



## Confidentiality Policy and Code of Conduct

Document Profile Box	
Document Category / Ref	QSSD 1302
Version:	0002.1
Ratified by:	Policy Review Group Joint Consultative Committee
Date ratified:	15 <sup>th</sup> September 2009
Name of originator / author:	Rahima Hoque – Information Governance Manager
Name of responsible committee / individual:	Information Governance Working Group
Date issued:	31 <sup>st</sup> October 2009
Review date:	1 year from issue date
Target audience:	All staff
Document owner:	Colin Cessford – Director of Strategy & Business Development
Approved by:	

## Version Control

Version	Release Date	Author	Status	Comments
0001	Oct 2007	Mark Glencorse	Final	First Issue.
0002	Apr 2009	Rahima Hoque	Draft	Revised in line with toolkit requirements and QSSD 612. Renamed Confidentiality Policy and Code of Conduct from Confidentiality Code of Conduct.
0002	Sept 2009	Rahima Hoque	Final	Following ratification.
0002.1	Nov 2009	Rahima Hoque	Final	Policy title in Docuviewer changed to match document title and document owner added to profile box.

### Did you print this document yourself?

Please be advised that the Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version.

### Document Location

The source of the document will be found in the Trust Quality System.

### Freedom of Information Act 2000 Access

This document will be available via the NEAS Publication Scheme.

## TABLE OF CONTENTS

	PAGE
1. INTRODUCTION	1
2. PURPOSE	1
3. SCOPE	1
4. DEFINITIONS	2
5. RESPONSIBILITY AND ACCOUNTABILITY	3
6. EQUALITY AND DIVERSITY STATEMENT	4
7. LEGAL AND PROFESSIONAL OBLIGATIONS	4
8. PROTECTING INFORMATION	6
9. CONFIDENTIALITY OF PATIENT INFORMATION	8
10. CONFIDENTIALITY OF STAFF INFORMATION	9
11. CONFIDENTIALITY CLAUSES	9
12. DISCLOSURE OF INFORMATION	9
13. PATIENT CHOICE	12
14. PATIENT CONSENT	13
15. RETENTION AND STORAGE OF CONFIDENTIAL INFORMATION	13
16. ABUSE OF PRIVILEGES AND NON COMPLIANCE	13
17. ADVERSE INCIDENT REPORTING	13
18. CONFIDENTIALITY AUDITS	14
19. SPECIFIC DEPARTMENTAL CONSIDERATIONS	14
20. CONSULTATION, APPROVAL AND RATIFICATION PROCESS	15
21. REVIEW AND REVISION ARRANGEMENTS	15
22. DISSEMINATION AND IMPLEMENTATION	15
23. DOCUMENT CONTROL INCLUDING ARCHIVING ARRANGEMENTS	16
24. MONITORING COMPLIANCE WITH AND THE EFFECTIVENESS OF PROCEDURAL DOCUMENTS	16
25. REFERENCES	18
APPENDIX B: SHARING INFORMATION WITH IMPLIED CONSENT	22
APPENDIX C: STATUTORY RESTRICTIONS ON DISCLOSURE	26
APPENDIX D: MENTAL CAPACITY ACT 2005	27

## **1. Introduction**

- 1.1. This policy and code of conduct has been developed in line with the national NHS Code of Practice on Confidentiality and describes the responsibilities of all staff and lays down guidelines in order to ensure confidentiality is maintained.
- 1.2. The nature of the work undertaken by the Trust's employees, volunteers and contractors brings them into possession of a great deal of confidential, and often highly sensitive information, both patient and non-patient related. Therefore, it is essential that the public at large believe that the organisation as a whole maintains confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose. The Trust also has statutory obligations to maintain records, systems and procedures ensuring data records are stored and disposed of accordingly.
- 1.3. All staff working for the North East Ambulance Trust (NEAS) have a legal duty of confidentiality to the subjects of information they come into contact with. This duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence (e.g. patient to healthcare professional).
- 1.4. Information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, where there is a legal basis to do so, when it is in the public interest or there is legal justification to do so.
- 1.5. The principle behind this policy and code of practice is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trusts security systems or controls in order to do so.

## **2. Purpose**

- 2.1. The purpose of this policy is to establish the principles that must be observed by all employees of the Trust, who have access to patient or staff confidential information, in their handling of confidential information, and to ensure that all staff are aware of their responsibilities, and the consequences of failing to adhere to Trust policy.

## **3. Scope**

- 3.1. This policy covers all sites and systems operating and utilised by NEAS.
- 3.2. The policy applies to any individual employed, in any capacity, by the Trust.
- 3.3. Any breach of the NHS Code of Practice on Confidentiality or the Trust Confidentiality Policy and Code of Conduct is considered to be an offence and in that event, NEAS disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Trust, and who have access to personal information, will be expected to have read

and comply with this policy. It is expected that departments / sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

#### **4. Definitions**

4.1. The Oxford English Dictionary definition of confidential is 'intended to be kept secret' (2002).

4.2. **Confidential information** is any information held, both personal and non-personal, that when provided was done so in the expectation it would not be disclosed without relevant authority. It can be anything that relates to patients, staff, their family and friends and also to Trust information that is protected from release under the Freedom of Information Act 2000 (FOI).

4.2.1. Confidential information includes but is not limited to:

- Personal details of any patient.
- Information pertaining to diagnosis, prognosis or treatment where this is linked to an identifiable individual.
- Personal details of any employee.
- Information contained within the personnel records of any employee.

4.2.2. This class of information may be stored in any manner e.g. on paper, electronically, video, photograph, and could be stored on any device, including portable such as laptops, mobile phones, palmtops and digital cameras. Confidential information may also be passed by word of mouth.

4.3. **Personal data** is data which relate to an individual who can be identified from those data or from those data and other information which is in the possession of, or likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any person in respect of the individual. Personal information includes name, address, date of birth, or any other unique identifier such as NHS Number, hospital number, national insurance number etc. It also includes information which, when presented in combination, may identify an individual e.g. postcode etc.

4.4. **Sensitive personal data** is defined in Section 2 of the Data Protection Act 1998 (DPA) as data regarding an individual's race or ethnic origin, political opinion, religious beliefs, trade union membership, physical or mental health, sex life, criminal proceedings or convictions. These data are subject to more stringent conditions on their processing when compared to personal information.

4.5. **Explicit or express consent** means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually

given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

- 4.6. **Implied consent** means patient agreement that has been signalled by behaviour of an informed patient.

## 5. Responsibility and Accountability

- 5.1. Overall responsibility for the confidentiality and security of patient and staff information lies with the Chief Executive. Implementation of and compliance with the policy is delegated to the Caldicott Guardian for patient information and Director of Human Resources for staff information.

### 5.2. Duties within the Organisation

- 5.2.1. **All staff** have an obligation to safeguard the confidentiality and security of personal information. This is governed by law; contracts of employment; local policies and procedures and in many cases by professional codes of conduct. All staff should be aware that a breach of confidentiality may be regarded as serious misconduct which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. In addition, unauthorised disclosure of personal information, or using such information in a way other than as described in the Trusts Data Protection Policy, is an offence and could lead to prosecution of individuals and / or the organisation.
- 5.2.2. Staff contracts of employment will include explicit reference to these obligations and the consequences of breaches of confidentiality. The key policy issues and procedures involved may be summarised in the staff Code of Conduct. Job descriptions will make particular responsibilities explicit.
- 5.2.3. Staff within the Trust who employ or use the services of an agency, external supplier or contractor will require them to agree contractually (by means of a signed contract or agreement) to maintain the confidentiality and security of any personal information.
- 5.2.4. Individuals who do not have a contract of employment with the Trust in which they work (and are not covered by an agreement / contract) will be required (by means of a signed code of conduct or equivalent) to agree to maintain confidentiality and security as if they were directly employed.
- 5.2.5. All line managers and senior managers are responsible for ensuring that this policy is communicated and implemented within their area of responsibility. Any advice or assistance regarding this policy is available from the Information Governance Lead.
- 5.2.6. **The NEAS Information Governance Working Group (IGWG) have a responsibility to:**
- Developing, maintaining and implementing the Confidentiality Code of Conduct and procedures across NEAS ensuring that they meet national and legislative requirements in relation to confidentiality.

- Promoting awareness of confidentiality issues.

## **6. Equality and Diversity Statement**

- 6.1. The Trust is committed to providing equality of opportunity, not only in its employment practices but also in the services for which it is responsible. As such, this document has been screened, and if necessary an EIA has been carried out on this document, to identify any potential discriminatory impact.
- 6.2. If relevant, recommendations from the assessment have been incorporated into the document and have been considered by the approving committee. The Trust also values and respects the diversity of its employees and the communities it serves. In applying this policy, the Trust will have due regard for the need to:
- Eliminate unlawful discrimination.
  - Promote equality of opportunity.
  - Provide for good relations between people of diverse groups.
  - For further information on this, please contact the Equality and Diversity Department.

## **7. Legal and Professional Obligations**

- 7.1. The disclosure of confidential information needs to be both lawful and ethical. There is a range of legislation and guidance that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range that require information to be used or disclosed.
- 7.2. **Data Protection Act 1998**
- 7.2.1. The key statutory requirement for NHS compliance with confidentiality is the DPA. This Act legislates for the processing of the personal information of living individuals. The term 'processing' includes any action performed on the data including obtaining, holding, recording, using and disclosing. The Act applies to staff as well as patient records and covers both paper and electronic records.
- 7.2.2. NEAS meets its obligations under the Act as it works in line with the 8 Data Protection principles:
- Data shall be processed fairly and lawfully.
  - Data shall be processed only for specified purposes.
  - Data shall be adequate, relevant and not excessive.
  - Data shall be accurate and kept up to date.
  - Data shall not be kept for longer than necessary.
  - Data shall be processed in accordance with individual's rights.
  - Data shall be kept secure.

- Data shall not be transferred outside the European Economic Area (EEA) without adequate protection.
- 7.2.3. The Act allows for third party access to personal information in certain specified circumstances, known as exemptions. Further information can be found on the Information Commissioner's website – [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk).
- 7.3. **Freedom of Information Act 2000**
- 7.3.1. This Act came into full effect on the 1st January 2005 and legislates from the general right of access to non-personal information held by public authorities. The idea behind this Act was to encourage greater openness by these authorities.
- 7.3.2. The Act contains a number of exemptions – valid reasons – why a request for information can be refused. Further information can be found on the Information Commissioner's website – [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk).
- 7.3.3. Non-personal, non-confidential information on NEAS and its services should be available through a variety of media in line with the Trust's Freedom of Information (FOI) Publication Scheme.
- 7.4. **Human rights Act 1998**
- 7.4.1. Article 8 of the Human Rights Act 1998 establishes a right to 'respect for private and family life'. This identifies a duty to protect the privacy of individuals and preserve the confidentiality of their health records. Compliance with the DPA ensures the Trust is meeting its obligations under Human Rights legislation.
- 7.5. **Common Law of Confidentiality**
- 7.5.1. Any personal information given or received in confidence for one purpose may not be used for a different purpose or disclosed without the consent of the provider of the information. Two exceptions to the common law duty exist where information may be disclosed without consent, these are:
- Where there is an overriding public interest in the disclosure, for example where there is a significant risk to the safety of one or more individuals.
  - Where the disclosure is required by law or requested by the court.
- 7.6. **Caldicott Principles 1998**
- 7.6.1. The Caldicott Principles are a set of guidelines developed specifically for handling patient identifiable information (PII). NEAS has an identified Caldicott Guardian who will oversee work to establish the highest practical standards for handling PII.
- 7.6.2. The 6 principles are:
- Justify the purpose for using PII.
  - Only use PII when absolutely necessary.
  - Only use the minimum PII necessary.

- Access to PII should be on a strict need-to-know basis.
- Everyone must be aware of their responsibilities when handling PII.
- Understand and comply with the law.

#### 7.7. **Crime and Disorder Act 1998**

7.7.1. The Crime & Disorder Act provides the power to disclose information to the Police for the purposes of preventing or detecting crime. It does not provide a duty to disclose, and does not override a healthcare professional's common law duty of confidence.

#### 7.8. **Computer Misuse Act 1990**

7.8.1. The Computer Misuse Act makes it an offence to access information held within a computer system without authority. Staff therefore must only access information that they are authorised to access, must not provide access to computer systems to others (by allowing others to use their password) and staff must not alter information where they are not authorised to do so.

7.8.2. The Computer Misuse Act creates three specific offences:

- Unauthorised access to computer material.
- Unauthorised access to a computer system with intent to commit or facilitate the commission of a crime.
- Unauthorised modification of computer material.

7.9. The Trust will undertake or commission regular audits to assess its compliance with legal requirements.

### 8. **Protecting Information**

8.1. All staff have a duty to protect the information they handle on a day-to-day basis, whether this is personal or non-personal.

#### 8.2. **Recognising that confidentiality is an obligation for all staff, external contractors, and volunteers**

8.2.1. The duty of confidentiality arises out of the common law of confidentiality, professional obligations, and also staff employment contracts (including those for contractors). Breach of confidence, inappropriate use of health records or abuse of computer systems may lead to disciplinary measures, bring into question professional registration and possibly result in legal proceedings. Staff should ensure that they are aware of the requirements and standards of behaviour that apply.

8.2.2. Voluntary staff who are not employees, contractors, researchers and students are also under obligations of confidentiality, and must sign an agreement indicating their understanding when helping within the NHS.

#### 8.3. **Recording patient information accurately and consistently**

8.3.1. Maintaining proper records is vital to patient care. If records are inaccurate, future decisions may be wrong and harm the patient. If information is recorded inconsistently, then records are harder to interpret, resulting in delays and possible errors. The information may be needed not only for the immediate treatment of the patient and the audit of that care, but also to support future research that can lead to better treatments in the future.

8.3.2. The practical value of privacy enhancing measures and anonymisation techniques will be undermined if the information they are designed to safeguard is unreliable.

#### 8.4. **Keeping patient information private**

8.4.1. This includes aspects such as:

- Not gossiping – this is clearly an improper use of confidential information.
- Taking care when discussing cases in public places - it may be pertinent to discuss cases with colleagues for professional reasons (to gain advice, or share experience and knowledge), but care must be taken to ensure that others do not overhear these conversations. Generally, there is no need to identify the patient concerned.

#### 8.5. **Keeping patient information physically and electronically secure**

8.5.1. Staff should not leave portable computers, medical notes or files in unattended cars or in easily accessible areas. Ideally, store all files and portable equipment under lock and key when not actually being used.

8.5.2. Staff should not normally take patient records home, and where this cannot be avoided, procedures for safeguarding the information effectively should be agreed via the Caldicott Guardian.

8.6. Do not leave confidential information on view. Paper files should be locked away in drawers / cabinets. Staff should 'log out' of computers when not at their desk.

- Never share your password with anyone else.
- Confidential phone calls should not be conducted in an open office.
- Adopt a 'clear desk policy'.
- Do not disclose confidential information over the telephone unless you are 100% certain of the identity of the caller. If in doubt, check the caller's identity and establish whether they are in fact entitled to receive the information. Call back if necessary. If in doubt, do not release the information and check with the Information Governance Lead.
- Faxing confidential information should only be used if the receiving fax is classified as a safe haven fax. Ask the recipient to confirm receipt of the fax as soon as it is received. Reference should be made to the NEAS Safe Haven Policy.
- Patient identifiable and personal information should not be sent via email as it's security cannot be assured.

- 8.7. Further information can be found in the NEAS Information Security and Records Management Policies.

## **9. Confidentiality of Patient Information**

### **9.1. General principles**

- 9.1.1. The confidentiality of patient information must be safeguarded, particularly where this information is shared between the NHS and its partner organisations. However it is essential that confidentiality does not act as a barrier to the provision of care. There are many situations where the exchange of patient identifiable information is necessary for the efficient and effective operation of the Trust and its partner organisations. The aim is to ensure that information remains accessible to those who need to know, whilst ensuring that the information is adequately protected from unauthorised access and that where appropriate patients are fully aware of who their information is disclosed to and why.
- 9.1.2. All staff must ensure that they are aware of and fully understand their legal obligations to keep information confidential. Patient information must be protected from unauthorised access, disclosure or destruction, regardless of the format in which it is held. In particular, staff must not leave confidential information unattended when not in use. Staff are only authorised to access information that is relevant to their role, where they are involved directly with the care of individual patients. Staff must not deliberately access their own clinical records, either manual or electronic, or the records of relatives or friends unless this is done through a formal Data Protection access request.
- 9.1.3. Staff may only access the records of friends or relatives where this is required as part of their job role at that time. Staff must refrain from having confidential discussions with other clinicians in public areas, or in areas where they can be overheard.
- 9.1.4. Patient information must not be removed from Trust without appropriate and documented authorisation. Electronic patient information must not be transferred to or stored on any removable storage device (such as a USB memory stick, CD or DVD etc) without explicit authority to do so from the Trust Caldicott Guardian.

### **9.2. Information relating to minors**

- 9.2.1. Children and young people are entitled to the same duty of confidentiality as adults – providing that those aged under 16 are judged by professionals to understand their choices and the potential outcomes of sharing information (known as Gillick competence). Parental consent should be sought to share information about a child or young person (in law, those under the age of 18).
- 9.2.2. Exceptions to this are when contact with an individual or individuals who have 'Parental Responsibility' would be more likely than not to jeopardise the safety or welfare of the child / young person; or, doing so would conflict with the wishes of the child / young person. Gillick

competence means that "...the parental right to determine whether or not their minor child below the age of 16 will have medical treatment terminates if and when the child achieves sufficient understanding and intelligence to enable him to understand fully what is proposed." Lord Fraser, Gillick v West Norfolk Area Health Authority 1985.

- 9.2.3. The Data Protection (Subject Access Modification)(Health) Order 2000 provides that; where information has been provided by a child in the expectation that it would not be disclosed to their parent / guardian, or where it has been obtained as a result of any investigation to which the child consented in the expectation that it would not be disclosed, or where the child has expressly indicated that the information should not be disclosed, parent / guardians have no automatic right of access where a child has been deemed Fraser competent and is aged 12 or over.

## **10. Confidentiality of Staff Information**

- 10.1. Information relating to employees of the Trust is governed by the DPA; information must not be disclosed without consent unless a legal duty to disclose exists.
- 10.2. Confidential information relating to employees must be provided with the same degree of protection as that afforded to patient information. Employees may only access information relating to themselves by exercising their rights of access under the DPA, subject to the exemptions from access contained within the Act.

## **11. Confidentiality Clauses**

- 11.1. **Staff contracts** - All staff contracts, whether permanent, temporary or agency, must contain a suitable confidentiality clause which outlines the employees responsibilities. Breaches of confidentiality may be viewed as gross misconduct under NEAS Code of Conduct, and could result in termination of employment.
- 11.2. **Professional Codes of Conduct** - In addition to clauses contained within staff contracts and terms and conditions, staff also have obligations in relation to confidentiality that are identified within their professional codes of conduct. All staff must ensure that they are fully aware of these and abide by their requirements.

## **12. Disclosure of Information**

### **12.1. General principles**

- 12.1.1. It is neither practical or necessary to seek the consent of a patient or other informants in every instance that information needs to be passed on. It is therefore important that patients are kept fully informed of how the information they provide is used.

12.1.2. Whilst it is necessary do disclose information about a patient to those staff who are providing or auditing care, it is important to ensure that those who see information have a genuine need to know.

12.1.3. Staff must ensure that patients within their care are kept fully informed of the purposes for which information about them is collected and those to whom this information may be disclosed. Specifically, patients have the right to make decisions as to whether or not information about them is disclosed either in relation to healthcare provision or for non-healthcare care purposes. The disclosure of information for healthcare purposes is not normally an issue for the great majority of patients, however where appropriate patients must be given opportunities to raise objections and concerns.

## 12.2. **Sharing information outside the NHS**

12.2.1. Sharing with partner organisations outside the NHS must be based on either patient consent or a statutory requirement. Where not required by legislation, information sharing must be covered by an appropriate Information Sharing Protocol.

## 12.3. **Requests for personal information from staff and patients**

12.3.1. Requests by individuals to access their own records, both staff and patient, are known as 'Subject Access Requests' and are a given right under the DPA. All requests must be made in writing and completed within 40 days. Reference should be made to the NEAS Data Protection Policy when handling these requests.

## 12.4. **Requests from the Police**

12.4.1. Requests are often received from the police for copies of patient report forms, incident logs and tapes of calls. The Police do not have an automatic right of access to information held by the Trust. Where a request is received, certain information can be released without consent if there is a legal justification for disclosure.

12.4.2. Where the information is required to assist the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty, Section 29 of the DPA can be applied. This section does not 'require' the disclosure of information; it merely provides the Trust with a legal basis under which it may release the information.

12.4.3. However, these requests must be made in writing using the official police form (these will differ from force to force) or a NEAS Police Request for Personal Data Form.

12.4.4. Under no circumstances should information be handed out at the scene of an incident. All requests are logged by Clinical Audit and the Control Room Manager.

## 12.5. **Requests for non-personal information**

12.5.1. Requests for non-personal information are governed by the requirements of the FOI Act. Reference should be made to the NEAS Freedom of Information Policy and Procedure prior to releasing information.

## 12.6. **Requests from the media**

12.6.1. Under no circumstance should personal or non personal information be given out to the media.

If you receive a request from the media by personal visit, phone, email or post, please forward and refer that person to the Trust PR Department.

## 12.7. **Requests from solicitors**

12.7.1. A letter of authorisation must accompany requests from solicitors for information pertaining to their client from the individual who is the subject of the information.

## 12.8. **Requests for information on other individuals**

12.8.1. Requests for information on other individuals, whether they be patients or staff should only be released on a 'need to know' basis. The requester must be able to justify why the request is being made and that they are entitled to make the request.

12.8.2. There are circumstances when information can be released to third parties. Further guidance can be found in the Data Protection Policy.

## 12.9. **Telephone enquiries**

12.9.1. If a request for information is made over the telephone, the response will be dependant on who is making the request, and what the request is for:

- Individuals making a request for their own personal information must be asked to put their request in writing (email is acceptable).
- An individual making a request under FOI must be asked to put their request in writing (email is acceptable).
- Never release any confidential information over the telephone unless you are entirely sure of the identity of the caller and their entitlement to receive the information. If in doubt, call them back. Further guidance can be found in the NEAS Safe Haven Policy.

## 12.10. **Requests from overseas**

12.10.1. There may be occasions when confidential information is requested from overseas or must be transferred overseas when accompanying a foreign national who may have received treatment from NEAS. Although these will be rare occurrences, procedures must be followed to protect the information. The 8th Data Protection Principle states:

*'Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or Territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data'*

12.10.2. The Act makes allowances for the transfer of medical information to accompany a patient. Ideally, when transferring personal information outside of the EEA, consent should be obtained from the data subject. However, if this is not possible, the following conditions must be satisfied prior to its release:

- The reason for the information request is valid.
- The method of transferring the information is secure.
- Details on how the information will be kept secure by the recipient are supplied and
- There is a documented retention period for the information.

12.10.3. Only when these conditions are satisfied should the information be released.

### **13. Patient Choice**

13.1. It is essential for patients to be informed, in ways they can understand, of the purposes for which information about them is collected and how their information will be shared.

13.2. Patients should be advised how information will be used at the time they are asked to provide it, and should have the opportunity to discuss any aspects that are special to their treatment or circumstances.

#### **13.3. Information leaflets**

13.3.1. Advice about the use of patient information will be made available through the use of newsletters, leaflets and posters displayed in appropriate areas. In particular, the Trusts leaflet "Patient Information and Confidentiality" should be used for this purpose. Such methods however will not be sufficient on their own. Patients should have made available to them the contact details of and who can answer detailed questions about how their information is used. Contact details can be found in the above leaflet.

13.3.2. Advice and information must be presented to patients in a convenient and understandable form. It should be available both for general purposes and before a particular programme of care or treatment begins.

13.3.3. Where patient identifiable information is being used in ways that do not directly contribute to, or support the delivery of their care, patients should be informed of this and the patient's decision to restrict the disclosure of their information is appropriately respected.

#### **13.4. Informing patients**

13.4.1. To ensure we inform patients correctly, the following guidelines should be followed:

- Make clear to patients when information is or may be disclosed to others - staff must ensure that patients know when data is disclosed or used more widely.
- Check that patients are aware of the choices available in respect of how their information may be used or shared.
- Check that patients have no concerns or queries about how their information is used.
- Answer any queries personally or direct patients to others who can answer their questions or other sources of information – if the patients concern cannot be addressed immediately, ensure back-up contacts for further information is provided e.g. PALS, Data Protection Lead, Caldicott Guardian.

- Respect the right of patients to have access to their health records – through access to health records and Data Protection Policy.
- Communicate effectively with patients to help them understand.
- Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of their care.
- Respect patients' decisions to restrict the disclosure and / or use of information.
- Explain the implications of disclosing and not disclosing.

#### **14. Patient Consent**

- 14.1. Where information about patients is required, but does not satisfy the tests of necessity and appropriateness that must govern the use of identifiable patient information, then it should be anonymised to protect the patient.
- 14.2. In all other circumstances efforts must be made to obtain and record consent unless there are statutory grounds for setting confidentiality aside or robust public interest issues.

#### **15. Retention and Storage of Confidential Information**

- 15.1. Records containing personal information should not be kept longer than necessary and should be stored appropriately. Guidance on retention periods and the storage of records for both patient and staff records is provided by the Trust Records Management Policy and the Information Security Policy.
- 15.2. The duty of confidentiality continues right through to the ultimate disposal of information. The Trust operates a Records Retention and Disposal Policy and reference should be made to this document prior to the destruction of any information.

#### **16. Abuse of Privileges and Non Compliance**

- 16.1. It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances without consent. Looking at patient or staff records out of curiosity is totally unacceptable. Disciplinary proceedings may be instigated should abuse of privilege be discovered.
- 16.2. All staff agree to uphold confidentiality on signing of their contract of employment with the Trust. This agreement continues after employment has ceased. Non-compliance with this statement and this code of practice may result in disciplinary action being taken in accordance with the NEAS Disciplinary Procedure.

#### **17. Adverse Incident Reporting**

- 17.1. Possible breaches or risks of breaches of patient confidentiality or other confidential information will constitute an adverse incident and will be reported through the Trust incident reporting

procedure. The Trust risk register will be used to log any identified risks to the confidentiality of information.

## **18. Confidentiality Audits**

### **18.1. Electronic information**

Audits of access to confidential information will be undertaken regularly by the Trust to identify misuse and compliance with this policy. Any incidents of suspected misuse will be fully investigated and may result in disciplinary action.

### **18.2. Manual information**

Each area where confidential information is retained must develop and implement procedures for the regular audit of access to that information.

## **19. Specific Departmental Considerations**

19.1. All staff need to be aware of the confidential nature of information they handle as part of their role. In addition there are specific considerations for certain areas of the Trust.

### **19.2. Operational staff**

19.2.1. Operational staff are the employees who will have the most direct contact with patients and their relatives. Information confided during treatment and / or transportation, whether this is by word of mouth or held in writing, must be kept confidential in accordance with this policy.

19.2.2. On occasions, staff may be required to provide statements to the police with reference to incidents they may have attended. This is acceptable if the police have completed the necessary paperwork (see Police Requests).

19.2.3. Operational staff may be required to obtain evidence of clinical experience to complete their portfolios, in the form of PRFs. If this is the case, staff members may photocopy the original document as long as it is ensured that all patient identifiable details have been blocked off and do not appear in the photocopied document.

### **19.3. Control staff**

19.3.1. Control staff who have contact with patients and their relatives on a day-to-day basis must respect the confidentiality of these individuals at all times. In addition, due to the nature of the functions carried out in the control room, it is also necessary to store information pertaining to operational staff on the CAD system. This information must be handled with the utmost confidentiality.

### **19.4. Human Resources and Occupational Health**

19.4.1. Personnel records and staff occupational health records afford the same level of protection as patient information, as laid down in this policy. All Human Resources staff should respect the privacy of other staff members at all times.

### **19.5. Clinical Audit Staff**

19.5.1. Clinical Audit staff have access to all the patient report forms completed by the operational staff throughout the Trust. As these forms contain a substantial amount of sensitive personal and patient information, these must be treated in accordance with the requirements of this policy.

#### **19.6. PALS and Complaints Staff**

19.6.1. Information handled by the PALS and Complaints staff may contain particularly sensitive information relating to both staff and patients. The confidentiality of this must be maintained at all times. Any disciplinary proceedings brought as a result of a complaint will also be kept strictly confidential.

### **20. Consultation, Approval and Ratification Process**

#### **20.1. Consultation**

20.1.1. This document has been produced by the author on behalf on the IGWG. This group was consulted upon and their comments added to the document as appropriate.

#### **20.2. Approval and Ratification**

20.2.1. The Trust Policy Review Group is the committee with the authority for the review of this document. The Joint Consultative Committee and the ultimately the Trust Board have responsibility for ratification of this policy.

20.2.2. The IGWG has carried out a full and proper consultation and has considered the content of the document in terms of current best practice, guidelines, legislation and mandatory and statutory requirements, in considering the document for approval the committee also took into account the results of the recommendations of the EIA.

### **21. Review and Revision Arrangements**

21.1. The document will be reviewed at least annually or when appropriate after changes in legislation or guidance. The document owner will be responsible for this review.

### **22. Dissemination and Implementation**

#### **22.1. Dissemination**

22.1.1. This policy is available for all staff to access via the Trust Quality System. Staff without computer network access should contact their line manager for information on how to access policies.

22.1.2. All staff will be notified of new or revised documents via internal communications systems.

22.1.3. This document will also be included in the Publication Scheme for NEAS in compliance with the FOI Act 2000.

#### **22.2. Implementation**

22.2.1. This policy will be implemented in the following ways:

- Regular communications to staff on new policies and procedures through Information Governance (IG) circulars.
- Regular audit of IG processes undertaken in line with policies and procedures in key areas i.e. records management, confidentiality, information security, FOI and data quality.
- Monitoring through the Information Governance Toolkit (IGT).

### **22.3. Training**

22.3.1. Training will be regularly assessed and refreshed in order that staff may remain appropriately skilled / knowledgeable over time.

22.3.2. Broad IG training will be included in the Trust induction programme. Additional training can be requested at the discretion of a manager, or by an individual wanting personal development along with mandatory yearly update training.

22.3.3. Further guidance and information relating to data protection issues will be distributed periodically via various media including the intranet site, 'The Pulse' (monthly service journal) and via email.

## **23. Document Control Including Archiving Arrangements**

### **23.1. Register / library of procedural documents**

All documents shall be held within the Trust Quality System and will be managed in line with quality standards.

### **23.2. Archiving arrangement**

Archiving of documents will be in line with the Records Management Policy.

## **24. Monitoring Compliance With and the Effectiveness of Procedural Documents**

### **24.1. Process for monitoring compliance**

24.1.1. All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for data protection.

24.1.2. Failure to follow this policy and related IG policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

24.1.3. Monitoring staff compliance through:

- Verifying that, where appropriate, agreement to disclosure decisions are recorded.
- Obtaining patient feedback of the process, e.g.:
  - Did they understand when and to whom their information would be disclosed?
  - Did they understand the choices available to them regarding disclosure?
  - Did they have the opportunity to ask questions and have them answered?

- Did they understand that withholding of consent does not affect the way they are handled by staff but may reduce the number of treatment options available to them?
- Did they feel under pressure to agree to disclosure?
- Evaluating whether staff understand disclosure issues and their responsibility for obtaining consent.
- Evaluate how staff handled questions about disclosure, and in particular review cases where:
  - Patients have declined to agree to disclosure.
  - Patients have changed their disclosure decision during the care episode.
  - A senior healthcare professional has overridden a non-disclosure decision.

## 24.2. Standards and Key Performance Indicators

There are a number of national standards and requirements relating to IG.

### 24.2.1. IG Toolkit

The connecting for Health IGT is a framework for implementing the IG agenda and consists of a series of requirements against which an organisation's current and planned attainment levels can be monitored. The Trust is required to complete a self assessment by 31st March each year, the results which will contribute to the assessment undertaken by the Healthcare Commission.

### 24.2.2. Standards for Better Healthcare

- The Department of Health's standards for better health include 24 core standards that all NHS healthcare providers in England should achieve, and 13 developmental standards that they should be working towards achieving.
- Core standard 13 requires that health care organisations have systems in place to ensure that:
  - Staff treat patients, their relatives and carers with dignity and respect;
  - Appropriate consent is obtained when required for all contracts with patients and for the use of any patient confidential information; and
  - Staff treat patient information confidentially, except where authorised by legislation to the contrary.

### 24.2.3. NHS Litigation Authority

- The NHSLA Risk Management Standard for Ambulance Trusts applies to all Ambulance Trusts are designed to address organisational, clinical, and non-clinical / health and safety risks.
- Parts of the Clinical Care standard are of relevance to IG, including patient / service user identification and quality of written and electronic clinical records.

## 25. References

- Department of Health NHS IG Guidance on Legal and Professional Obligations.
- NHS Connecting for Health IG Toolkit <https://www.igt.connectingforhealth.nhs.uk/>

## **APPENDIX A: Sharing Information without Consent**

Information can be shared without consent if requested to do so under the following circumstances but service users should usually be informed that disclosure has been required. Whoever authorises disclosure must record the decision so that there is clear evidence of the reasoning used and the circumstances prevailing.

### **1. Prevention of Serious Harm**

Information can be shared if not doing so would risk serious harm to the patient or other individuals.

### **2. Child Protection**

All staff have a duty to assist and provide information in support of Child Protection enquiries. The sharing of information amongst practitioners and other agencies working with children and their families is essential to identifying and safeguarding children at risk of abuse or neglect. Legal and professional obligations do not generally prevent the sharing of confidential information where the public interest in disclosure to safeguard the child's welfare overrides the need to keep information confidential. Where it is necessary to disclose information where abuse or neglect is suspected, the prime duty of staff is to act in the child's best interest. Information should only be disclosed to other professionals or agencies involved in the child's care on a 'need to know' basis.

The Children's Act (1989) and The Protection of Children Act (1999) allow information to be shared if a child is considered at risk. This can include the risk of physical or mental harm; including neglect (see Safeguarding Children Policy). The NEAS is part of the Contact Point collaboration between agencies and families to support the wellbeing of children and young people. Information Sharing Protocols have been developed as part of this collaboration.

### **3. Disclosure to Relatives / Carers**

Disclosures to relatives or carers of patients should generally only be made with explicit consent; however this may not always be possible dependant on the patient's medical condition. Where it is not possible to obtain the consent of the patient to disclose information, staff have a duty to act in the best interests of the patient. Where information is disclosed without consent, a record of the disclosure must be kept including the justification for disclosure without consent.

### **4. Court Orders, including a coroner's court, tribunals and enquiries**

Only give the information requested in the order and no more. Many different Acts give courts the powers to issue court orders.

## **5. General Medical Council (GMC) investigations**

The GMC are entitled to access confidential patient health records as part of an investigation under the Medical Act 1983. The GMC have indicated that they would always try to obtain consent first—refer to the GMC website at <http://www.gmcuk.org/index.htm>.

## **6. Audit Commission investigations**

The Audit Commission are entitled to access confidential patient health records as part of an investigation under section 6 of the Audit Commission Act 1998 (refer to the Audit Commission website at <http://www.auditcommission.gov.uk/>).

## **7. Health Service Ombudsman investigations**

The Ombudsman has the same powers as the courts to require disclosure of person identifiable information. Any request made should be complied with, without obtaining a court order.

## **8. Care Quality Commission audits and inspections**

The Care Quality Commission is the new health and social care regulator for England which regulates health and adult social care services in England <http://www.cqc.org.uk>.

## **9. Public Health and Infectious Diseases notifications**

For details, see Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985.

## **10. Immunisations and vaccinations**

Under the Education Act 1944 information must be passed to NHS Trusts from schools.

## **11. Births and Deaths**

The Births and Deaths Act 1984 provides for the registration of births, stillbirths and deaths.

## **12. Orders under Section 60 of the Health and Social Care Act 2001**

Section 60 of the Health and Social Care Act 2001 provides the Secretary of State for Health with a power to authorise, or require that patient identifiable information is used, to support essential NHS activity, where there is currently no secure basis in law, other than the consent of the patient concerned and it is thought that there are real barriers to seeking or obtaining consent. This power can only be used to support a limited range of purposes that are in the interests of service users or the wider public, where consent is not a practicable alternative and anonymised information will not suffice.

### **13. Requests from Members of Parliament**

Non statutory investigations (e.g. Members of Parliament). If an MP states, in writing that he / she has a service user's consent for disclosure this may be accepted without further contact with the service user, however if in any doubt it may be prudent to contact the service user.

### **14. Prevention and Detection of Crime**

Section 115 of the Crime and Disorder Act 1998 and section 29(3) of the DPA allow for the disclosure of information to aid in the prevention or detection of crime – although the information holder is not legally required to make a disclosure. Serious consideration should be given as to whether the disclosure is in the public interest i.e. if the potential harm from breaching confidentiality outweighs the potential harm of not doing so. However, there is an obligation to share information about a serious crime that has been (or is going to be) committed, such as murder, manslaughter, rape, treason or kidnapping (Police and Criminal Evidence Act 1984) or about suspected terrorism (Antiterrorism, Crime & Security Act 2001 and Terrorism Act 2000).

### **15. Deceased Patients**

The NHS Confidentiality Code of Trust / Practice makes clear that within the NHS the common law duty of confidentiality extends beyond the death of an individual. Access to information relating to deceased patients is governed by the Access to Health Care Records Act 1990. Each individual request for access to records of the deceased must be reviewed and decisions taken to release information must be taken by either the Responsible Medical Officer or the Trust / Practice Caldicott Guardian.

Requests for access under the Access to Healthcare Records Act can only be made by;

- The Patient's personal representative, or
- A person who may have a claim arising out of the patient's death.

The DPA does not apply to deceased patient's records. However, the ethical duty of confidentiality extends beyond the death of the patient, although legislation covering records made since 1 November 1991 (Access to Health Records Act 1990) permits limited disclosure in order to satisfy a claim arising from the death. However, the legislation does not permit the disclosure of information that the patient gave on the understanding that it would not be revealed after his or her death, nor may the results of examinations or investigations be disclosed, which the patient thought would be confidential at the time they were carried out. Where there is no evidence of a refusal to permit disclosure, information necessary to satisfy the claim may be released. In circumstances where there

is no claim, no one can claim a legal right of access to information about a deceased patient, although doctors may consider disclosure to be justifiable, based on the particular circumstances and knowledge of the patient's wishes. In all cases of posthumous disclosure the General Medical Council recommends that the consent of the patient's executor or a close relative, be sought. (Confidentiality, GMC, October 1995).

## **16. Public Interest**

According to the 'Confidentiality: NHS Code of Practice' (2003), the public interest is: 'where exceptional circumstances justify overruling the right of an individual to confidentiality in order to serve a broader societal interest'. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of a free and democratic society in the continued maintenance of an individual's right to confidentiality. Before deciding to share information those making public interest decisions should consult the Caldicott Guardian and any appropriate health professional concerned. The patient should be notified where a decision to disclose in the greater public interest, is to be made or has been made, outlining the reasons for doing so unless there are strong reasons not to do this.

## **17. Incapacitated Adults**

Under current law, no one can provide consent on behalf of another adult. However, under common law, it is generally accepted that decisions about the disclosure of information should be made by those responsible for providing care – in the best interest of the individual. It is also generally accepted that close family and / or guardians should be consulted.

Under the DPA, the rights of individuals who lack capacity to consent are no different from those who do not, except that decisions relating to the disclosure of information may be made by a person who has been appointed by a Court to manage their affairs. From 2007 when fully implemented, the position regarding individuals who lack capacity will be governed by the Mental Capacity Act 2005. See appendix 5 for further information.

## **APPENDIX B: Sharing Information with Implied Consent**

Implied consent will usually be sufficient to allow the sharing of patient information for the purposes of *providing the direct continuing healthcare of a service user*.

### **Definition of *direct continuing healthcare purposes***

The Confidentiality: NHS Code of Practice (Department of Health 2003) defines *Healthcare Purposes* as:

All activities that directly contribute to the:

- Diagnosis.
- Care and treatment of an individual.
- Audit / assurance of the quality of the healthcare provided.
- Social Services (Only as long as the service is involved in the direct healthcare of the service user. The service user must be properly informed of the likely disclosures to non NHS staff and to social workers, otherwise consent will be required).

The Information Commissioner (2002) further defines ***Care and Treatment*** as:

- Routine record keeping, consultation of records etc, in the course of the provision of care and treatment.
- Processing of records in the event of a medical emergency.
- Disclosures made by one health professional or organisation to another, e.g. where a GP refers a patient to a specialist.
- Clinical audit (e.g. the monitoring of a patient care pathway against existing standards and benchmarks), and as the Patient Information Advisory Group (2004) now states: where sharing between different organisations is necessary because more than one organisation has treated that service user, (NHS Trusts only) i.e. Ambulance and Acute Trust, then sharing can take place as long as:
  - The organisation has played a part in delivering care or treatment to that individual.
  - The audit is carried out in accordance with clinical governance guidelines.
  - It has been approved by the medical director and Caldicott Guardian for the Trust in question.

According to Confidentiality: NHS Code of Practice 2003, the use of information for management purposes requires explicit consent. However, this does not include where management requires information to make a decision for the provision of a specific service for the direct continuing healthcare of a service user e.g. information for assessments, individual care plans etc. as long as the service user is properly informed and has not raised any objections with regard to information sharing.

The Department of Health has identified certain situations where explicit consent is required for information sharing that does not directly contribute to direct continuing healthcare of a service user.

**In the following instances, explicit consent will always be required unless there is a robust public interest in favour of releasing information without consent:**

### **1. NHS Complaints Committees**

Complaints committees will invariably need patient information. However, explicit consent of the complainant, and any other patients whose records may need to be reviewed, is required prior to disclosure.

### **2. Management Purposes**

Commissioning, prescribing advisors, financial audit, resource allocation etc, no restrictions are imposed if the data is anonymised. The explicit consent of patients must be sought for information about them to be disclosed for these purposes in an identifiable form, unless disclosure is exceptionally justified in the public interest, or has temporary support in law under section 60 of the Health & Social Care Act 2001.

### **3. Occupational Health Professionals**

Information on staff referred to occupational health departments. However, if clinicians are the patients, the powers of professional regulatory bodies for disclosure may apply.

### **4. Researchers**

The use of anonymised data is preferable for research purposes. Where systems that are capable of providing anonymised data sets for researchers do not yet exist, the use of identifiable patient information to support research may well be appropriate and necessary but normally requires explicit patient consent. Whilst patients are generally aware and supportive of research it is not reasonable to assume that they are aware of and consent to each and every research subject or proposal. All research in the NHS or other research involving NHS patients, their tissue and / or data must meet appropriate standards of research governance, including ethical approval from an appropriate ethics committee – a mandatory requirement for all NHS supported research.

If a patient cannot be contacted to obtain consent, it should not be assumed that their medical details can be used for research purposes. In some exceptional circumstances, where the research subject

is of such significance or a patient cannot be located in order to seek consent, the public interest may justify disclosure.

Where explicit consent has not been gained and the public interest does not justify breaching patient confidentiality, the research project needs support under section 60 of the Health & Social Care Act 2001. The Patient Information Advisory Group (PIAG) Secretariat can help clarify uncertain cases.

## **5. Teaching**

According to the Confidentiality: NHS Code of Practice; teaching is not to be regarded as direct healthcare purposes and will require explicit consent.

## **6. Sure Start Teams**

Disclosures to Sure Start teams for anything, other than the direct continuing healthcare of young children, needs explicit consent from those with parental responsibility.

## **7. Hospital Chaplains**

When a service user is unable to give explicit consent because they are unconscious, the decision rests with the healthcare professional treating the service user. Care should be taken to restrict the amount of information disclosed to 'what is necessary' in the service user's best interests, and, where appropriate, listening to the views of relatives before making a decision to share or not to share.

## **8. The Media**

You need explicit consent to release information to the media about care and treatment (including a service user's presence in a hospital) unless there is an *exceptional robust public interest* in releasing information. All media requests for information should be referred to the PR department at Ambulance Headquarters.

## **9. Police**

Information required by the Police usually needs explicit consent of the service user or a Court Order. However, disclosure is also justified for the purposes of the prevention and detection of crime (Section 115 of the Crime and Disorder Act 1998 / Section 29(3) of the DPA) e.g. requests from the Police where someone is suspected of committing a serious crime.

- If you believe someone has committed a crime, the Crime and Disorder provisions in section 115 of that Act state you can share this information with the police. However, this legislation does not enforce you to do so.

- DPA (the Act), section 29(3) provides that the nondisclosure rules will not apply if information sharing is required for: the prevention or detection of crime, the apprehension or prosecution of offenders or the collection or assessment of any tax or duty. (The police may request information under section 29(3) of the Act).

## **10. Solicitors**

Solicitors requesting service user information must produce an up to date written, signed consent from the service user, before any information should be released. If you have any doubts as to the authenticity of the consent or the fact that the whole of the service user's record has been requested, contact the service user direct – you must obtain consent from any third parties before releasing third party information. Further information can be found in the Data Protection Policy.

## **11. Insurance Companies and Genetic information**

The paper Concordat and Moratorium on Genetics and Insurance effective from 14<sup>th</sup> March 2005 states that patients do not have to disclose predictive genetic tests results when applying for insurance cover unless required to do so under certain conditions. Care should be taken so that accidental disclosure of this information is avoided when insurance companies request medical reports in relation to an insurance policy to be taken out by a service user.

## **APPENDIX C: Statutory Restrictions on Disclosure**

NHS (Venereal Diseases) Regulations 1974 and the NHS Trust (Venereal Diseases) Regulations 1991 prevent the disclosure of any identifying information about a patient with a sexually transmitted

disease, including HIV and AIDS, other than to a medical practitioner (or to a person employed under the direction of a medical practitioner) in connection with and for the purpose of the treatment of the patient, or to prevent the spread of disease. The regulations do not prevent the normal notification of other communicable diseases in such patients.

The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertility and Embryology (Disclosure of Information) Act 1992, limits the circumstances in which information may be disclosed by centres licensed under the Act.

The Abortion Regulations 1991, made under the Abortion Act 1967, limit and define the circumstances in which information submitted under the Act to the Chief Medical Officer may be disclosed.

## **APPENDIX D: Mental Capacity Act 2005**

The Mental Capacity Act 2005 provides a statutory framework to empower and protect vulnerable Adults who are not able to make their own decisions. It makes clear who can take decisions, in which situations, and how they should go about this. It deals with decisions made on behalf of a person

lacking capacity by those acting formally under an order of the Court of Protection, by designated decision makers under a Lasting Power of Attorney and decisions and actions taken by people without formal powers in matters of day to day care. The legislation is not applicable to those under the age of 16.

The Act is underpinned by a set of five principles:

1. A person must be assumed to have capacity unless it is established that he lacks capacity.
2. A person is not to be treated as unable to make a decision unless all practicable steps to help him to do so have been taken without success.
3. A person is not to be treated as unable to make a decision merely because he makes an unwise decision.
4. An act done, or decision made, under this Act for or on-behalf of a person who lacks capacity must be done, or made, in his best interests.
5. Before the act is done, or the decision is made, regard must be had to whether the purpose for which it is needed can be as effectively achieved in a way that is less restrictive of the person's rights and freedom of action.

The Act covers decisions made, or actions taken, on behalf of people lacking capacity, whether they relate to day-to-day matters or represent major life changing events. These decisions can range from choosing what to wear, what to eat, etc to decisions about minor medical issues such as attending a routine dental check up to more major decisions such as whether the person should move into residential care or undertake a major surgical operation.

The Act establishes legal rules which apply to everyone working with and / or caring for adults who lack capacity. This includes relatives, professionals and other carers. Within the NHS and Social Care any professional, such as Doctors, Nurses, Paramedics or Social Workers, have a duty to have regard to the legislation and associated Code of Trust / Practice when making any judgements as to whether an individual has the capacity to consent to any action or decision that is to be made regarding their care. The underlying philosophy of the Act is to ensure that individuals who lack capacity are the focus of any decisions made, or actions taken, on their behalf. The interests of the person who lacks capacity should prevail; not the views or convenience of those caring for that person.

Mental Capacity means the ability to make decisions or take actions affecting daily life, which may have consequences for the individual or for other people. The Act provides that the starting point should be a presumption of capacity, i.e. that when looking at an individuals ability to make a decision that they do have that capacity and that only after an assessment of capacity has taken place should their decisions be made for them. In legal proceedings, the burden of proof will fall on any person who

asserts that capacity is lacking. For the purposes of the Act, "...a person lacks capacity in relation to a matter if at the material time he is unable to make a decision for himself in relation to the matter because of an impairment or, or a disturbance in the functioning of, the mind or brain."

"...a person is unable to make a decision for himself if he is unable –

- (a) To understand the information relevant to the decision;
- (b) To retain that information;
- (c) To use or weigh that information as part of the process of making the decision or
- (d) To communicate his decision."

Prior to an individual's decisions being made for him, his capacity to make decisions must be formally tested, as defined by Section 3 of the Act.

Section 5 of the Mental Capacity Act identifies the rules in relation to acts or decisions that are taken concerning a person who lacks capacity. Section 5 applies both to informal carers (family members) formal carers (those paid for providing care) and health and social care professionals. It related specifically to certain acts in connection with the personal care, healthcare or medical treatment of a person lacking capacity to consent to these acts.

The provisions within the legislation are intended to give legal backing, in the form of protection from liability, for actions considered to be in the best interests of someone who lacks capacity. Within the provision of healthcare, many acts are undertaken by both professionals and carers. Which could be deemed unlawful unless the person affected has given permission. This creates a problem where that person lacks the capacity to give consent. For example; if a person lacks the ability to dress themselves, the individual who undertakes this act for them is potentially committing assault in touching their person without their consent. The purpose of Section 5 is to ensure that when people need to perform such acts, they ensure that they do so only in the context of the legislation.

The types of action which may be permitted under Section 5 are those carried out in connection with the care or treatment of a person who is believed to lack capacity. For example:

- Acts in connection with personal care, such as giving assistance with attending to personal hygiene, or,
- Acts in connection with health care and treatment, such as diagnostic examinations and tests, medical and dental treatment or nursing care. Where no advance decision to refuse treatment is in place.

To ensure that individuals who undertake these acts benefit from the protection from liability that Section 5 of the Act provides, they must ensure that they have taken reasonable steps to ascertain whether the person concerned has capacity in relation to the action and if having determined that they do not have the capacity ensuring that there are reasonable grounds for believing that the action taken will be in the person's best interests. In all cases, the least restrictive option must be considered in accordance with Section 1 of the Act. Section 5 however does not provide a defence to negligent acts. Whilst Section 5 would, for example, protect a Doctor who performs an operation which is in the person's best interests, even though the person lacks the capacity to consent. It would not provide any protection were that operation to be carried out negligently.

In addition to this, Section 6 of the Act imposes limitations on this protection. No protection is offered where there has been use or a threat to use violence in order to carry out any action in connection with the care of treatment of a person lacking capacity. Many of the provisions of the Act are based upon existing Common Law principles. The Act seeks to clarify and build upon these existing principles and build upon current good Trust / Practice which has derived from them. In particular, the Act clarifies and expands the position regarding Power of Attorney which in the past has been unclear as to the extent of its provisions, and expanding the provisions to include decisions relating to a persons welfare.

Prior to the Mental Capacity Act, powers to act on the behalf of an individual / donor were defined in the Enduring Powers of Attorney Act 1985. This act allowed the Attorney / Donee to act on behalf of the donor in relation to property and financial affairs. The Mental Capacity Act introduces a new form of power of attorney called the Lasting Power of Attorney. This extends the areas in which an individual can authorise others to make decisions for them in the event of them losing capacity. In addition to property and finance, an individual can now choose to delegate decisions affecting their personal welfare, including healthcare and consent to medical treatment. It is important to note, that a Lasting Power of Attorney can only be created when the individual to whom it relates has capacity. Where an individual already lacks capacity, this will fall under the Court of Protection and Court-Appointed Deputies. The Mental Capacity Act establishes a specialised court, with jurisdiction to deal with decision-making for adults who lack capacity. This new Court of Protection takes over the role and functions of the former Court of Protection. The Court of Protection will deal with serious decisions affecting healthcare and personal welfare matters of those who lack capacity, and is supported in its role by the Office of the Public Guardian. The Court of Protection will provide a judicial forum or last resort to deal with complex decisions or disputes which cannot be resolved in any other way, and would previously have been dealt with by the High Court. Where the Court believes that there is a need for on-going decision-making powers for a person lacking capacity, it may appoint a deputy to act for and make such decisions on behalf of the person.

Sections 35 – 39 of the Mental Capacity Act establishes an Independent Mental Capacity Advocate Service, and provides additional safeguards for vulnerable people who lack capacity and also lack contact with individuals who can help to protect their interests, such as close relatives. Regulations, yet to be produced, will identify the categories of people who will qualify for the additional safeguards and will also identify the obligations placed on NHS bodies to consult with and take account of the advice of Independent Mental Capacity Advocates. The functions and role of the Independent Mental Capacity Advocates will be set out in these regulations, however, it is expected that their role will be to provide advice on what is in the vulnerable person's best interests.

Section 37 of the Act places a duty on NHS bodies to instruct an advocate to represent the patient, in those circumstances where it wishes to provide or secure the provision of serious medical treatment and it is satisfied that there is no person whom it would be appropriate to consult in determining the best interests of the patient before the treatment is provided, except where it needs to be provided as a matter of urgency.

Health Professionals are required to respect a competent patients' autonomy to make decisions in relation to the treatment they receive. Competent individuals have a legal right to refuse medical procedures or treatment. Section 24 of the Mental Capacity Act establishes in statute the capacity of adults aged 18 or over to make advanced decisions to refuse medical treatment. The Act provides important safeguards to ensure the validity and applicability of advance decisions. For example by requiring that the advance decision identifies specific treatments and that the patient is not capable of making the decision at the time. For example, a Jehovah's Witness makes an advance decision to refuse blood transfusions. The advance decision is only applicable if the treatment that is proposed is a blood transfusion and the patient is not capable of making a decision at the time. The medical professional in withholding the blood transfusion in line with the advanced decision would not be held liable for any consequences of that action.

Individuals who make decisions on behalf of those who lack capacity will need to have access to personal information relating to the person lacking capacity so that they may act in that person's best interests. Decisions and actions cannot be carried out properly without the person making the decision using information about the individual who lacks capacity. However, unrestricted access to sensitive personal information is neither acceptable nor lawful and those disclosing information relating to someone who lacks capacity must ensure that they follow the requirements of the DPA, The Common Law Duty of Confidentiality and the NHS Confidentiality Code of Trust / Practice. Individuals disclosing information must be assured that they are acting lawfully and also that such disclosures are justified. It should also be remembered that whilst an individual may not have the capacity to make complex

decisions in relation to their healthcare, they may be perfectly capable of making the decision to allow disclosure of their personal information.