Milton Keynes Hospital NHS
NHS Foundation Trust

Confidentiality Code of Practice

Document No.	Version	Issue Date	Last Review	Next Review	Impact Assessed	Author/Contact Person
ICT/GL/17	**2.1**	**02/2006**	**02/2010**	**02/2015**	✓	Information Governance Manager

Approved By:
MEC

For use in (clinical area)	Yes
For use by (staff groups)	Yes
For use for (patients/staff/public)	
Document Owner:	Information Governance Team
Document Status:	APPROVED
Care Quality Commission (CQC)	Outcome 21

Document and Consultation History

Version	Date	Author	Reason
1	**February 2006**	**Dawn Budd**	**To originate document**
2	**May 2008**	**Dawn Budd**	**Reviewed and updated**
	February 2010	**Dawn Budd**	**Reviewed – no change required**
2.1	**February 2013**	**Dawn Budd**	**Reviewed – minor changes**

Consultation History

Stakeholders Name	Area of Expertise	Date Sent	Date Received	Comments	Changes Made
Information Governance Steering Group	Information Governance				

Key messages

- What constitutes confidentiality and its meaning
- Applying good practice and legislation
- Patient consent
- Sharing Information
- Disclosure

CONTENTS

1.0 Introduction

Patients entrust the NHS or allow it 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 this trust. 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.

This document is a guide to required practice for those who work within or under contract to Milton Keynes Hospital NHS Foundation Trust concerning confidentiality of staff and patient information and patients' consent to the use of their health records. Its key reference being the Department of Health guidance *"Confidentiality: NHS Code of Practice" -November 2003.*

This Policy should be read in conjunction with all other Information Governance Policies.

2.0 Responsibility

Every member of staff (including agency, bank, locums, volunteers, non-contract and student placements) will at some time in the course of their work, have to handle confidential personal information whether relating to patients or staff or, their carers, family or friends or any other individuals connected to the Trust in some way.

Staff need to be aware that:

- They are individually responsible for the safekeeping of that information on behalf of the Trust, when it is in their possession.
- Everyone working for the Trust who records, handles, stores or comes across information that could identify a patient/staff member has a Common Law Duty of Confidence to that patient / Individual and to the Trust.
- They have signed a contract of employment that includes a statement of the need to maintain absolute confidentiality of personal information.
- Professional obligations of confidentiality must be applied.
- Unlawful disclosure or misuse of personal data (including staff accessing their own personal staff or health records without authorisation or the records of colleagues, family or friends) is a breach of Trust policy and may constitute a criminal offence. All incidents of this nature will be fully investigated and following procedures outlined in the Trust disciplinary procedure, may be treated as a serious disciplinary offence and may lead to dismissal.

Everyone working for the Trust has a responsibility to comply with the statutory acts that affect the processing and handling of information, confidentiality, the use of systems, and the protection of software. These are specifically:

- The Data protection Act 1998
- The Computer Misuse Act 1990
- The Copyright, Design and Patents Act 1988
- The Human Rights Act 1998

- Health & Social Care Act – Section 60, 2001
- The Freedom of Information Act 2000

3.0 What is Confidential Information?

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:–

a) is a legal obligation that is derived from case law

b) is a requirement established within professional codes of conduct; and

c) must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures

Information should be considered confidential if it can be related in any way to a specific individual. The main areas of concern are about patient and staff records and include any information that has not been fully anonymised. E.g. if name and address are not present but an NHS number is, this is not considered anonymous because it is still possible to trace that individual from the NHS number.

Confidential information will be found in a variety of formats including paper, computerised (including portable devices such as laptops and palmtops), visual and other versions of information storage media such as digital images and photographs. In addition, it covers oral communications including the use of the telephone (including mobiles) and general conversation.

The terms ‘person-identifiable information’ and ‘person-identifiable data’ are commonly used to mean any data item or combination of items by which a person’s identity may be established. The main person-identifiable data items are:

- Forename
- Surname
- Date of Birth
- Sex
- Address
- Postcode
- NHS Number, hospital Number or other patient numbers
- Staff payroll number

In this context, some key examples of flows of person-identifiable data would include:

- routinely sent free-text correspondence, e.g. discharge letters, employment correspondence
- manually completed forms, e.g. referral letters, positive reporting
- print-outs from systems, clinic/theatre listings
- electronically exchanged data (both structured and unstructured messages)
- telephone communication

In addition to the above, other information such as audio, video or photographic is also deemed as confidential information if an individual can be identified from any facial or physical attribute.

4.0 Applying Good Practice

In writing these guidelines the aim is to comply with the requirements of the Data Protection Act 1998 and Caldicott Report 1997, other associated legislation and guidance dealing with confidentiality and security.

Good practice working should be applied to all areas such as the office, at the reception desk, on the ward, in the outpatient's clinic, in the laboratory, information moving into and out of and around the Trust.

4.1 Data Protection 1998

The Data Protection Act 1998 is the fundamental legal requirement that applies to all organisations and individuals processing data of a personal nature. It is founded on the following set of eight good practice principles:

- **Principle 1** – Personal data shall be processed fairly and lawfully and in particular shall not be processed unless specified conditions can be met.

- **Principle 2** – Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or purposes.

- **Principle 3** – Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- **Principle 4** – Personal data shall be adequate and where necessary kept up to date.

- **Principle 5** – Personal data processed for any purpose or purposes shall not be kept any longer than is necessary for that purpose or those purposes.

- **Principle 6** – Personal data shall be processed in accordance with the rights of data subjects.

- **Principle 7** – Appropriate technical and organisational measures shall be taken against unauthorised or unlawful: processing of personal data and against accidental loss or destruction of or damage to personal data.

- **Principle 8** – Personal data shall not be transferred to any 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.

4.2 Caldicott Report 1997

Following a review of confidential patient information by the NHS and its subsequent Caldicott report published in 1997, a series of recommendations for improvements to practice were made along with a basic set of six good practice principles for all NHS organisations to adopt.

- **Principle 1 – Justify the purpose**
  Every proposed use or Transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appointed Guardian**.**

- **Principle 2 – Don't use patient-identifiable information unless it is absolutely necessary**
  Patient-identifiable information items should not be used unless there is no alternative.

- **Principle 3 – Use the minimum necessary patient-identifiable information**
  Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

- **Principle 4 – Access to patient-identifiable information should be on a strict need to know basis**
  Only those individuals who need access to patient-identifiable information should have access to it and they should only have access to the information items that they need to see.

- **Principle 5 – Everyone should be aware of their responsibilities**
  Action should be taken to ensure that those handling patient identifiable information, both clinical and non-clinical staff, are aware of their responsibilities and obligations to respect patient confidentiality.

- **Principle 6 – Understand and comply with the law**
  Every use of the patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

5.0 Using and Disclosing Patient Confidential

It is extremely important that patients are made aware of the information uses and 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 always be the case and the efforts to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies.

6.0 Informing Patients Effectively About the Uses of Their Information for Healthcare

Patients must be made aware that the information they give may be recorded and may be shared, In order to provide them with their care. It may also 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 or shared in a particular way – if so, then they are not effectively being informed.

In order to inform patients effectively, staff must:

- check where practicable that patients have received, read and understood the Trust's patient information leaflet "*A Guide to Patients on the use and storage of information"* which should be available in all patient accessible areas.

- make clear to patients the purpose of the health record and why and how the information is recorded.

- make clear to patients when they are or will be disclosing information to others and who these others may be.

- check that patients are aware of the choices available to them in respect of how their information may be disclosed or used and that by the withholding of consent will not effect their healthcare or treatment

- check that patients have no concerns or queries about how their information is disclosed and used

- where possible, answer any queries personally or direct the patient to others who can answer their questions (see Appendix 3 for list of Key Contacts).

- respect the rights of patients and facilitate them in exercising their right to have access to their health records

7.0 Consent

There are situations where the need to obtain consent to collect/disclose information is clear (see 8.1 & 8.2) below. In other circumstances, the law may either require or enable disclosure and in these cases seeking consent may not be supportive of the purpose for collecting/sharing information. Section 10 explains in detail how to cope with such situations.

8.0 When is Consent Required?

8.1 Explicit or Express Consent need not be obtained when:

a) A patient has provided confidential information relating to their medical condition for the purpose of receiving treatment and related services for that condition i.e. "Healthcare Purposes" (see glossary of terms Appendix 2) and, who has been made fully aware of who

will need to see information about them in order to provide treatment and care (see section 6). Their consent to their information being used in this way can be termed "implied" (see glossary of terms Appendix 2).

b) Information is being disclosed under Section 60 of the Health & Social Care Act 2004. Where practicable patients should be informed of the use.

8.2 Explicit or Express Consent must be obtained when:

a) The purpose/use of information changes or could include disclosure outside that deemed as "Healthcare Purposes" (see glossary of terms Appendix 2). For example, consent must be obtained prior to disclosure to or use for research, teaching (excluding local audit/assurance of quality of healthcare provided), supporting the work of chaplaincy departments, government departments, police & law courts. Consent where possible should in writing.

8.3 Patient Choice

Patients generally have the right to object to the use or disclosure of confidential information that identifies them, and 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.

Remember, patients have a right to change their mind about giving, withholding or withdrawing consent at any time. Full explanation must be given to the patient in cases where the withdrawing of consent may not always be possible (i.e. publications –where an article written with prior consent has already been published).

8.4 Children and Young People

Young people aged 16 or 17 are presumed to be competent for the purpose 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. 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 informing 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 persons have a proper authority (as parents or guardians).

9.0 Seeking and Recording Consent

9.1 Who is responsible for seeking consent for "Non Healthcare Purposes"?

Ideally, the senior health professional (see glossary of terms Appendix 2) involved in the care of the patient should seek consent for non healthcare purposes. The health professional should be supplied with all the necessary supporting information to appropriately inform the patient of the proposed use of their information and to answer any questions or queries arising.

To ensure that consent is appropriately sought the following should be applied:

- consent should be obtained *prior* to the information being used for other non healthcare purposes
- consent should be obtained where possible in writing. In other cases the method of obtaining consent should be recorded fully and, where appropriate, witnessed
- consent should be reviewed or further consent sought when:
  a) there is a change or extension to the purpose/use or information flow (i.e. disclosure)
  b) the legal status of the patient changes (i.e. child becomes adult)

Where possible inform and agree with the patient a lifetime of use.

10.0 Disclosure

10.1 Legally Required to Disclose

Some statutes place a strict requirement on clinicians or other staff to disclose information. Care should be taken however to only disclose the information required to comply with and fulfil the purpose of the law. If staff have a reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the patient or another person, then they should seek legal advice. Consent of the patient or data subject is not always required but he/she should be informed preferably prior to disclosure, unless, informing the data subject is likely to place them or another person at risk.

10.2 Legally Permitted to Disclose

Legislation may also create a statutory gateway that allows information to be disclosed by an NHS body where previously it might have been unlawful to do so e.g. section 115 of the Crime & Disorder Act 1998. This sort of permissive gateway generally stops short of creating a requirement to disclose therefore, common law duty of confidentiality (see glossary of terms Appendix 2) must still be satisfied, as must the Data protection Act 1998. Consent of the patient or data subject is not always required but he/she should be informed preferably prior to disclosure, unless, informing the data subject is likely to place them or another person at risk.

10.3 Disclosing (Sharing information with others) information with appropriate care

The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form except as originally understood by the confider, without his or her permission.

a. Follow any established information sharing protocols.

NHS organisations should have developed, or be in the process of developing, information sharing protocols that set out the standards and procedures that should apply when disclosing confidential patient information with other organisations and agencies. Staff must work within these protocols where they exist and within the spirit of this code of practice where they are absent.

b. *Identify enquirers, so that information is only shared with the right people.*

Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (**using an independent source for the phone number**). Check also that they have a legitimate right to have access to that information.

c. *Ensure that appropriate standards are applied in respect of e-mails, faxes and surface mail*

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be.

d. *Share the minimum necessary to provide safe care or satisfy other purposes.*

This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence. The Caldicott Principles should always be applied see 4.2.

10.4 Safeguarding Children and Young People

The general principles of consent and confidentiality apply to situations involving safeguarding issues. There are areas which are more complicated, particularly over disclosure without consent and disclosure of information relating to family members rather than to the index case.

In safeguarding there is a reversal of the normal weighting against disclosure. This means that a practitioner may be asked to justify a decision **not** to disclose.

Full information is contained in the document “Information sharing: Practitioners’ guide” detailed in Annex A. Help and advice is always available from the Named/Designated professionals listed *in “Departments – Child Protection*” on the MKHFT Intranet.

10.5 Legal Restrictions on Disclosure

There are two particular areas where there are legal restrictions on disclosing information and NHS organisations should take the necessary steps to secure any information capable of identifying an individual is not disclosed. These are:-

10.5.1 Sexually Transmitted Diseases (STD)

Sexually transmitted diseases include HIV and AIDS. Information shall not be disclosed except:

- where there is explicit consent

- for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and
- for the purpose of such treatment or prevention

10.5.2 Human Fertilisation & Embryology

Generally before disclosure explicit consent is required except in the connection with the:

- provision of treatment services, or any other description of medical, surgical or obstetric services, for the individual giving the consent
- carrying out of an audit or clinical practice; or
- auditing of accounts

10.6 General Guidance

For more detailed guidance on disclosure please refer to the Department of Health: *"Confidentiality: NHS Code of Practice"* -November 2003, Annex B – Confidentiality Decisions, pages 25-28 and Annex C – Index of Confidentiality Decisions in Practice, pages 39-45.

11.0 Review of this Code of Practice

This code of practice should be subject to review when any of the following conditions are met:

a) The adoption of the code of practice highlights errors and omissions in its content

b) Where other codes of practice issued by the Trust conflict with the information contained

c) Where the knowledgebase regarding interpretation of the legislation evolves to the extent that revision would bring about improvement

d) 3 years from the date of approval of the current version

12.0 Monitoring this Code of Practice

The Information Governance Steering Group will monitor the implementation of this code of practice and any subsequent revisions.

13.0 Policy Breaches

Any breach of this policy may result in appropriate disciplinary action.

14.0 Discrimination

This policy is considered to be compatible with the Human Rights Act, and not to discriminate against any group.

15.0 Implementation and dissemination of document

This policy will be placed on the Trust's intranet and internet sites.

16.0 Overall responsibility for the document

This policy will be maintained by the Information Governance Team

Appendix 1: Equality Impact Assessment

Impact	Age	Disability	Race	Gender	Religion or Belief	Sexual Orientation
Do different groups have different needs, experiences, issues and priorities in relation to the proposed policy?	NO	NO	NO	NO	NO	NO
Is there potential for or evidence that the proposed policy will not promote equality of opportunity for all and promote good relations between different groups?	NO	NO	NO	NO	NO	NO
Is there potential for or evidence that the proposed policy will affect different population groups differently (including possibly discriminating against certain groups)?	NO	NO	NO	NO	NO	NO
Is there public concern (including media, academic, voluntary or sector specific interest) in potential discrimination against a particular population group or groups?	NO	NO	NO	NO	NO	NO

Appendix 2 : Audit and Monitoring Criteria

Document Audit and Monitoring Table	
Monitoring requirements ***What in this document do we have to monitor** (e.g. processes)	Confidentiality of our data
Monitoring Method: **(***e.g. statistics, report***)**	Complaints, Breaches and Audits
Monitoring prepared by :- (name job titles)	a) ICT Security Team
Monitoring presented to:- (e.g. Committees)	a) Information Governance Steering Group
Frequency of presentation:- (e.g. annually, six-monthly etc)	The Information Governance Steering Group takes place bi-monthly and issues will be taken as when they occur

Appendix 3 : Good Practice

Keeping Confidential Information Secure
Good Practice

Confidential information must:

- Not be shared or discussed with, or in the presence of, anyone who does not need to know, or is not specifically authorised to know that information.
- Have appropriate control applied, having regard to professional ethics and patient consent. Applying formal access controls for clinical records and statutory requirements.
- Have appropriate control applied over the disclosure on non-patient information e.g. staff, relative, visitors in accordance with statutory requirements.
- Not be shared with parties outside the NHS e.g. solicitors, insurance companies, employers, police without the written consent of the individual concerned unless there are specific powers to do so.
- Always stored in a secure location, preferably a room that is locked and in some cases alarmed when unattended.
- Must not in the majority of cases be taken home or removed from the Trust without specific authorisation, this specifically applies to patients health records or patient data.

For all types of records, staff working in areas where personal records may be seen must:

- Shut/lock doors and cabinets as required.
- Adopt a “clear desk” policy where possible.
- Wear Trust identification badges or other authorised identification
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- Not tell unauthorised personnel how the security systems operate.
- Not breach security themselves.

Manual records must be:

- Formally booked out from their normal filing system.
- Tracked if transferred, with a note made or sent to the filing location of the transfer.
- Returned to the filing location as soon as possible after use.
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored closed when not in use so that contents are not seen accidentally.

- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons.
- Held in secure storage with clear labelling. Protective 'wrappers' indicating sensitivity – though not indicating the reason for sensitivity – and permitted access, and the availability of secure means of destruction, e.g. shredding, are essential.

With electronic records, staff must:

- Always log-out of any computer system or application when work on it is finished.
- Not leave a terminal unattended and logged-in.
- Not share logins with other people. If other staff have a need to access records, then appropriate access should be organised for them – this must not be by using others' access identities.
- Not reveal passwords to others.
- Change passwords at regular intervals to prevent anyone else using them.
- Avoid using short passwords (use 6-8 characters), or using names or words that are known to be personally associated with them (e.g. children's or pet names or birthdays).
- Always clear the screen of a previous patient's information before seeing another.
- Use a password-protected screen-saver where possible to prevent casual viewing of patient information by others.
- Protect information from the view of others as far as possible, particular care when there is a visitor present.
- Ensure that unwanted confidential printouts are shredded where possible and disposed of in confidential waste sacks and in accordance with Trust policy on record disposal.
- Ensure that electronic media such as floppy disc's, CD ROMs and Computer hard drives are disposed of in accordance with IT policy and procedures.

Telephone enquiries should be validated by:

- Checking the identity of the caller.
- Checking whether they are entitled to the information they request.
- Verify calls independently and call back if necessary.

Staff should ensure that general conversation involving discussions about individuals (including telephone) is:

- Where appropriate, undertaken in an area out of earshot of others, preferably in a closed office.
- Not undertaken with anyone who is not authorised to receive the information, including family and friends.
- Restricted to the use of personal identifiers (e.g. hospital number) when in public/reception areas

Confidential information sent via internal post or in internal transit should always be:

- Appropriately addressed to a named recipient, post holder, consultant or legitimate Safe Haven (Trust nominated secure area).
- Sealed in an appropriately secure envelope/package based on sensitivity and volume
- Marked accordingly, with “Confidential” or “Addressee Only” as appropriate.
- Traced in or out and signed for as appropriate.

Confidential information sent via external post or in external transit should always:

- Be addressed fully and marked accordingly, with “Confidential” or “Addressee Only” as appropriate.
- Be sealed in an appropriately secure envelope/package based on sensitivity and volume and using tamper proof seals where practicable and appropriate.
- Be sent via an approved carrier such as NHS courier, Internal transport or recorded delivery for any confidential information sent in quantity such as patient health records or a collection of patient information on paper or printout, floppy disc, CD Rom or other media. Obtaining a receipt as proof of sending/delivery is advised where possible.
- Traced in or out and signed for as appropriate.
- Have appropriate authorisation for leaving the Trust particularly in the case of patient’s health records.

Staff wishing to send or receive confidential patient information via fax must:

- Adhere to the Trust “Fax Safe Haven Procedure".
- Only send personal identifiable data to a recognised NHS safe Haven (nominate secure area) fax number.
- Remove all identifiable data if not sending to a recognised NHS safe Haven number
- Address the fax to a named recipient.
- Always check the number to avoid misdialling, check the number is correct and current if stored in a fax memory prior to sending.
- Ensure that trust fax machines are placed in secure locations

Staff using E-Mail must:

- Not e-mail patient identifiable information outside the local network.
- Only e-mail patient identifiable information when the Caldicott Principles are applied (anonymised where possible and the minimum identifiable data necessary).
- Apply adequate protection by placing the information in a password attachment where possible.
- Check to ensure that the recipient is authorised to receive the data (be

careful of shared mailboxes).

- Ensure that extra care is taken to ensure that it is sent to the correct.

Appendix 4 : Glossary of Terms

Patient Identifiable Information	Key identifiable information includes: • Patient's name, address, full postcode, date of birth • Pictures, photographs, videos, audio-tapes or other images (including digital) • 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 analysis which identify 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 post code 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 means of identifying individuals. This will often be achieved by attaching codes or other unique references to information so that data will only be identifiable to those that have the key or index. Pseudonymisation allows for 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 generalised 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/Express Consent	This means articulated patient agreement. The terms are interchangeable and relate to 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 patients agreement that has been signalled by the behaviour of an informed patient.
Common Law Duty of Confidentiality	This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgments. The key principle is that the information confided should not be used or disclosed further, except as originally understood by the confider, or without their subsequent permission.
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 Protocols	Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security and 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 & Social care Act 2001 explicitly broadened the definition to include social care.
Health Professional	See Section 69 of the Data Protection Act 1998 and any subsequent orders or statutory instruments.
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 other others where these are commissioned by CSSRs (Councils with Social Service Responsibilities).

Appendix 5 : Key Contacts

For further information or advice please contact:

Information Governance Manager

Head of Patient Services

Medical Records Manager

Caldicott Guardian

Director of Human Resources