

**SUTTON AND MERTON  
HEALTH AND SOCIAL CARE COMMUNITY**

**INFORMATION SHARING**

**For agencies delivering services to adults**

**PART A**

**THE LEGAL FRAMEWORK**

**March 2004**

Review March 2005

## **INFORMATION SHARING**

### **THE LEGAL FRAMEWORK**

The Information Sharing Protocol (Part B) is based on a number of legislative and policy drivers as detailed below.

1. Data Protection Act 1998
2. The Caldicott Principles
3. The Human Rights Act 1998
4. Access to Health Records Act 1990
5. Crime and Disorder Act 1998
6. Criminal Procedures and Investigations Act 1996
7. Freedom of Information Act 2000
8. Regulation of Investigatory Powers Act 2000
9. Computer Misuse Act 1990
10. Health and Social Care Act 2001
11. Common Law Duty of Confidentiality
12. Codes and Standards of Confidentiality

#### **NB: For agencies delivering services for Children**

- The law surrounding consent is different for children but they have the same rights to confidentiality and human rights as adults. In addition, the Children Act 1989 aims to protect children from abuse and neglect.
- Sharing information about children therefore needs additional consideration to sharing information about adults. Staff are advised to discuss such concerns with the lead professional for child protection in their agency or with the social services referral and assessment team for children and families in the local authority where the child lives. Clear written guidance can be found in *London Child Protection Procedures* (2003) and in *What to do if you think a child is being abused* (Dept of Health 2003)

#### **1. DATA PROTECTION ACT 1998**

The key legislation governing the protection and use of identifiable patient/client information (“personal data”) by public organisations is the **Data Protection Act 1998**.

The Act gives seven rights to individuals in respect of their own personal data held by others, they 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
- right to take action to rectify, block, erase or destroy inaccurate data
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened

### **The rules of data protection - the principles**

Anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights (noted above);
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply.

To meet the requirements of these principles, personal information should:-

- Only be obtained and processed for one or more specified and lawful purposes.
- Be sufficient, relevant in relation to the specified purpose (s).
- Be accurate and contemporaneous.
- Stored/held no longer than necessary.
- Be accessible to the individual to whom it pertains.
- Be adequately protected by organisations, whether it is electronic or paper-based.
- Should not be transferred outside of the European Union unless appropriately protected.

The basic functions related to the processing of personal data, together with the standards which must be adhered to in undertaking such processing are set out below:-

	<b>Information Processing</b>	<b>Information Processing Standards</b>
<b>H</b>	<b>Holding</b>	<b>Securely &amp; Confidentially</b>
<b>O</b>	<b>Obtaining</b>	<b>Fairly &amp; Efficiently</b>
<b>R</b>	<b>Recording</b>	<b>Accurately &amp; Reliably</b>
<b>U</b>	<b>Using</b>	<b>Effectively &amp; Ethically</b>
<b>S</b>	<b>Sharing</b>	<b>Appropriately &amp; Lawfully</b>

**Schedule 2 : Conditions related to the processing of any personal data**

As stated above, the processing of personal data of any type must fulfil at least one of the following conditions :-

- The data subject (patient/client) has given consent to the processing.
- The processing is part of an activity that the data subject understands and is party to; or, has initiated.
- The processing is necessary to protect the vital interests of the data subject.
- The data controller has legal obligations that have to be met by the processing of such data.
- The processing is necessary for the administration of justice, or for any other functions of a public nature (as in the “public interest”).
- The processing is necessary for the purposes of legitimate interests pursued by the data controller.

Health/care professionals use some or all of the above conditions on a daily basis in their work with clients/patients. Schedule 2 sees the data subject as ‘active’ in the ‘ownership’ of their information. The issue of consent is very explicit indeed.

However, there are a number of exemptions where the right of the individual to actively control the processing of their data is overridden. They relate to the “best interests” of the individual themselves, and in the context of the wider, “public interest”.

**Schedule 3 : Conditions related to the Processing of Sensitive Personal Data**

As stated above the processing of “sensitive” personal data such as that within the health and social care field, not only has to fulfil one of the conditions under Schedule 2 but also one of those under Schedule 3, as set out below : -

1. The data subject has given his explicit consent to the processing of the personal data.

2. (1) 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.

3.1 The processing is necessary-

(a) in order to protect the vital interests of the data subject or another person, in a case where-

(i) consent cannot be given by or on behalf of the data subject, or,

(ii) 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.

4. The processing –

(a) is carried out in the course of its legitimate activities by any body or association which-

(i) is not established or conducted for profit, and

(ii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c) relates only to individuals who either are members of the body or association or 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.

5. The information contained in the personal data has been made

public as a result of steps deliberately taken by the data subject.

6. 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.

7. (1) The processing is necessary –

(a) for the administration of justice,

(b) for the exercise of any functions conferred on any person by or under an enactment, or

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

8. (1) The processing is necessary for medical purposes and is undertaken by-

(a) a health professional, or

(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9. (1) 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 or maintained, and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

There is a wide range of conditions identified in Schedule 3 that recognise the functional need of health/care organisations and professionals to legitimately process personal data. It supports the necessity of statutory interventions and the inevitable need to process very sensitive personal data as a result.

To summarise:

- Processing of personal information must satisfy one of the conditions in Schedule 2 of the Act.
- "Sensitive" personal information (including health information) is further protected, the processing of it has to meet one of the conditions of Schedule 3 of the Act.

Data that is processed within the context of health and social care is subject to satisfying one condition of Schedule 2 and one of Schedule 3 of the Act.

**However, the basic premise is to seek explicit consent from the person to whom the information belongs.**

### **Section 29 – crime and taxation exemption**

Personal data processed for any of the following purposes:

- (a) the prevention or detection of crime,
- (b) the apprehension or prosecution of offenders, or
- (c) the assessment or collection of any tax or duty or of any imposition of a similar nature

are exempt from the first data protection principle (except to the extent that it requires compliance with the conditions in Schedules 2 and, 3 as described above, and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of matters mentioned in this exemption.

## **2. THE CALDICOTT PRINCIPLES**

All organisations which are party to the Information Sharing Protocol and the related Service Specific Information Sharing Agreements are

committed to the six Caldicott principles when considering whether confidential information should be shared.

### **Principle 1 – Justify the purpose(s) for using confidential information**

Every proposed use or transfer of personally-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the Caldicott Guardian.

### **Principle 2 – Don't use personally-identifiable information unless it is absolutely necessary**

Information items which can identify an individual should not be used unless there is no alternative.

### **Principle 3 – Use the minimum that is required**

Where use of personally-identifiable information is considered to be essential, each item of information should be justified with the aim of reducing identifiability.

### **Principle 4 – Access to personally-identifiable information should be on a strict “need-to-know” basis**

Only those individuals who need access to personal information should have access to it, and they should only have access to the information items that they need to see.

### **Principle 5 – Everyone should be aware of their responsibilities**

Action should be taken to ensure that those handling personally-identifiable information – both practitioner and non-practitioner staff – are aware of their responsibilities and obligations to respect an individual's confidentiality and privacy.

### **Principle 6 – Understand and comply with the law**

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

The Caldicott Principles clearly accord with Schedules 2 & 3 of the Data Protection Act, and Article 8 of the Human Rights Act.

Compliance with these principles also requires that each partner organisation is able to map and track information streams flowing in and

out of it and to be aware of where, why and with whom information is being exchanged.

### **3. THE HUMAN RIGHTS ACT 1998**

The Human Rights Act 1998 (HRA) is based upon the *European Convention of Human Rights*, and maps out a number of rights and freedoms that individuals can expect to enjoy in a democratic society. Its purpose is to curtail the power of the state from ‘interfering’ with, or unfairly controlling the lives of its citizens.

The HRA works with the ‘primary legislation’ of the countries in which it has become law. This means that in making a ruling on a case, a Judge or Magistrate has to first address whichever primary legislation is relevant to the case, before taking into account the Human Rights implications.

There are eighteen articles in this Act, but the one most likely to be invoked, with respect to confidentiality and security of personal information, is:

#### **Article 8 : Right to Respect for Private and Family Life**

*“Everyone has the right to respect for his private and family life, his home and his correspondence.*

*There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.*

This clearly supports the Data Protection Act in respect of both Schedules 2 and 3. The HRA requires that any obvious act of curtailment of such rights and freedoms by the State (or any instrument of it) be justified and evidenced. The Act recognises the issue of ‘proportionality’, in that the rights of one individual might be at variance with those of another. An example of this in terms of Article 8 would be where a child might be at risk of “significant harm”, or indeed, where an individual with a severe mental illness poses a risk to the safety of others. In the case of a child at risk of ‘significant harm; the professionals involved will work within the context of the Children Act 1989, and share information in order to protect that child or children. In this situation therefore, Article 8 is overridden in the child’s “best interests”.

## **Article 6 : Right to a Fair Trial**

As the provisions of this Article can also be applied to the right to a fair assessment, it is clearly necessary for there to be accurate recording of information and the appropriate use of risk assessment and management processes, when disclosing information without consent. If a risk assessment is found to be without professional rigour and judgement based on the presenting information, then the individual has grounds to say that the assessment was not 'fair' within the context of Article 6.

This would in turn constitute a breach of Article 8 and Schedules 2 and 3 of the Data Protection Act, as the grounds for overriding these rights and freedoms are brought into play.

### **4. ACCESS TO HEALTH RECORDS ACT 1990**

The Data Protection Act 1998 supersedes the **Access to Health Records Act 1990** apart from the sections dealing with access to information about the deceased. The Access to Health Records Act 1990 provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

### **5. CRIME AND DISORDER ACT 1998**

The **Crime and Disorder Act 1998** introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area. Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purpose of the Act. However, whilst all agencies have the power to disclose, Section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the data. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

### **6. CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996**

The **Criminal Procedures and Investigations Act 1996** requires the police to record in durable form any information that is relevant to an investigation. The information must be disclosed to the Crown Prosecution Service, who must in turn disclose it to the defence at the

relevant time if it might undermine the prosecution case. In cases where the information is deemed to be of a sensitive nature then the CPS can apply to a judge or magistrate for a ruling as to whether it should be disclosed.

## **7. FREEDOM OF INFORMATION ACT 2000**

The Freedom of Information Act 2000 requires that public organisations put procedures in place to facilitate the disclosure of information under the Act. This includes adopting and maintaining a publication scheme and to publish information in accordance with it. Publication schemes should be in operation in all NHS organisations by 31 October 2003. Full access regimes under the Act will be in force from January 2005. Freedom of Information Act 2000 only relates to an organisations corporate activity as patient records are accessible via the Data Protection Act 1998.

## **8. REGULATION OF INVESTIGATORY POWERS ACT 2000**

The Regulation of Investigatory Powers Act 2000 ensures that investigatory powers are used in accordance with the Human Rights Act. It updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It also puts other intrusive investigative techniques on a statutory footing for the very first time; provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act.

## **9. COMPUTER MISUSE ACT 1990**

Under the **Computer Misuse Act 1990** a person is guilty of a criminal offence if:

- he causes a computer to perform any function with intent to secure access to any program or data held in any computer
- the access he intends to secure is unauthorised; and
- he knows at the time when he causes the computer to perform the function that this is the case

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring that staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities.

## 10. HEALTH AND SOCIAL CARE ACT 2001 (HSCA)

Section 60 of the HSCA gives the Secretary of State the power to make regulations relating to the processing of prescribed patient information for medical purposes in the interests of the patients or the wider public good e.g. (disclosing patient identifiable information to specified bodies, such as cancer registries).

Section 60 does not change DPA 1998 requirements but where regulations apply it does set aside the legal duty of confidentiality and replace it with a range of safeguards intended to ensure that the use of a patients information has no detrimental effect on that patient.

## 11. COMMON LAW DUTY OF CONFIDENTIALITY

All staff working in both the statutory and independent sector are aware that they are subject to a **Common Law Duty of Confidentiality**, and must abide by this. The duty of confidence only applies to identifiable information and not to aggregated data derived from such information or to information that has otherwise been effectively anonymised – i.e. it is not possible for anyone to link the information to a specific individual.

The 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. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect other from harm). Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and professional bodies responsible for setting ethical standards for health professionals accept that this is the case.

Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained (deceased individuals may have provided their consent prior to death). Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence.

Where it is judged that an individual is unable to provide consent (for example due to mental incapacity or unconsciousness), other conditions in Schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the *vital interest* of the individual).

Whilst, under current law, no-one can provide consent on behalf of an adult in order to satisfy the common law requirement, it is generally accepted that decisions about treatment, and the disclosure of information, should be made by those responsible for providing care and that they should be in the best interests of the individual concerned.

## **12. CODES AND STANDARDS OF CONFIDENTIALITY**

All agencies and professional bodies are subject to their own codes or standards relating to confidentiality.

There are other Acts of Parliament and codes of practice that govern working practices. Where relevant, these will be referred to in the Service Specific Information Sharing Agreements.