Doc level: Trustwide
Code ref:

Confidentiality of Patient and Employee Information Policy

Lead executive	Medical Director
Authors details	Health Records & Information Governance Manager

Type of document	Policy
Target audience	All Trust staff and patients
Document purpose	This policy details how North Staffordshire Combined Healthcare NHS Trust will meet its legal obligations under Data Protection legislation and NHS requirements concerning confidentiality of their information.

Approving meeting	PCD Trust Board	Meeting date	10th September 2018 26th September 2018
Ratification date	30th September 2018	Review date	30th September 2021

Trust documents to be read in conjunction with	
Document code	Document name
4.18	Risk Management Policy
5.01	Incident Reporting Policy
7.02	Subject Access Request Policy
7.03	Information Security & Data Protection Policy
7.05	One Staffordshire Information Sharing Protocol

Document change history		Version	Date
What is different?	– This policy has been revised in line with legislation changes under the Data Protection legislation. –		
Appendices / electronic forms	–		
What is the impact of change?	– Making all staff aware of changes in legislation which impact on confidentiality – Ensuring that the Trust is compliant with its legal requirements under Data Protection and other associated legislation.		

Training requirements	There are no specific training requirements for this document. Confidentiality training is covered under the Data Security Awareness national training tool

Document consultation	
Directorates	
Corporate services	
External agencies	

Financial resource implications	No

External references
1. Data Protection Bill 2. General Data Protection Regulations (GDPR)

Monitoring compliance with the processes outlined within this document	Any breaches to this policy will be recorded within the Trust's incident reporting system and any breaches will be investigated accordingly.

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Less favourable / More favourable / Mixed impact**
Does this document affect one or more group(s) less or more favorably than another (see list)?		
– **Age** (e.g. consider impact on younger people/ older people)	No	
– **Disability** (remember to consider physical, mental and sensory impairments)	No	
– **Sex/Gender** (any particular M/F gender impact; also consider impact on those responsible for childcare)	No	
– **Gender identity and gender reassignment** (i.e. impact on people who identify as trans, non-binary or gender fluid)	No	
– **Race / ethnicity / ethnic communities / cultural groups** (include those with foreign language needs, including European countries, Roma/travelling communities)	No	
– **Pregnancy and maternity, including adoption** (i.e. impact during pregnancy and the 12 months after; including for both heterosexual and same sex couples)	No	
– **Sexual Orientation** (impact on people who identify as lesbian, gay or bi – whether stated as 'out' or not)	No	
– **Marriage and/or Civil Partnership** (including heterosexual and same sex marriage)	No	
– **Religion and/or Belief** (includes those with religion and /or belief and those with none)		
– **Other equality groups?** (may include groups like those living in poverty, sex workers, asylum seekers, people with substance misuse issues, prison and (ex) offending population, Roma/travelling communities, looked after children, local authority care leavers, and any other groups who may be disadvantaged in some way, who may or may not be part of the groups above equality groups)	No	

If you answered yes to any of the above, please provide details below, including evidence supporting differential experience or impact.	
Enter details here if applicable	
If you have identified potential negative impact: - Can this impact be avoided? - What alternatives are there to achieving the document without the impact? Can the impact be reduced by taking different action?	
Enter details here if applicable	
Do any differences identified above amount to discrimination and the potential for adverse impact in this policy?	No
If YES could it still be justifiable e.g. on grounds of promoting equality of opportunity for one group? Or any other reason	N/A
Enter details here if applicable	
Where an adverse, negative or potentially discriminatory impact on one or more equality groups has been identified above, a full EIA should be undertaken. Please refer this to the Diversity and Inclusion Lead, together with any suggestions as to the action required to avoid or reduce this impact. For advice in relation to any aspect of completing the EIA assessment, please contact the Diversity and Inclusion Lead at Diversity@northstaffs.nhs.uk	
Was a full impact assessment required?	No
What is the level of impact?	Low

CONTENTS

1. INTRODUCTION

1.1 The purpose of this policy is to lay down the principles that must be observed by all who work within North Staffordshire Combined Healthcare and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. The Trust must ensure that it complies with Data Protection Law in its management and disclosure of person identifiable information, in addition to providing clear guidance for managers and staff. Additionally, all NHS organisations are required to comply with a number of standards that underpin the confidentiality of personal data, notably with the integration of the Data Security and Protection Toolkit (DSP).

1.2 The DSP framework allows organisations and individuals to ensure that personal and corporate information is managed legally, securely and efficiently in order to assist in the delivery of the best possible care.

1.3 The framework integrates previously separated but interrelated initiatives within a single transparent package which represents the Department of Health Policy. There are similarities and overlaps between the core components of this framework. These core components currently include:-

- Freedom of Information Act 2000/Corporate Records Management including HSC 1999/053 For the Record;
- Data Protection Law (DPA);
- The Confidentiality NHS Code of Practice;
- Records Management NHS Code of Practice;
- Information Security Management;
- Information Quality Assurance;
- Caldicott Principles;

1.4 This policy details the rights of a “data subject” together with the responsibilities of the Trust. The Trust definition of a data subject is in accordance with Data Protection Law (DPA). Therefore, a data subject is defined as a living individual who is the (main) subject of personal data.

1.5 This policy details the “data controller”. The Trust definition of a data controller is in accordance with Data Protection Law (DPA). Therefore a data controller is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

2. POLICY STATEMENT

In general any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. This duty of confidence is long established in common law. In addition, health professionals have ethical and professional duties of confidence.

The disclosure and use of confidential personal information needs to be both lawful and ethical. Whilst law and ethics in this area are largely in step, the law provides a minimum standard that does not always reflect the appropriate ethical standards that the government and the professional regulatory bodies require. For example, the Department of Health and the General Medical Council are in agreement that, whilst there are no clear legal obligations of confidentiality that apply to the deceased, there is an ethical basis for requiring that

confidentiality obligations must continue to apply. Further, where the law is unclear, a NHS standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

Data subjects provide personal information for the employment/health records and have an expectation that their privacy will be maintained.

In this policy and supporting guidance 'personal information' applies to all such information about data subjects held in whatever form by the Trust.

It is neither practicable nor necessary to seek a person's specific consent every time information needs to be passed on for a particular purpose. Data subjects expect the NHS, often in conjunction with other agencies, to respond effectively to their needs. It can do so only if it has the necessary information. It is therefore essential that data subjects are fully informed of the uses to which information about them may be used. If the nature of the use of that information changes then the person to who the information relates must be informed and consent obtained before the information is passed on.

3. SUPPORTING GUIDANCE

The Duty of Confidence derives from the personal nature of the information recorded. It is unaffected by questions of who owns or holds particular records. Consequently, the following all have responsibilities for protecting information:-

- Everyone working for or with the NHS is bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within common law duty of confidence and Data Protection Law. It is also a requirement within the NHS Care Record Guarantee. This applies equally to those working on a voluntary basis or on a temporary placement such as students.

- Health Professionals have by virtue of professional regulation, an ethical duty of confidence which, when considering whether information should be passed on, includes special regard to the health of the patient and to his/her wishes.

- Other individuals or agencies to which information is passed legitimately may only use that information for specific purposes, possibly subject to particular conditions.

3.2 Human Rights Act 1998 (HRA98)

3.2.1 Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their records. Current understanding is that compliance with the Data Protection Law and the common law of confidentiality should satisfy Human Rights requirements. Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:-

- Pursue a legitimate aim;
- Be considered necessary in a democratic society; and
- Be proportionate to the need.

3.2.2 There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be

justified as being necessary to support legitimate aims and be proportionate to the need.

3.3 Data Protection Law

3.3.1 Data Protection Law relates to the rights and freedom of living individuals. The Act gives individuals the right to access personal data held about them. Personal data relates to a living individual who can be identified from that data and includes any facts, opinion or any indication of intentions of the data controller about that individual. This includes personal data held in either electronic or manual systems.

3.3.2 NHS bodies that use personal information must register with the Information Commissioner. It is a criminal offence to hold or disclose information in breach of the registration requirement.

3.3.3 Any person who believes that the Trust has used or disclosed their personal information contrary to the requirements of the Law can apply to the Information Commissioner for an assessment to be undertaken as to whether any of the provisions of the Law have not been adhered to or to the Court for redress.

(See appendix 1 for the principles of Data Protection Law)

3.4 Caldicott Report

Following a review of confidential patient information by the NHS, a series of recommendations for improvements to practice were made. NHS organisation must appoint a Caldicott Guardian to oversee the arrangement for the use and sharing of clinical information. The Trust's Caldicott Guardian is the Medical Director. The Trust must also comply with the principles set out in the Caldicott report.

4. MANAGEMENT OF INFORMATION

4.1 The administration of personal information encompasses many elements. In all cases the use of personal information will be covered by a model referred to as HORUS (Holding, Obtaining, Recording, Using, and Sharing).

4.2 The Trust should ensure that data subjects are aware of the nature and source of any information kept about them, how it will be used and whom it may be disclosed to.

4.3 The Trust must inform data subjects about their rights under Data Protection Law, including their right to access the information kept about them.

4.4 Data subjects will be requested to confirm personal details kept on record that may be subject to change e.g. home address, GP etc.

4.5 The Trust will incorporate accuracy, consistency and validity checks into its associated systems.

5. RESPONSIBILITY FOR DISCLOSING INFORMATION

5.1 The Caldicott Guardian ensures that the Trust is compliant in protecting the confidentiality of personal information and enabling appropriate information-sharing. The Caldicott Guardian will actively support work to facilitate and enable information sharing and advice on options for lawful and ethical processing of information as required.

5.2 Personal information may be disclosed on a 'need to know' basis, if the following circumstances apply:

- The use of the information can be justified e.g. confirmation of employment for mortgage application purposes.
- The information is required by statute or court order; or
- Passing on the information can be justified for other reasons, usually for the protection of the public or data subject.

5.3 The Trust is accountable for any decisions to disclose information. Such decisions should usually be taken by the health professional responsible for a patient's care or the manager holding the employee's personal information. If in doubt contact the Caldicott Guardian for advice.

5.4 Disclosure of personal information may also be decided on the advice of a nominated senior professional within the body or the directorate senior manager. Only the minimum identifiable information should be used.

5.5 Prevention of processing causing damage or distress – If an individual believes the Trust is processing personal data in a way that causes, or is likely to cause, substantial unwarranted damage or distress to them or to another, the Data Protection Law provides that the individual has the right to send a notice to the data controller requiring him, within a reasonable time, to stop the processing.

5.6 If a data subject wants information withheld from someone who might otherwise have received it in connection with their employment, then that data subject should be informed of any implications or other relevant factors.

Data subjects must make a request in writing if they do not want personal information disclosed which includes a description of:-

- The personal data;
- The purpose for which they are being processed; and
- Those to whom it may not be disclosed.

5.7 The data subject's wishes should be respected unless there are overriding considerations to the contrary. The reason for disclosing the information must be noted.

5.8 The data subject has a right to rectification if they feel that information recorded on their record is incorrect. This should be discussed with their line manager or clinician.

6. ANONYMISED INFORMATION

6.1 Where anonymised information would be sufficient for a particular purpose**,** identifiable information should be omitted. The Trust will endeavour to ensure that the recipient is unable to trace the data subject's identity. The fact that the information has been anonymised does not remove the legal obligations under the common law of confidentiality, Data Protection Law and the Human Rights Act.

6.2 Anonymising the information may not in all cases be sufficient to protect the data subject's identity: for example if they are from a professional group with only a small number of data subjects in the Trust.

7. CORPORATE AND STATISTICAL

7.1 The Freedom of Information Act 2000 (FOIA) is an element of the Government's commitment to greater openness in the public sector, a commitment which is fully supported by the Trust. The FOIA will progress this aim by helping to transform the culture of the public sector to one of greater openness. It will enable members of the public access to substantial amounts of corporate information and documents therefore allowing the public to question the decisions of public authorities more closely, ensuring that the services we provide are efficiently and properly delivered.

7.2 Disclosure of information about performance and activity in the NHS is an important aspect of accountability and a means of fostering public awareness of how taxpayers' money is spent and the range of services provided.

7.3 Provided that the data subject is made aware that personal information may be used to prepare statistics for management use, the aggregated information may be used or passed on for those purposes.

8. RIGHTS AND REDRESS

8.1 The unauthorised disclosure of data subject information by any member of staff or person in contact with the NHS is a serious matter and may result in the implementation of the performance management procedure or disciplinary action and possible legal action. In addition, health professionals may be subject to action by their regulatory bodies.

8.2 A duty of confidence forms part of the Trust's employment contract and terms and conditions of employment. All staff must be aware of the possible severe consequences of breaching confidence in relation to disclosure of personal information relating to data subjects.

8.3 **Patients** who feel their confidentiality has been breached should be encouraged to use the Trust's Listening and Responding PALS and Complaints policy (see policy 4.26)

8.4 **Employees** who feel their confidentiality has been breached have a duty to report this immediately to their line manager and in addition, if they feel appropriate can take action in line with the Trusts Resolution of Grievances and Disputes policy. (See policy 3.02)

8.5 Data subjects have the right to refer their case direct to the Information Commissioner at the address below, to assess whether the requirements of Data Protection Law have been met.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow, Cheshire
SK9 5AF

Website: www.informationcommissioner.gov.uk
Email: casework@ico.org.uk
Telephone: 01625 545745

9. RISK & MONITORING COMPLIANCE WITH DOCUMENT

9.1 Risk management involves a two-stage approach to identifying both the points at which risk occurs in a system and solutions to reduce those risks. The first depends on reporting adverse incidents and near misses the second depends on the systems, structures and processes linked to the incident.

9.2 Monitoring of this policy will be through the incident reporting process (Ulysses) as any incidents of non-compliance with this policy (e.g. breach of confidentiality) must be reported via the Trust's electronic Incident reporting system

9.3 Failure to comply with the policy may result in the invocation of the performance management procedure or disciplinary action.

(Ref: Incident Reporting Policy No 5.01)

10. ACCESS TO DATA SUBJECTS INFORMATION

10.1 Data subjects have a legal right under Data Protection Law to access personal data about themselves which is held in either computerised or manual form by the Trust. This legal right is referred to as "Subject Access Request" which enables an individual to review or to be provided with copies of information contained within any personal or occupational health record.

Legally, the data subject must make a written request; a subject access should be dealt with in line with the Trust's Subject Access Request policy No 7.02.

11. SECURITY OF PERSONAL INFORMATION

11.1 Ensuring the security and accuracy of data subject information is the responsibility of management and staff at all levels including:

- Arrangements for the storage and disposal of all data subject information (both manual and electronic) must protect confidentiality.

- Under Data Protection Law security measures must be in place to protect manual/paper and electronic information. (see Information Security and Data Protection Policy 7.03 and Records Management Policy 7.07)

- Care should be taken to ensure that unintentional breaches of confidentiality do not occur e.g. by leaving confidential information in publicly accessible areas or allowing conversations about sensitive personal information to be overheard.

- A non NHS agency or individual is contracted to carry out NHS functions, the contract must draw attention to obligations on confidentiality. (see Information Security and Data Protection policy 7.03)

- Those who work in the NHS must be aware that people may attempt to seek personal information by deception, for example, posing as a relative. If a member of staff is asked to provide non routine information by a person not known to them, they should make every effort to verify that the person has a right to the information before releasing it.

12. CO-ORDINATING INFORMATION WITH EXTERNAL SERVICES

12.1 Access to personal identifiable information should be restricted to those who have a justifiable need to know in order to effectively carry out their jobs. The Caldicott Principles underpin the approach taken by the Trust when requested to share information with other NHS organisations and non NHS organisations for example Social Services. Sharing information, current or proposed, should be tested against the Caldicott Principles (see appendix A)

12.2 Trust protocols provide a robust framework for staff when sharing personal identifiable information. The purpose(s) for which information is required by different organisations will clearly differ and each needs to be sensitive to the particular requirements of others in respect of confidentiality.

12.3 The data subject needs to be aware that some information sharing for direct care will be necessary and this must be discussed with the individual as part of the care planning process.

12.4 If the data subject raises any objections to the passing of information to other sources, the possible consequences must be explained and an assurance given that other sources would receive only information which they really need to know. However, the data subject's ultimate decision must be respected unless there are overriding considerations to the contrary: for example, in some cases involving a history of violence, or where an elderly frail person shows signs of non-accidental injury, it may be justifiable to pass information to another agency without the individual's agreement.

12.5 When creating inter-agency registers or pooling information to assist joint commissioning of services, NHS (and other) bodies should ensure that patients know in general terms what is being done and to whom information may be passed.

13. PATICULAR RESTRICTIONS ON PASSING ON INFORMATION

NHS bodies or those carrying out NHS functions must not allow personal details of data subjects (most obviously names and addresses of named individuals) to be passed on or sold for fundraising or commercial marketing purposes.

14. DISCLOSURE OF INFORMATION FOR OTHER PURPOSES OR AS A LEGAL REQUIREMENT

14.1 There are statutory powers to order:

- The disclosure of documents before and during proceedings for personal injury or death.

- The production of information following an application to the court and to the applicants, legal, medical and professional advisors. Such orders should specify clearly what information is required and by whom. If any aspect is unclear, clarification and/or legal advice should be sought without delay. The manager responsible for the information relating to the data subject should be consulted about the disclosure, in case disclosure may result in a risk to the data subject. If there is a risk, legal advice should be sought on the possibility of seeking an amendment to the order.

- Where an order requires information about a data subject who has not instigated a court action, that data subject should be notified immediately in case the individual may wish to seek advice.

At the data subject's request, information relevant to legal proceedings may be released, usually to the individual's legal adviser. This information should also be passed to solicitors acting for the Trust where the action involves the Trust. Ref: Subject Access Request Policy No 7.02.

14.2 Relatives, friends and carers, if data subjects agree can be kept up-to-date with the progress of treatment. With the data subjects consent, the significant role of carers may need to be recognised in the type of information provided. If the data subject has not given their consent then information should not be passed to relatives etc.

15. DISCLOSURE OF INFORMATION TO PROTECT THE PUBLIC

15.1 It may sometimes be justifiable to pass on data subject information without consent or statutory authority. Most commonly these involve the prevention of serious crime, but can extend to other dangers to the general public, such as public health risk or violence. Essential information may need to be shared with other agencies.

15.2 Each case must be considered on its merits, the main criterion being whether the release of information to protect the public should prevail over the duty of confidence to the data subject. The possible consequences for the data subject must always be considered.

15.3 Decisions will sometimes be finely balanced and may concern matters on which NHS staff finds it difficult to make a judgement. In such cases legal or other specialist advice e.g. Caldicott Guardian should be sought. It is important not to confuse 'the public interest' with what may be 'of interest' to the public.

16. TACKLING SERIOUS CRIME

16.1 Passing on information to help tackle serious crime may be justified in accordance with the Crime and Disorder Act 1998.

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

In the absence of a requirement to disclose there must be either explicit consent of the data subject 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 the data subject 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.**

16.2 Disclosure must be justified on the grounds that the public interest outweighs the common law duty of confidentiality and the principles of the Human Rights Act 1998 (HRA98).

Article 8 of the HRA98 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with Data Protection Law and the common law of confidentiality should satisfy Human Rights requirements.

Legislation generally must also be compatible with HRA98, so any proposal for setting aside obligations of confidentiality through legislation must:

- Pursue a legitimate aim;
- Be considered necessary in a democratic society; and
- Be proportionate to the need.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need. Ref: Subject Access Request Policy No 7.02.

17. TEACHING AND RESEARCH

17.1 Advice to data subjects about the use of personal information must emphasise:

- The importance of teaching and research to the maintenance and improvement of care within the NHS, inter-agency care and public health generally;

- That such information, anonymised or aggregated wherever possible, may sometimes be used for teaching and research (and that universities or other bodies carrying out approved research are required to treat it in confidence and must not use if for other purposes);

- That any research proposals involving access to patient records require regulatory approvals including a favourable ethics opinion from a Research Ethics Committee, who must be satisfied that:

    - Arrangements to safeguard confidentiality are satisfactory;

    - Any additional conditions relating to the use of information that the Research Ethics Committee thinks are necessary are met;

- Any application to use **identifiable** patient information is fully justified: for example, because this is essential to a study of major importance to public health. **If not, approval to proceed should not be given;**

- That their specific consent will be sought to any activity relating to teaching or research that would involve them personally. Individuals may at any time state that they do not wish to be contacted for involvement in such activity and this must be formally recorded so that they are not contacted.

- That any publicised research findings will not identify them without their specific consent.

18. TRAINING REQUIREMENT

18.1 Confidentiality training is included within the annual Data Security Awareness e-learning training tool and will be monitored through the Trust Mandatory training and the Personal Review process.

19. COMMUNICATION WITH THE MEDIA

19.1 The maintenance of good relations with the press and broadcasting organisations is important. The Trust will ensure that there is someone with suitable experience and level of responsibility available or contactable at all times to answer enquiries.

19.2 If the media interest relates to a data subject, then the individual's valid consent must be obtained before release of information. If the person is incapable of providing valid consent then the consent of the nearest relative should be sought.

19.3 Neither the Trust nor anyone who works in the Trust should confirm that any individual is a data subject or divulge any information about them without the person to which the information refers consenting to its release.

19.4 Subject to the necessary consent being given, a brief indication of the patient's progress or the employee's job title and work base may be given in response to media enquiry if authorised by the Senior Manager.

19.5 As referred to above, other than straightforward data subject enquiries, media requests for information should be referred to the Communications Manager, Corporate Services or the Caldicott Guardian.

19.6 Where the data subject is unable to take a decision, the provision of basic information may sometimes be judged to be in their best interests (e.g. correcting misleading or damaging speculation).

19.7 If a data subject has invited the media to report their case, the Trust may comment in public but should confine itself to factual information or the correction of any misleading assertion or published comment. The duty of confidence to the data subject still applies. If in doubt, legal advice should be sought.

20. EQUALITY IMPACT ASSESSMENT

An equality impact assessment has been undertaken for this policy with no potential or adverse impact identified.

21. REFERENCES & OTHER SOURCES OF INFORMATION

- Risk Management Policy No 4.18a
- Incident Reporting Policy No 5.01
- Serious Incident Policy No. 5.32
- Subject Access Request Policy No 7.02
- One Staffordshire Information Sharing Protocol Policy No 7.05
- Information Governance Policy No 7.08
- Information Security & Data Protection Policy No 7.03
- Records Management Policy 7.07
- Safe Haven Policy No 7.14
- Caldicott Guardian www. gov.uk
- NHS Confidentiality Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- Record Management: NHS Code of Practice https://www.gov.uk/government/publications/records-management-nhs-code-of-practice
- The Care Record Guaranteehttp://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf
- Information Security Management: NHS Code of Practicehttps://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice

APPENDIX 1

DATA PROTECTION; PRINCIPLES OF DATA PROCESSING

Principle 1	Personal data shall be processed lawfully, fairly and in a transparent manner;
Principle 2	Collected for specific; explicit and legitimate purposes;
Principle 3	Personal data shall be adequate, relevant and limited to what is necessary;
Principle 4	Personal data shall be accurate and, where necessary, kept up to date;
Principle 5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
Principle 6	Personal data shall be processed in an appropriate manner to maintain security;

APPENDIX 2

THE CALDICOTT GUARDIAN: PRINCIPLES

Principle 1	Justify the purpose(s) for using confidential information
Principle 2	Do not use person identifiable information unless it is absolutely necessary.
Principle 3	Use the minimum necessary person-identifiable information.
Principle 4	Access to person-identifiable information should be on a strict need to know basis.
Principle 5	Everyone with access to person-identifiable information should be aware of their responsibilities...
Principle 6	Understand and comply with the law.
Principle 7	The duty to share information can be as important as the duty to protect person-identifiable confidentiality