

CONFIDENTIALITY POLICY

Amendments			
Date	Page(s)	Comments	Approved by
March 2009		Replaces the original Confidentiality Policy previously reviewed by the Management Board in September 2000	
March 2010	10	Section 10: Research, audit & monitoring – research ethics committee detailed	Information Governance Steering Group.
	11	Section 14: Access to Health Records – Medico Legal team changed to Subject Access team.	
	13	Section 14: Access to Health Records – Clarification of access to maternity hand held records	

Ratified by: Hospital Executive Committee
Reviewed by: Information Governance Steering Group
Review date: 13th March 2009
Approved by: Trust Executive Committee
Date: 8 May 2009
Reviewed by: Information Governance Steering Group
Review date: 13th March 2010
Next Review date: February 2013
Target Audience: All Staff
Impact Assessment Carried Out By: Tracey Street, Information Governance Manager
Contact for comments: Tracy Street, Information Governance Manager

CONFIDENTIALITY POLICY

See Also:

- Standards for Practice and Care for all Clinical and Support Staff Working with Patients
- Maintenance of Records and Record Keeping for Registered Nurses and Midwives
- Generic Medical Record Keeping Standards – Royal College of Physicians
- Confidentiality: NHS Code of Practice
- Work Shadowing, Work Experience, Work Attachment and Observer Attachments Policy
- IM&T Policies:
 - Fax Policy
 - Internet Usage and Security Policy
 - Information Security Policy
 - Records Management Policy
 - Email Policy
 - Freedom of Information Policy
 - Portable Computer Device Policy
- Standard Operating Policy for Health Records Department
- Abuse or Suspected Abuse of Vulnerable Adults Guidelines
- Trust Security Policy
- Policy for Handling Press Enquiries
- Patient Consent Policy
- Policy for the reporting and management of Incidents
- Complaints Procedure
- Information Governance – Staff Induction Booklet
- Guidance around Mental Capacity Act
- Multi Agency Information Sharing Protocol for Surrey (MAISPS)
- Guidance for Dealing with the Police and other Public Bodies

1. Introduction and Policy Principles

Any staff member working or volunteering in the NHS has a legal duty to keep information about patients confidential. The Trust requires all staff who receive or have access to information regarding patients or staff, or information regarded as 'commercial in confidence', to keep it confidential. The confidentiality of patient information is an essential component of Information Governance.

NHS organisations are required to appoint a Caldicott Guardian who is responsible for ensuring that all person identifiable information is held securely, shared appropriately and confidentiality is maintained at all times. There are 6 Caldicott Principles which were issued as part of a review carried out in 2007 by Dame Fiona Caldicott which looked at how information was shared in the Health Service. These are as follows:

- Principle 1: Justify the purpose(s) for using confidential information
- Principle 2: Only use it when absolutely necessary
- Principle 3: Use the minimum that is required
- Principle 4: Access should be on a strict need-to-know basis
- Principle 5: Everyone must understand his or her responsibilities
- Principle 6: Understand and comply with the law

The Caldicott Guardian for Ashford and St Peter's Hospitals NHS Trust is the Medical Director who is also the Chair of the Information Governance Steering Group. This group monitors the Trust's compliance on all matters relating to Information Governance including the maintaining of person identifiable information and the confidentiality thereof.

This Policy is based primarily on the Confidentiality: NHS code of Practice published in 2003 and which replaces previous guidance, HSG (96) 18 / LASSL (96) 5 – The Protection and use of Patient Information. This new Code of Practice details how the NHS should handle and protect patient information in relation to confidentiality.

The NHS is committed to the delivery of a first class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- Understand the reasons for processing personal information
- Give their consent for the disclosure and use of their personal information
- Gain trust in the way the NHS handles information
- Understands their rights to access information held about them.

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 generally not confidential and may be used with relatively few constraints.

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 3 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

Patients should be assured that confidentiality will be maintained and given examples of the permissible disclosure of information such as for audit, research and data collection or teaching purposes. In these cases patients are not personally identified.

2. Obligations on individuals working in the NHS

All staff should meet the standards outlined in the Confidentiality: NHS Code of Conduct document as well as their terms of employment with the Trust. This includes all permanent staff members, contract staff members, bank staff, volunteers and locums.

Whilst individuals are employed within the Trust they may come into contact with confidential information/data relating to the work of the Trust, its patients or staff. Staff are bound by the conditions of service to respect the confidentiality of any information they may come into contact with which identifies patients, staff or other Trust personnel and or the business information of the Trust. Under no circumstances should such information be divulged or passed to any unauthorised persons or organisations.

Disciplinary Action will be taken against an employee who is found to have breached confidentiality. Employees could also face prosecution under the Data Protection Act 1998.

Where employees who use a computer misuse their rights of access to computer information eg disclose their password to someone else or use someone else's password to gain access to information, they could be subject to disciplinary action. They may also be prosecuted under the Computer Misuse Act 1990.

Managers must ensure that confidentiality is discussed on the first day of employment with all new employees as part of an induction checklist. It is recommended that staff sign to acknowledge that they have taken note of the contents of this policy and other related policies regarding confidentiality and Information Governance.

Volunteers and work experience students must also have their role in maintaining confidentiality made clear by the member of staff responsible for them and must be aware of and adhere to this policy.

3. Providing a Confidential Service

The following guidance was taken directly from the Confidentiality: NHS code of Practice. Please consult this document should you need further detail on the points detailed below.

In order to provide patients with a confidential service certain requirements must be met. Record holders must inform patients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures. These processes are inter-linked and should be ongoing to aid the improvement of a confidential service

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 4 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

3.1. Protect Patient Information

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

- 3.1.1. Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality;
- 3.1.2. Recording patient information accurately and consistently;
- 3.1.3. Keeping patient information private;
- 3.1.4. Keeping patient information physically and electronically secure;
- 3.1.5. Disclosing and using information with appropriate care.

3.2. 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. In order to inform patients properly staff must:

- 3.2.1. Check where practicable that information leaflets on patient confidentiality and information disclosure have been read and understood;
- 3.2.2. Make clear to patients when information is recorded or health records are accessed;
- 3.2.3. Make clear to patients when they are or will be disclosing information with others outside their immediate clinical team;
- 3.2.4. Check that patients are aware of the choices available to them in respect of how their information may be disclosed and used;
- 3.2.5. Check that patients have no concerns or queries about how their information is disclosed and used;
- 3.2.6. Answer any queries personally or direct the patient to others who can answer their questions or other sources of information;
- 3.2.7. Respect the rights of patients and facilitate them in exercising their right to have access to their health records;
- 3.2.8. Communicate effectively with patients to help them understand.

3.3. 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 conditions 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:

- 3.3.1. Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of, their care;

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 5 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

- 3.3.2. Respect patients' decisions to restrict the disclosure or use of information except where exceptional circumstances apply;
- 3.3.3. Communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to or restrict the disclosure of information.

3.4. Improve Wherever Possible

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

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

4. Patient Information and Other Agencies

As detailed above, patients should be made aware of what happens to information about them.

Appendix 1: Model Notice for Patients is adopted for use within the Trust and is included as guidance.

There may be a need to share information during an investigation by Surrey Social Services or Surrey Police. In such cases the MAISPS (Multi Agency Information Sharing Protocol for Surrey) should be followed. The principles set out in the protocol are based on good practice and the legal and professional requirements relating to Surrey's public bodies. This protocol can be obtained from the Trust's Information Governance Manager. The Golden Rules are as follows:

- Confirm the identity of the person you are sharing with;
- Obtain consent to share if safe, appropriate and feasible;
- Confirm the reason the information is required;
- Be fully satisfied that it is necessary to share;
- Check with a manager/specialist or seek legal advice if you are unsure;
- Do not share more information than is necessary;
- Inform the recipient if any of the information is potentially unreliable;
- Ensure that the information is shared safely and securely;
- Be clear with the recipient how the information will be used;
- Record what information is shared.

5. Relatives/Next of Kin

If patients agree they can expect their relatives and friends to be kept up to date with the progress of their treatment. Such agreement needs to be explicitly secured in line with the Data Protection Act 1998 and the Confidentiality: NHS Code of Practice. Clinical staff must exercise caution when discussing a patient's condition with relatives or next of kin.

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 6 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

There may be occasions where, in the judgement of the managing clinician (but incorporating the advice of the wider multidisciplinary team as appropriate), knowledge of a patient's condition might seriously affect their physical or psychological well being if divulged to them. In these instances it may be decided to have discussions with the carer or next of kin. However, a careful judgement will need to be made and the basis for the decision and the content of the discussion must be carefully documented.

In the event that a patient lacks mental capacity to understand information given or make a decision and it is the managing clinician's opinion that it is 'in the patient's best interest' that information be divulged to the carer or next of kin, this should take place with the recipient's understanding that it is given in confidence.

The patient's consent and recipient's understanding, date, time and place of interview and those present should be documented in the patient's notes.

6. The Right to withhold or withdraw consent

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 healthcare. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected. This is no different from a patient exercising his or her right to refuse treatment. There are a number of things to consider if this circumstance arises:

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

Every effort must be made to find a satisfactory solution. The development of technical measures that support patient choice is a key element of work to determine the standards for electronic integrated care records. Careful documentation of the decision making process and the choices made by the patient must be included within the patient's record.

7. Vulnerable Adults

Disclosure of abuse may be made by a vulnerable adult who may ask for that information to remain confidential and for no action to be taken. Staff should explain to the vulnerable adult or to their relative or carer, or anyone else seeking to disclose concerns about abuse, that they may not be able to keep all information confidential.

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 7 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

Staff have a duty to alert their line manager, or a more senior manager if they are made aware of any actual or potential abuse of patients. Failure to do so will lead to disciplinary action. This is important for the protection of the person reporting the abuse and also for the safety and protection of other potential victims of the abuser's behaviour.

Staff must not disclose information to any third party as a decision about who needs to be told will be made by a senior manager.

All agencies receiving information in the course of an investigation must treat it as confidential, although priority must at all times be given to the protection of the vulnerable person. Other agencies must not disclose information for any purpose without the consent of the professional or senior manager who provided it. The person at risk should be advised when information is passed to other professionals or key individuals.

8. Children and Young People

Special conditions apply to children as patients of the Trust.

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 (eg 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 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 the proper authority (as parents or guardians). Ideally, there should be notes within the child's file as to any unusual arrangements.

In child safeguarding cases the overriding principle is to secure the best interests of the child. Therefore, if a health professional or other member of staff has knowledge of abuse or neglect it may be necessary to share this with others on a strictly controlled basis so that decisions relating to the child's welfare can be taken in the light of all relevant information. In the first instance, the member of staff should seek advice from their line manager.

9. Statutory Requirements

There are some instances where there is a statutory responsibility to pass on information. Prior consultation with the patient is not required but may be judged appropriate. If there are any doubts legal advice should be sought. The patient and relevant health professional should be

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 8 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

informed as soon as possible and a note made in the patient's record. Statutory notification is required for:

- Births and deaths
- Communicable diseases
- Abortion
- Substance misuse
- Serious Incidents – see policy for the reporting and management of incidents.
- Certain obligations under the Mental health Act 1983

It is the responsibility of the named officers of the organisation to pass on this information to the relevant body.

10. Research, Audit and Monitoring

Access to patient identifiable information or anonymous data may be sought for research, audit or monitoring purposes either by Trust employees or by other individuals or organisations. Internal requests related to research projects must be approved by the Research Ethics Committee and a formal submission will be required. Internal requests related to audit must be directed to the Clinical Effectiveness and Audit committee via the Clinical Effectiveness and Audit Manager.

All external requests or enquiries must be directed in the first instance to the Trust's Caldicott Guardian.

11. Public Interest, Police and Legal Enquiries

There may be a conflict between an employee's role as a Health Professional and as a 'responsible citizen'. Consideration will need to be given to the 'best interests' not only of the patient but also of other individuals or society in general. Some guidance is provided for registered healthcare professionals in their respective Codes of Conduct but advice may also be sought directly from the professional's registering body, professional organisation or Trade Union. Staff should also seek advice and support from an appropriate and senior officer of the Trust to ensure that correct action is taken.

Whilst the police have no general right of access to health records, there are a number of statutes which require disclosure to them and some that permit disclosure. These have the effect of making disclosure a legitimate function in the circumstances they cover.

In the absence of a requirement to disclose there must be either explicit patient consent or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the Courts.

Where disclosure is justified it should be limited to the minimum necessary to meet the need and patients should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk.

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 9 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	--------------

Any requests for information from the Police should always be referred to the site-co-ordinator or on-call manager unless there is immediate threat to human life as a result of the patient's actions.

A formally issued Court order directed by a Judge or other presiding Officer is required in order to release information for legal proceedings. Verbal or written requests from lawyers are not sufficient. This type of request must be referred to the Head of Customer Affairs, Head of Information Services or the on-call manager out of hours.

12. Media

All media enquiries must be directed to a representative of the Trust with suitable experience. This will normally be the press officer, or on-call manager out of hours.

13. Health Records (casenotes)

Staff must ensure that medical case notes and nursing and other professional records are:

- Kept in secure locations at all times.
- Secure when being transported throughout the Trust - it is recommended that case notes are transferred using a zipped bag when accompanying patients on transfer between clinical areas (other than A&E and theatres).
- Not left unattended in public areas.
- Tracked to locations to which they are forwarded.
- Not removed from the Trust's premises other than for transfer between the two hospital sites by making use of the appropriate secure transport methods provided. Where certain services require records to be made use of by staff outside of the hospital for example Birth Reflections counsellor services, it is the responsibility of the staff member to ensure that records are transported and used in line with the confidentiality policy and other policies as detailed in this document.

Offices and departments containing records must be kept locked when staff are absent.

The Trust has a policy of safeguarding patient records – Standard Operating Policy for Health Records Department. Points relevant to the issue of confidentiality are:

- Responsibility for NHS Casenotes: the Chief Executive and Senior Managers are ultimately accountable for the quality of records management although there is an individual responsibility on all staff who use the records. Training in the need for confidentiality is the responsibility of the line manager.
- Requests for casenotes: there is a 'closed' library system, which allows only authorised members of staff to locate and retrieve casenotes from the storage areas.
- Transportation of casenotes: movement of casenotes across the two hospital sites is controlled by the Health Records Manager. The notes are secured appropriately,

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 10 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

collected and delivered into the Health Records Department by the Trust's transport team. For clinics at other sites the notes will be delivered by the transport service.

- Casenotes should not be transferred to any other hospital. There may be some instances when copies are made and sent with the patient in a sealed envelope.
- NB it is not acceptable for staff to leave casenotes unattended in a private vehicle.

14. Access to Health Records

The Data Protection Act 1998 came into force on 1 March 2000. It encompasses the former Access to Health Records Act 1990.

Patients or where appropriate their relatives who seek access to their medical records should apply to the Subject Access Team for an application form which sets out the regulations and charges which the Trust may levy.

If clinicians of any discipline who have entered details in manual records wish to share this information with their patients this is permissible.

Patients and their relatives must not be handed their medical records for perusal unless a healthcare professional is available to:

- Be able to answer questions related to the contents of the medical record.
- Ensure that sections of the record are not removed.

Members of staff who receive requests for disclosure of medical records and are in any doubt about how to proceed should refer to the Subject Access Team via their line manager (site coordinator out of hours).

Maternity records are held by the patient during pregnancy and in the postnatal period. These are then returned to the maternity unit when discharged from maternity care. Should a patient want access to these records after the discharge date, this request would need to be made to the Subject Access Team.

15. Verbal Communication

Staff employed by the Trust have a duty to ensure that patient information is divulged only in accordance with the patient's wishes.

Care should be taken when talking to patients or relatives that the conversation is not overheard inappropriately. Private facilities should be offered for interviews of a sensitive nature.

Staff should satisfy themselves that information given over the telephone regarding a patient's condition or diagnosis is only given within the principles of these guidelines and that the identity

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 11 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

of the caller is correctly established. Care should also be taken as to who may overhear telephone conversations.

General guidance around how information should be shared securely in line with the Data Protection Act and the Caldicott Principles is detailed in a staff guide used at induction sessions covering all Information Governance issues. This is available via TrustNet on the Information Governance page or contact the Information Governance Manager for assistance.

16. Breach of Confidence

Any instance of unauthorised passing on of patient information may result in disciplinary action. Patients who feel that confidentiality has been breached may wish to use the Trust's complaints procedure. Patients have a right to be given advice about the complaints procedure.

17. Implementation and Monitoring of the Confidentiality Policy

The principles and requirements identified within this policy will require the development of associated systems and protocols/procedures in order for the Trust and its employees to achieve full compliance. Monitoring of the policy will be undertaken as relevant by the following Trust groups:

- Information Governance Steering Group
- Health Records Group in respect of case notes and other patient records and documentation.

The confidentiality Policy will be reviewed every 3 years or in line with any change of legislation or process

18. References

Data Protection Act 1998

Confidentiality: NHS Code of Practice 2003

Guidance on Implementation of the NHS complaints procedure 1996: section 3.3 Patient confidentiality, section 3.9 Access to Health Records. NHSE 1996

Human Rights Act 1998

The Caldicott Guardian manual 2009

1. The Mental Capacity Act

19. Archiving Arrangements

Responsibility for archiving trust-wide policies lies with the Quality Department where all paper copies will be stored, and electronic folders have been set up to hold master copies.

Requests for retrieval of documents can be made to the Quality Dept.

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 12 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

20. Equality Impact Assessment

The Equality Impact Assessment Is attached as an Appendix 2

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 13 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

PROTECTION AND USE OF PATIENT INFORMATION – NOTICE FOR PATIENTS

Your Information – What you need to know

- **Why we collect information about you**

Your doctor and other health professionals caring for you keep records about your health and any treatment and care you receive from the National Health Service. These help ensure that you receive the best possible care from us. They may be written down (manual records), or held on a computer. The records may include:

- basic details about you, such as address and next of kin
- contacts we have had with you, such as clinic visits
- notes and reports about your health and any treatment and care you need
- details and records about the treatment and care you receive
- results of investigations, such as X-rays and laboratory tests
- relevant information from other health professionals, relatives or those who care for you and know you well

- **How your records are used to help you**

Your records are used to guide and administer the care you receive to ensure:

- your doctor, nurse or any other healthcare professionals involved in your care have accurate and up-to-date information to assess your health and decide what care you need when you visit in the future
- full information is available should you see another doctor or be referred to a specialist or another part of the NHS
- there is a good basis for assessing the type and quality of care you have received
- your concerns can be properly investigated if you need to complain

- **How your records are used to help the NHS**

Your information may also be used to help us:

- look after the health of the general public
- pay your GP, dentist and hospital for the care they provide
- audit NHS accounts and services
- investigate complaints, legal claims or untoward incidents
- make sure our services can meet patient needs in the future
- prepare statistics on NHS performance
- review the care we provide to ensure it is of the highest standard
- teach and train healthcare professionals
- conduct health research and development

Some of this information will be held centrally but where this is used for statistical purposes stringent measures are taken to ensure that individual patients cannot be identified. Anonymous

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 14 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

statistical information may also be passed to organisations with a legitimate interest, including universities, community safety units and research institutions.

Where it is not possible to use anonymised information, personally identifiable information may be used for essential NHS purposes. These may include research and auditing services. This will only be done with your consent unless the law requires information to be passed on to improve public health.

- **How we keep your records confidential**

Everyone working for the NHS has a legal duty to keep information about you confidential.

You may be receiving care from other organisations as well as the NHS (like Social Services). We may need to share some information about you so we can all work together for your benefit.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to third parties without your permission unless there are exceptional circumstances, such as when the health or safety of others is at risk or where the law requires information to be passed on.

Anyone who receives information from us is also under a legal duty to keep it confidential.

We are required by law to report certain information to the appropriate authorities. This is only provided after formal permission has been given by a qualified health professional. Occasions when we must pass on information include:

- notification of new births
- where we encounter infectious diseases which may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS)
- where a formal court order has been issued

Our guiding principle is that we are holding your records in strict confidence.

- **Who are our partner organisations?**

The principal partner organisations with whom information may be shared:

- Health Authorities
- NHS Trusts
- Primary Care Trusts
- General Practitioners (GPs)
- Ambulance Services

Your information may also, subject to strict agreements describing how it will be used, be shared with:

- NHS Common Services Agencies
- Social Services
- Education Services
- Local Authorities
- Voluntary Sector Providers
- Private Sector Providers

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 15 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

- **How you can get access to your own health records**

The Data Protection Act 1998 allows you to find out what information about you is held on computer and in certain manual records. This is known as “right of subject access.” It applies to your health records. If you want to see them you should make a written request to the NHS organisations where you are being, or have been, treated. You are entitled to receive a copy but should note that a charge will usually be made. You should also be aware that in certain circumstances your right to see some details in your health records may be limited in your own interest or for other reasons.

- **Further information**

If you would like to know more about how we use your information or if, for any reason, you do not wish to have your information used in any of the ways described in this leaflet please speak to the health professionals concerned with your care or the Trust’s Information Governance Manager.

If you would like a large print version or a translation of this leaflet in a foreign language, please contact the Patient Advice and Liaison Services (PALS) Officer.

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 16 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

ASHFORD & ST. PETER'S HOSPITAL NHS TRUST

Equality Impact Assessment Summary

Policy/Service: Confidentiality Policy

<p>Background</p> <ul style="list-style-type: none"> • Description of the aims of the policy • Context in which the policy operates • Who was involved in the Equality Impact Assessment 					
<p>The guidance provided in this policy is to assist all staff members in ensuring that correct procedures are followed in relation to the confidentiality of patient and staff information. This Policy details guidance around ensuring that personal identifiable information or that of a confidential manner is kept secure and confidentiality is maintained</p>					
<p>Methodology</p> <ul style="list-style-type: none"> • A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age) • The data sources and any other information used • The consultation that was carried out (who, why and how?) 					
<p>Confidentiality affects all staff members regarding use of patient information, staff information or corporate information. This Policy was drafted as guidance in line with confidentiality and data protection guidelines. Data sources include confidentiality – NHS Code of Practice; Data Protection Act 1998 and guidance as issued by the Information Commissioner. This was originally drafted by the Head of Information Services and has recently been updated by the Information Governance Manager and the Information Governance Steering Group.</p>					
<p>Key Findings</p> <ul style="list-style-type: none"> • Describe the results of the assessment • Identify if there is adverse or a potentially adverse impacts for any equalities groups 					
<p>No adverse or potentially adverse impacts have been assessed for any equalities groups. The policy equally effects all from any equalities group.</p>					
<p>Conclusion</p> <ul style="list-style-type: none"> • Provide a summary of the overall conclusions 					
<p>The policy reflects statutory legislation and national guidance on the use of information and the maintaining of confidentiality at all time.</p>					
<p>Recommendations</p>					

Vol 1 Organisational & Finance	Section 1	First Ratified April 1996	Last Review March 2010	Issue 3	Page 17 of 18
--------------------------------------	-----------	------------------------------	---------------------------	---------	---------------

<ul style="list-style-type: none"> • State recommended changes to the proposed policy as a result of the impact assessment • Where it has not been possible to amend the policy, provide the detail of any actions that have been identified • Describe the plans for reviewing the assessment
No changes recommended

Guidance on Equalities Groups

Race and Ethnic origin (includes gypsies and travellers) (consider communication, access to information on services and employment, and ease of access to services and employment)	Religion or belief (include dress, individual care needs, family relationships, dietary requirements and spiritual needs for consideration)
Disability (consider communication issues, access to employment and services, whether individual care needs are being met and whether the policy promotes the involvement of disabled people)	Sexual orientation including lesbian, gay and bisexual people (consider whether the policy/service promotes a culture of openness and takes account of individual needs)
Gender (consider care needs and employment issues, identify and remove or justify terms which are gender specific)	Age (consider any barriers to accessing services or employment, identify and remove or justify terms which could be ageist, for example, using titles of senior or junior)
Culture (consider dietary requirements, family relationships and individual care needs)	Social class (consider ability to access services and information, for example, is information provided in plain English?)