REF: IG 01

VERSION: 4.0

North Cumbria University Hospitals NHS Trust

Confidentiality Code of Practice

SUMMARY & AIM

This document is a guide to required practice for all staff who work within or under contract to North Cumbria University Hospitals NHS Trust, concerning confidentiality and patient consent to the use of their information.

It defines the confidentiality code of conduct that will apply to all staff and it provides a general summary of applicable law and Trust policies.

TARGET AUDIENCE:

- This code of practice applies to all staff working for North Cumbria University Hospitals NHS Trust irrespective of whether they are full-time, part-time or voluntary staff. It also applies to any third-party contractors working for or at the Trust.

TRAINING:

- Information Governance training which includes confidentiality, is provided to all members of staff at their induction, followed by the Trust's Statutory and Mandatory training (either Workbook or Online) which also covers Information Governance issues. This must be completed by all staff on an annual basis.

EVIDENCE OF IMPLEMENTATION:

- An information incident report, which includes breaches of confidentiality, is submitted to the Information Governance Group on a quarterly basis. The report is generated from incidents recorded through the Trust's incident reporting system (Ulysses).
- The Information Governance Group ensure that an action plan is in place for any deficiencies identified and actions are monitored on a regular basis until they have been completed.

KEY REQUIREMENTS

1. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

2. Information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent.

3. Confidential information can be anything that relates to patients, staff their family or friends, however stored.

4. The four main requirements of the Department of Health's Confidentially Code of Practice are:

   - **Protect** – look after the patient's information
   - **Inform** – ensure that patients are aware of how their information is used
   - **Provide Choice** – allow patients to decide whether their information can be disclosed or used in particulars ways
   - **Improve** – always look for better ways to provide these requirements

DOCUMENT CONTROL

Author/Contact	Information Governance Officer Tel: 01228 602186 Email: anne.gadsden@ncuh.nhs.uk
Executive Director	Director of Finance
Equality Impact Assessed	01/03/2011
Version	4.0
Status	Approved
Publication Date	15/04/2014
Review Date	30/04/2017

Approved by: -

Information Governance Group	Date: 14/02/2014
Trust Policy Group	Date: 28/03/2014
Safety and Quality Committee (for noting)	Date: 08/04/2014

Please note that the Intranet version of this document is the only version that is maintained.
Any printed copies should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Approved documents related to this policy

Name Policy	Document Reference / Hyperlink
Data Protection Policy	http://nww.staffweb.cumbria.nhs.uk/policies/categories/information-governance/data-protection-policy.pdf
E-mail Policy	http://nww.staffweb.cumbria.nhs.uk/policies/categories/information-governance/email-policy.pdf
Safe Haven Procedure	http://nww.staffweb.cumbria.nhs.uk/policies/categories/information-governance/safe-haven-procedure.pdf
Statement Writing Guidelines	http://nww.staffweb.cumbria.nhs.uk/policies/categories/governance/statement-writing-guidelines.pdf
Disciplinary Procedure	http://nww.staffweb.cumbria.nhs.uk/policies/categories/human-resources/disciplinary-procedure.pdf

Statement of changes made

Version	Date	Changes made from previous version
3.0	19/04/2011	Published
3.1	10/10/2013	Put in to current policy template
3.2	03/02/2014	Removed all references to 'Department of Health Care Record Guarantee'. Added responsibilities for CEO, SIRO, DPO, Caldicott Guardian to Section 5. Information

		Governance Group responsibilities amended (Section 5.6) and new monitoring section added (Section 8). Addition of abbreviations to Section 3
3.3	12/02/2014	Amended Caldicott principles in S6.2.7 to include principle 7
3.4	14/02/2014	Amended following IG Group meeting: • Moved 'Definition of terms' to Appendix 3 • Minor amendment to S5.6 to provide clarity of the process in place
3.5	02/04/2014	Amended following Trust Policy Group meeting: • Section 7 'health & safety training' changed to 'statutory and mandatory training' • Addition of hyperlinks to 'approved documents'

List of Stakeholders who have reviewed the document

Name	Job Title	Date
Paul Wiggins	Deputy Director IM&T and Data Protection Officer	04/02/2014
Graham Putnam	Consultant OMFS and Caldicott Guardian	04/02/2014
Steve Shanahan	Director of Finance, and Senior Information Risk Owner	04/02/2014
	Information Governance Group	14/02/2014

SUMMARY

This document is a guide to required practice for all staff who work within or under contract to North Cumbria University Hospitals NHS Trust, concerning confidentiality and patient consent to the use of their information.

TABLE OF CONTENTS

1. INTRODUCTION

Patients have different needs and values – this has to be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information. Patients have the right to choose whether or not to accept a form of care and the information disclosure needed to provide that care, and to choose whether or not information that can identify them can be used for non-healthcare purposes.

The disclosure of information even for health care purposes cannot be taken for granted, and patients must be given opportunities to raise objections and concerns. The development of a truly confidential service will maximise patient trust and minimise the number of objections raised. While it is necessary to 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.

2. PURPOSE OF THE DOCUMENT

This document defines the confidentiality code of conduct that will apply to all staff during the course of their work within North Cumbria University Hospitals NHS Trust. It provides a general summary of applicable law and Trust policies.

3. DEFINITION OF TERMS USED / ABBREVIATIONS

CSSR	Councils with Social Service Responsibilities
PID	Personally Identifiable Data
IM&T	Information Management and Technology
NHS	National Health Service
SIRO	Senior Information Risk Owner

(Further definitions in Appendix 3)

4. SCOPE

This code of practice applies to all staff working for North Cumbria University Hospitals NHS Trust irrespective of whether they are full-time, part-time or voluntary staff. It also applies to any third-party contractors working for or at the Trust.

5. DUTIES (ROLES & RESPONSIBILITIES)

5.1 The Chief Executive Responsibilities

The Chief Executive has ultimate responsibility for ensuring that the appropriate Information Governance policies and procedures are in place and enacted accordingly.

5.2 Director of Finance and Senior Information Risk Owner (SIRO) Responsibilities

The Senior Information Risk Owner (SIRO) is responsible to the Chief Executive and the Trust Board of Directors for the development and implementation of the Information Governance policy and procedures, act as an advocate for Information Governance on the Board and in internal discussions.

5.3 The Caldicott Guardian Responsibilities

The Caldicott Guardian is appointed by the Trust Board to oversee the safe and secure use and sharing of patient information. The Caldicott Guardian will take a lead role in respect of Clinical Information Assurance Requirements.

5.4 The Deputy Director of IM&T and Data Protection Officer Responsibilities

The Deputy Director of IM&T and Data Protection Officer is responsible to the SIRO for the operational management of data protection, the confidentiality code of conduct, information security and for ensuring that the Trust complies with all legal requirements in respect of its processing of Personally Identifiable Data (PID), including security and legal compliance Requirements. He is responsible for the preparation of the annual Improvement Plan to ensure compliance with the Requirements, assigning management leads, monitoring progress and producing reports to the Information Governance Group and Governance & Quality Committee.

5.5 Staff Responsibilities

All Trust Staff and contractors acting for the Trust have a statutory duty of confidentiality to protect patient information and only use it for the purposes for which it was intended.

All staff and contractors have a duty to

- Conform to System Security Policies and Security Operating Procedures
- Be aware of their security responsibilities
- Attend suitable security training when arranged
- Safeguard hardware, software and information in their care
- Prevent the introduction of malicious software on the organisation's IT systems
- Report on any suspected or actual breaches in security

5.6 Information Governance Group Responsibilities

The Information Governance Group is responsible for reporting to the Safety and Quality Committee of the Trust Board via its minutes with regard to

serious risks identified through the code of practice monitoring arrangement (see Section 8).

6. CODE OF PRACTICE

6.1 Confidential Patient Information

6.1.1 Duty of Confidence

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence.
It: -

- is a legal obligation that is derived from case law
- is a requirement established within professional codes of conduct
- is part of NHS employment contracts as a specific requirement linked to disciplinary procedures

Patients entrust us with, or allow us to gather, sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately. In some circumstances patients may lack the competence to extend this trust, or may be unconscious, but this does not diminish the duty of confidence.

It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

A key guiding principle is that a patient's health records are made by the health service to support that patient's healthcare.

One consequence of this is that information that can identify individual patients, must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, some other legal basis, or where there is a robust public interest or legal justification to do so. In contrast, anonymised information is not confidential and may be used with relatively few constraints.

Patient information is generally held under legal and ethical obligations of confidentiality. Information provided in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule, but it applies in most circumstances.

6.1.2 Disclosing and using confidential patient information

It is extremely important that patients are made aware of information disclosures that must take place in order to provide them with high quality

care. In particular, clinical governance and clinical audits, which are wholly proper components of healthcare provision, might not be obvious to patients and should be drawn to their attention. Similarly, whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be obvious to them, and efforts made to inform them should reflect the breadth of the required disclosure.

This is particularly important where disclosure extends to non-NHS bodies. Many current uses of confidential patient information do not contribute to or support the healthcare that a patient receives. Very often, these other uses are extremely important and provide benefits to society – e.g. medical research, protecting the health of the public, health service management and financial audit. However, they are not directly associated with the healthcare that patients receive and we cannot assume that patients who seek healthcare are content for their information to be used in these ways.

6.1.3 Patient consent to disclosing

Patients generally have the right to object to the use and disclosure of confidential information that identifies them, and they need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options.

Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment.

Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

Where patients have been informed of: -

- the use and disclosure of their information associated with their healthcare;

  and

- the choices that they have and the implications of choosing to limit how information may be used or shared;

Then explicit consent is not usually required for information disclosures needed to provide that healthcare. Even so, opportunities to check that patients understand what may happen and are content should be taken. Special attention should be paid to the issues around child consent (see appendix 1).

Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information must be considered.

6.2 Detailed Provisions

All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust.

6.2.1 Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including non-contract, volunteers, bank and agency staff, locums, student placements), their family or friends, however stored.

Patient identifiable information includes:

- patient's name, address, full post code, date of birth
- pictures, photographs, videos, audio-tapes or other images of patients
- NHS number and local patient identifiable codes
- anything else that may be used to identify a patient directly or indirectly.

It includes information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras.

It can take many forms including medical notes, audits, employee records, occupational health records etc.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy).

During your duty of work you should consider all information to be sensitive, even something as simple as a patients name and address. The same standards must be applied to all information you come into contact with.

Records made about patient care are disclosable in law. It is therefore important that record keeping is of a consistently high standard (see appendix 2).

6.2.2 The Confidentiality Model

The Department of Health has defined a model to outline the four main requirements that must be met to provide patients with a confidential service (Department of Health: Confidentiality: NHS Code of Practice (November 2003)

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253)

The four main requirements are:

- **Protect** – look after the patient's information
- **Inform** – ensure that patients are aware of how their information is used
- **Provide Choice** – allow patients to decide whether their information can be disclosed or used in particulars ways
- **Improve** – always look for better ways to provide these requirements

6.2.3 Protect Patient Information

Patients' health information and their interests must be protected through a number of measures:

- Recognising that confidentiality is an obligation for all staff, external contractors, and volunteers.
- Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality.
- Recording patient information accurately and consistently;
- Keeping patient information private;
- Keeping patient information physically secure;
- Disclosing and using information with appropriate care.
- Follow any established information sharing protocols.
- Identify enquirers, so that information is only shared with the right people.
- Ensure that appropriate standards are applied in respect of e-mails, faxes and surface mail
- Share the minimum necessary to provide safe care or satisfy other purposes.

6.2.4 Inform Patients Effectively

Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support clinical audit and other work to monitor the quality of care provided.

Consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then they are not being effectively informed.

In order to inform patients properly, staff must:

- check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood

- make clear to patients when information is recorded or health records are accessed
- make clear to patients when they are or will be disclosing information with others
- check that patients are aware of the choices available to them in respect of how their information may be disclosed and used
- check that patients have no concerns or queries about how their information is disclosed and used
- answer any queries personally or direct the patient to others who can answer their questions or other sources of information
- respect the rights of patients and facilitate them in exercising their right to have access to their health records
- Communicate effectively with patients to help them understand.

6.2.5 Provide Choice to Patients

Patients have different needs and values – this must be reflected in the way they are treated, both in terms of their medical condition and the handling of their personal information.

What is very sensitive to one person may be casually discussed in public by another – just because something does not appear to be sensitive does not mean that it is not important to an individual patient in his or her particular circumstances.

Staff must:

- 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
- ensure patients understand what the implications may be if they chose to agree to or restrict the disclosure of their information

6.2.6 Improve Wherever Possible

It is not possible to achieve best practice overnight. Staff must:

- Be aware of the issues surrounding confidentiality, and seek training or support where uncertain in order to deal with them appropriately
- Report possible breaches or risk of breaches

6.2.7 Use the Caldicott Principles

1) Justify the purpose
2) Don't use patient identifiable information unless it is absolutely necessary
3) Use the minimum necessary patient identifiable information

4) Access to patient identifiable information should be on a strict need to know basis
5) Everyone should be aware of their responsibilities
6) Understand and comply with the law
7) The duty to share information can be as important as the duty to protect patient confidentiality

6.2.8 Non-compliance with the code of practice

Non-compliance with this code of practice by any person working for the Trust may result in disciplinary action being taken in accordance with the Trust's disciplinary procedure.

7. IMPLEMENTATION AND TRAINING REQUIREMENTS

Information Governance training (including confidentiality) is provided to all members of staff at their induction, followed by the Trust's Statutory and Mandatory training (either Workbook or Online) which also covers Information Governance issues.

8. PROCESS FOR MONITORING COMPLIANCE WITH PROCEDURE

The process for monitoring compliance with the effectiveness of this policy is as follows:

Monitoring/audit arrangements	Methodology	Reporting		
		Source	Committee	Frequency
An information incident (including breaches of confidentiality) report	Incidents recorded through the Trust's incident reporting system	Information Governance Officer / Information Security Officer	Information Governance Group	3-monthly

Wherever the above monitoring has identified deficiencies, the Information Governance Group ensures that an action plan is in place, and progress of the action plan is monitored by IGG. Serious risks are considered by IGG for inclusion in the appropriate risk register.

9. REFERENCES

- Common Law Duty of Confidentiality
- Data Protection Act 1998
  http://www.legislation.gov.uk/ukpga/1998/29/contents
- Human Rights Act 1998
  http://www.legislation.gov.uk/ukpga/1998/42/contents
- Health & Social Care Act 2001:s60
  http://www.legislation.gov.uk/ukpga/2001/15/contents

- The Human Fertilisation and Embryology Act 1990 - as amended by the Human Fertilisation and Embryology Act (Disclosure of Information) Act 1992 http://www.legislation.gov.uk/ukpga/1990/37/contents
- Mental Capacity Act 2005 http://www.legislation.gov.uk/ukpga/2005/9/contents
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000 http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsLegislation/DH_4083027
- The Abortion Regulations 1991 http://www.legislation.gov.uk/uksi/1991/499/contents/made
- Computer Misuse Act 1990 http://www.legislation.gov.uk/ukpga/1990/18/contents
- Department of Health: Confidentiality: NHS Code of Practice (November 2003) http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253
- Disability Discrimination Act 1995 http://www.legislation.gov.uk/ukpga/1995/50/contents

APPENDIX 1 CONSENT ISSUES

(From Department of Health – Confidentiality Code of Practice Section B)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

2.1 Competence to consent (to use of information)

Seeking consent may be difficult, either because patients' disabilities or circumstances have prevented them from becoming informed about the likely uses of their information, or because they have a difficulty in communicating their decision (be it to consent or object)

In the former case, extra care must be taken to ensure that information is provided in a suitable format or language that is accessible (e.g. providing large print or Braille versions of leaflets for those with reading difficulties) and to check that it has been understood.

In the latter case, it will be important to check for a clear and unambiguous signal of what is desired by the patient, and to confirm that the interpretation of that signal is correct by repeating back the apparent choice.

Failure to support those with disabilities could be an offence under the Disability Discrimination Act 1995 and Equality Act 2010, and may prevent consent from being gained.

2.2 Children and young people

Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidentiality as adults. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to make decisions about the use and disclosure of information they have provided in confidence (e.g. they may be receiving treatment or counselling about which they do not want their parents to know).

However, where a competent young person or child is refusing treatment for a life threatening condition, the duty of care would require confidentiality to be breached to the extent of information those with parental responsibility for the child who might then be able to provide the necessary consent to the treatment.

In other cases, consent should be sought from a person with parental responsibility if such a person is available. It is important to check that person has proper authority (as parent or guardian). Any unusual arrangements should be noted in the child's health record.

2.3 Where patients are unable to give consent

If a patient is unconscious or unable, due to a mental or physical condition, to give consent or to communicate a decision, the health professionals concerned must take decisions about the use of information. This needs to take into account the patient's best interests and any previously expressed wishes, and be informed by the views of relatives or carers as to the likely wishes of the patient. If a patient has made his or her preference about information disclosures known in advance, this should be respected.

Sometimes if may not be practical to locate or contact an individual to gain consent. If this is well evidenced and documented and anonymised data is not suitable, the threshold for disclosure in the public interest may be lessened where the likelihood of detriment to the individual concerned is minimal. Where explicit consent cannot be gained and the public interest does not justify breaching confidentiality, then support would be needed under Section 60 of the Health and Social Care Act 2001.

Where the patient is incapacitated and unable to consent, information should only be disclosed in the patient's best interest, and then only as much information as is needed to support their care. This might however, cause unnecessary suffering to the patient's relative, which could in turn cause distress to the patient when they later learned of the situation. Each situation must be judged on its merits, and great care taken to avoid breaching confidentiality or creating difficulties for the patient. Decisions to disclose and the justification for disclosing must be noted in the patient's health record. Focussing on the future and care needs rather than past records will normally help avoid inappropriate disclosures.

Such circumstances will usually arise when a patient has been unable to give informed consent to treatment, and, provided the patient has not objected, this may justify the disclosure of some information with relatives in order to better understand the patient's likely wishes. There may also be occasions where information needs to be shared with carers in order to assess the impact of disclosures to the patient him or herself. Such occasions are rare and justifiable only in the best interests of the patient.

Patients are often asked to indicate the person they would like to be involved in decisions about their care should they become incapacitated. This will normally, but not always, be the 'next of kin'. It should be made clear that limited information will be shared with that person, provided the patient does not object. This gives patients the opportunity to agree to disclosure or to choose to limit disclosure, if they so wish.

2.4 Explicit consent for the use of a patient's information

When seeking explicit consent from patients for the use of their information, the approach must be to provide:

- honest, clear, objective information about information uses and the patient's choices – this information must be multi-layered, allowing patients to seek as much detail as they require
- an opportunity for patients to talk to someone they can trust and of whom they can ask questions
- reasonable time (and privacy) to reach decisions
- support and explanations about any form that they may be required to sign
- a choice as to whether to be contacted in the future about further uses, and how such contacts should be made; and
- evidence that consent has been given, either by noting this within a patient's health record or by including a consent form signed by the patient.

The information provided must cover:

- a basic explanation of what information is recorded and why, and what further uses may be made of it
- a description of the benefits that may result from the proposed use or disclosure of the information
- how the information and its future uses will be protected and assured, including how long the information is likely to be retained, and under what circumstances it will be destroyed; any outcomes, implications, or risks, if consent is withheld (this must be honest, clear and objective – it must not be or appear to be coercive in any way); and
- an explanation that any consent may be withdrawn in the future (including any difficulties in withdrawing information that has already been shared)
- The information provided must allow for disabilities, illiteracy, diverse cultural conditions and language differences

2.5 The right to withhold or withdraw consent for use of information

Patients do have the right to object to information they provide in confidence being disclosed to a third party in a form that identifies them, even if this is someone who might provide essential health care. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision has to be respected. This is no different from a patient exercising their right to refuse treatment.

There are a number of things to consider if this circumstance arises:

a. The concerns of the patient must be clearly established and attempts made to establish whether there is a technical or procedural way of satisfying their concerns without unduly compromising care.
b. The options for providing an alternative form of care or to provide care through alternative arrangements must be explored.

c. Decisions about the options that might be offered to the patient have to balance the risks, staff time and other costs attached to each alternative that might be offered, against the risk to the patient of not providing health care.

Every effort must be made to find a satisfactory solution. Careful documentation of the decision making process and the choices made by the patient must be included within the patient's health record.

APPENDIX 2 KEY PRINCIPLES OF RECORD KEEPING

Records made about patient care are disclosable in law. It is therefore important that record keeping is of a consistently high standard. Additionally, records are disclosable to patients and should be written, wherever possible, with the involvement of the patient or carer (if appropriate). Records must be understandable using plain English, without abbreviations, wherever possible.

Records must be:

- **Objective**. Use precise, non-emotive language and avoid subjective 'casual' remarks and abbreviates that might not be understood.
- **Contemporaneous.** Write as soon as possible after the event has occurred (contemporaneously), providing current information on the care and condition of the patient.
- **Accurate.** All records must be dated, timed and signed with the name printed next to the first signed entry. Ensure that the year that entries relate to is clearly stated.
- **Clear**. Records must be legible and written clearly in language that can be understood by the patient or in a court of law. They should be written in such a manner that the text cannot be erased (indelible). Draw a single line through any incorrect entries. Annotate the error with your initials. Make a note in the margin that the entry was made in error, and note what the correct entry should be Date and time your annotation. Never erase or use Tipp-Ex / white-out liquid. Do not include abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements
- **Readable.** Your records must be readable on photocopy. Use only Trust approved ink. Black, blue and red are Trust approved ink colours.
- **Understandable**. Written in terms that the patient can understand
- **Logical**. Written and filed in consecutive / chronological order. Do not skip lines or leave blank spaces
- **Timely.** Discharge letters and clinical letters following Outpatients attendance (i.e. ones that will be sent from the hospital to other healthcare staff) should be timely, neat and accurate.
- **Auditable.** Health records are audited on a regular basis.

Your record keeping should also:

- Ensure that correct patient identification is continued throughout the health records.
- Identify the source of referral of the patient (which general practitioner, hospital consultant etc.)
- Provide clear evidence of the care planned, the decision made, the care delivered and the information shared.
- Identify problems that have arisen and the action taken to rectify those problems.

- Provide evidence that notes / key points are made about relevant conversations with the family or friends of the patient (e.g. discussions about consent to treatment, risks and options available)
- Note that all relevant discharge information has been provided at the time of discharge.
- Evidence that you have understood and honoured your duty of care, that you have taken all reasonable steps to care for your patient and that any actions or omissions on your part have not compromised their safety in any way
- Provide a record of any arrangements you have made for the continuing care of a patient
- Evidence that printed test results have been signed by the doctor to confirm s/he has read them
- Record any information you have given to the patient before they have made the decision to sign or any consent for; this helps ensure that you have informed consent
- Demonstrate that Consent Forms are signed by the patient after the treatment has been discussed with the doctor and that the patient is given / offered a copy of the consent form.
- Record any adverse reaction or problems including drug allergies on: prescription charts, health records and head sheets / treatment sheets. Also record any other allergies e.g. to latex on the alert forms provided in the health records.

See also: Guidelines on Statement Writing

APPENDIX 3 DEFINITION OF TERMS

Patient identifiable information	Key identifiable information includes: - patient's name, address, full post code, date of birth; - pictures, photographs, videos, audio-tapes or other images of patients; - NHS number and local patient identifiable codes; - anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
Anonymised Information	This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.
Pseudonymised Information	This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.
Clinical Audit	The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services. This should be distinguished from studies that aim to derive, scientifically confirm and publish generalisable knowledge. The first is an essential component of modern healthcare provision, whilst the latter is research and is not encompassed within the definition of clinical audit in this document.
Explicit or Express Consent	This 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.
Implied consent	This means patient agreement that has been signalled by behaviour of an informed patient
Disclosure	This is the divulging or provision of access to data.
Healthcare Purposes	These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.
Information Sharing	Documented rules and procedures for the disclosure and use of patient information, which specifically relates to security,

Protocols	confidentiality and data destruction, between two or more organisations or agencies.
Medical Purposes	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001explicitly broadened the definition to include social care.
Public Interest	Exceptional circumstances that 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 society in the continued provision of confidential health services.
Social Care	Social care is the support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments. It excludes "pure" health care (hospitals) and community care (e.g. district nurses), but may include items such as respite care. There is therefore, no clear demarcation line between health and social care. Social care also covers services provided by others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).