any functions conferred by or under any enactment, or
  c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

  The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.
- The processing is necessary for medical purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by:-
  a) a health professional (as defined in the Act), or
  b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
- The processing:-
  a) is of sensitive personal data consisting of information as to racial or ethnic origin,

b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted and maintained, and
c) is carried out with appropriate safeguards for the rights and freedoms of data subjects. The Secretary of State may by order specify circumstances in which such processing is, or is not, to be taken to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

- The personal data are processed in circumstances specified in an order made by the Secretary of State.

APPENDIX 5.

REFERENCES

Data Protection Act 1998.

Data Protection (Subject Access Modification) (Health) Order 2000.

PSO 9020: Data Protection.

HSG (96) 18, Protection and Use of Patient Information. Department of Health guidance on confidentiality.

HSC 1998/217, Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients.

HSC 1999/053, For The Record. Contains overview of key issues and solutions and best practice to follow when preparing a records management strategy. Also contains the NHS retention and disposal schedule setting out **minimum** retention periods for medical records.

The Caldicott Committee Report on the Review of Patient Identifiable Information, December 1997, and subsequent guidance on improving confidentiality and security, including implementation **(HSC 1998/089, Implementing the Recommendations of the Caldicott Report)** and the appointment of Guardians **(HSC 1999/012, Caldicott Guardians).**

LAC (2000)9, Implementation of Health Act Partnership Arrangements. Includes guidance on information sharing between the NHS and local authorities.

Confidentiality: Protecting and Providing Information. GMC, 2000.

Seeking Patients' Consent: The Ethical Considerations. GMC, 2000.

UKCC Professional Code of Conduct.

PSO 2710: Follow up to deaths in custody.

PSO 1301: Investigating a death in custody.