NHS
North East Hampshire and Farnham
Clinical Commissioning Group

Confidentiality Policy - Data Protection Act 1998

Subject and version number of document:	Confidentiality Policy - Data Protection Act 1998 Version 2.0
Serial Number:	
Operative date:	November 2015
Author:	Information Governance Team, NHS South, Central and West Commissioning Support Unit NHS North East Hampshire and Farnham Clinical Commissioning Group
Review date:	November 2017
For action by:	All NHS North East Hampshire and Farnham Clinical Commissioning Group staff Data Custodians Information Governance Team
Policy statement:	This policy describes the CCG's responsibilities under the Data Protection Act 1998 and ensures all employees abide by the legal duty of confidence to protect personal confidential data.
Responsibility for dissemination to new staff:	NHS North East Hampshire and Farnham CCG Managers
Training Implications:	Other than those stated within the policy, there are no further training implications arising from this policy.
Further details and additional copies available from:	Governance Team
Equality Impact Assessment Completed?	The content of this policy does not raise any equality and diversity issues in relation to the protected characteristics
Consultation Process	Corporate Review Group Audit and Risk Committee
Approved by:	Corporate Review Group
Date approved:	11 January 2016

Intranet and Website Upload:

Intranet	Electronic Document Library Location:	
Website	Location in FOI Publication Scheme	
Keywords:	Data Protection, Information Governance, NHS Confidentiality Code of Practice, Caldicott Report 1997 and 2013	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1		5	Include Gender Reassignment Legislation	November 2015
2		6	Include Accredited Safe Haven and Cyber Security information	November 2015
3		7	Change Hampshire IT Solutions to South, Central and West CSU	November 2015
4		7	Include Section 9 – Use of Cloud echnology	November 2015
5		11	Include Gender Reassignment information	November 2015
6		16 & 17 (Appendix 1)	Include information under heading of Managing Protected Information about Transsexual People	November 2015

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
2.0	November 2015	Jackie Thomas, Information Governance Manager, SCW CSU		

Contents

1.0 Introduction

1.1 The NHS North East Hampshire and Farnham Clinical Commissioning Group (CCG) has a legal obligation to comply with all appropriate legislation in respect of, Confidentiality, Data, Information and IT Security. It also has a duty to comply with guidance issued by NHS England, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

1.2 Monetary penalties of up to £500k could be imposed upon the CCG, and/or employees for non-compliance with relevant legislation and NHS guidance.

2.0 Aim

2.1 This Confidentiality Policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 as that is the key piece of legislation covering security and confidentiality of personal information.

3.0 Legislation

3.1 For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. The legislation listed below also refers to issues of security of personal confidential data:

- Data Protection Act 1998
- Access to Health Records 1990
- Access to Medical Reports Act 1988 Human Rights Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008
- Health and Social Care Act 2012
- Section 22 of the Gender Recognition Act 2004

4.0 NHS & Related Guidance

4.1 The following are the main publications referring to security and or confidentiality of personal confidential data:

- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Information Security: NHS Code of Practice
- Employee Code of Practice (Information Commissioner)
- Caldicott Report 1997 and 2013

5.0 Responsibilities

5.1 The Accountable Officer has overall responsibility for the Confidentiality Policy within the CCG. The implementation of, and compliance with this Policy is delegated to the CCG Senior Management Team and will have

responsibility for bringing Information Governance issues to the attention of the CCG Audit and Risk Committee.

5.2 The CSU IG Service Lead role includes:

- Maintaining registrations
- Facilitating training sessions
- Advising on subject access requests
- Acting as initial point of contact for any Information Governance issues which may arise within the CCG
- Being an active member of the Operational Management Team
- Providing reports to the CCG Executive Management Team as required
- Auditing data protection compliance
- Facilitating action in areas identified as being non-compliant
- Assisting with complaints concerning data protection breaches

5.3 This Policy will be reviewed biennially or more frequently if appropriate, to take into account changes to legislation that may occur, and/or guidance from NHS England, Health and Social Care Information Centre and the Information Commissioner or any relevant case law.

5.4 The day to day responsibilities for enforcing this Policy will be devolved to Data Custodians. In order to fulfil their roles, the CSU Information Governance Team will ensure that regular training is provided to remind these personnel of these responsibilities and the most effective way of ensuring adequate information security and confidentiality.

6.0 Security & Confidentiality

6.1 All information relating to identifiable individuals and any information that may be deemed sensitive, must be kept secure at all times. The CCG will ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

6.2 Accredited Safe Havens (ASH) are an accredited organisation with a secure electronic environment in which personal confidential data and/or weakly pseudonymised data can be obtained and made available to users, generally in de-identified form. An accredited safe haven will need a secure legal basis to hold and process personal confidential data. Weakly pseudonymised data can be held under contract with obligations to safeguard the data. The CSU IG Team can advise on the ASH arrangements for the CCG's.

6.3 Information and cyber security concerns the comprehensive risk management, protection and resilience of data processing that the digital networks that connect them. All references to information security are inclusive of cyber security measures.

7.0 Database Management

7.1 The CCG will ensure that all databases that require registration are registered in accordance with the Act's requirements and these registrations are reviewed on a regular basis. Each computer system/database will have a

designated contact/administrator. A list of these nominated personnel will be maintained by the CCG.

7.2 For the purposes of this policy the term “Database” refers to a structured collection of records or data held electronically which contains personal confidential data. In the event that further guidance is needed in respect to what constitutes a database please contact the CSU Information Governance Team.

8.0 Back-ups

8.1 The NHS South, Central and West CSU ICT Service are responsible for ensuring that appropriate back up procedures are available and implemented under the Service Level Agreements in place for the systems they manage and service.

9. Use of Cloud Technology

9.1 Before considering whether a cloud service or cloud provider is right for the CCG, consideration should be given to how it is intended to process personal data in the cloud.

9.2 Once the CCG is clear which personal data it holds and how it intends to process it in the cloud, the associated risk should be assessed and appropriate steps taken to mitigate them. A clear record about the categories of data the CCG intends to move to the cloud should be kept.

9.3 If services within the CCG are looking to process personal data in a cloud service, a privacy impact assessment should be carried out in order to assess and identify any privacy concerns and address them at an early stage. Both the CCG senior information risk owner (SIRO) and Caldicott Guardian should be involved in this process and the decision to proceed should be approved by the appropriate senior management or committee.

9.4 The Data Protection Act requires the CCG, as data controller, to have a written contract with the data processor (cloud provider) which clearly requires the data processor to act only on instructions from the data controller and also requires the data processor to comply with security obligations equivalent to those imposed on the CCG itself.

9.5 The existence of a written contract should mean that the cloud provider will not be able to change the terms of data processing operations during the lifetime of the contract without the CCG’s knowledge and agreement.

9.6 As a data controller, the CCG should ensure appropriate steps are taken to inform the public of the use of the cloud service if any personal identifiable data is to be stored by this method. This should be done via the CCG fair processing notification which should be available on the CCG public website.

9.7 Further information regarding the use of the cloud can be found on the Information Commissioners Office website at ICO - Cloud Information

10.0 Disclosure of Information & Information in Transit

10.1 It is important that information about identifiable individuals (such as the general public and/or staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of identifiable information is also a requirement of the Caldicott recommendations.

10.2 All disclosures of computer held identifiable information should be included in the relevant Information Asset Register.

10.3 Some disclosures of information may occur because there is a statutory requirement upon the CCG to disclose e.g. with a Court Order or because other legislation requires disclosure (for staff to the tax office, pension agency)

10.4 If personal confidential information needs to be transported in any media such as: disc, memory stick or manual paper records, this should be carried out to maintain strict security and confidentiality of this information. For further information regarding transporting, sending and receiving person identifiable information please contact the CSU Information Governance Team.

10.5 Contracts between the CCG and third parties must include an appropriate confidentiality clause that must be disseminated to the third parties employees.

11.0 Disclosure of information outside the European Economic Area (EEA)

11.1 No personal data should be disclosed or transferred outside of the EEA to a country or territory which does not ensure an adequate level of protection unless certain exemptions apply or adequate protective measures are taken.

11.2 In the event that there is a need to process personal information outside of the United Kingdom, the CSU Information Governance Team must be consulted prior to any agreement to transfer or process the information.

12.0 Training for Data Custodians

12.1 The CSU Information Governance Team has overall responsibility for maintaining awareness of confidentiality and security issues for all staff. Detailed training given to the Data Custodians will cover:

- How to provide awareness to teams regarding their personal responsibilities, such as locking doors and avoiding gossip in open areas
- Confidentiality of personal information
- Relevant NHS Policies and Procedures e.g. Record Management Lifecycle Protocol
- Compliance with the Data Protection Principles
- Registration of automated databases
- Individuals rights (access to information and compliance with the principles)
- General good practice guidelines covering security and confidentiality
- Contact details for the CSU IG Team

- A general overview of all Information Governance requirements
- How to inform staff about the relevant policies and procedures and also how to provide good practice guidance.
- A brief overview of the Data Protection and Freedom of Information Acts.

13.0 Training

13.1 All new starters to the CCG must undertake Information Governance training via the online IG Training tool, to include compliance with the Data Protection Act and general IT security training, as part of the induction process. Extra training in these areas will be given to those who need it such as Data Custodians and those dealing with requests for information. A register will be maintained of all staff who have completed the online training and those who have attended face to face sessions.

13.2 Annual IG refresher training should be undertaken by all CCG staff via the Information Governance Training Tool

13.3 All staff will be made aware of what could be classed as an information security incident or breach of confidentiality. They will be made aware of the process to follow and the forms to complete, so that incidents can be identified, reported, monitored and investigated. Please see the CCG Information Governance SIRI Reporting Policy for further guidance on this area.

14.0 Contracts of Employment

14.1 Staff contracts of employment are produced and monitored by the CSU Human Resources department. All contracts of employment include a clause on data protection and general confidentiality. Agency and non-contract staff working on behalf of NHS must be subject to the same rules via a confidentiality agreement.

14.2 All CCG employees will be made aware of their responsibilities in connection with the Acts mentioned in this Policy through their Statement of Terms and Conditions.

15.0 Disciplinary

15.1 A breach of the Data Protection requirements could result in a member of staff facing disciplinary action. A copy of the CCG Disciplinary Procedure is available from the CSU Human Resources Department.

16.0 Monitoring & Audit

16.1 This policy will be monitored by the Senior Management Team to ensure any legislative changes that occur before the review date are incorporated. All exceptions will be reported to the Audit and Risk Committee. This policy will also be reviewed every 2 years.

16.2 Please refer to the CCG Subject Access Request Policy for guidance on how to handle a Subject Access Request

17.0 Disclosure of Personal and Confidential Information

17.1 To ensure that information is shared appropriately, care must be taken to check that there is a firm legal basis in place.

17.2 It is important to consider how much confidential information is required and ensure that the minimal amount necessary is disclosed.

17.3 Information can be disclosed:

- When effectively anonymised.
- When the information is required by law or under a court order, which may include the detection and prevention of serious crime. In this situation staff must discuss with their Line Manager or the CSU Information Governance Team before disclosing, they will then inform and obtain approval of the CCG Caldicott Guardian.
- In identifiable form, with the individual's written consent or with support from NHS England who will apply for the necessary approval from the appropriate authority for example, the Confidentiality Advisory Group (CAG) within the Health Research Authority.
- In potential safeguarding situations or when it is deemed in the public interest and before disclosure takes place, staff should contact their line manager and the CSU Information Governance Team, who will then inform and obtain approval from the CCG Caldicott Guardian.

17.4 When necessary a Data Sharing, Data Re-Use or Data Transfer Agreement should have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the CSU Information Governance Team

17.5 Care must be taken when transferring information to ensure that the method used is secure. Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and post. See the Safe Haven Procedure for guidance on the safe transfer of personal confidential data.

17.6 CCG Staff may only transfer personal, confidential or commercially sensitive information by using either an NHS.net account or Secure File Transfer. Staff should also be aware that this security is only assured if the email is transferred by nhs.net to one of the following other secure email addresses:

another NHS.net account	x.gsi.gov.uk	gsi.gov.uk
gse.gov.uk	gsx.gov.uk	pnn.police.uk
cjsm.net	scn.gov.uk	gcsx.gov.uk
mod.uk		

If information is required to be sent to a member of the public, using their non-secure email address, it is the responsibility of the member of staff to ensure that the member of public is provided with a clear explanation of the risks of using unsecure email addresses and consent should be obtained.

17.7 There are Acts of Parliament that govern the disclosure of personal information. Some of these Acts make it a legal requirement to disclose and others that state that information cannot be disclosed. These Acts are detailed below:

- Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to NHS Public Health England from schools)
- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- Children Act 2004
- Section 22 of the Gender Recognition Act 2004

17.8 In the event that a request for disclosure is made referencing any of these Acts the CSU information governance team must be notified prior to any information being released.

17.9 Managing protected information about transsexual people. Section 22 of the Gender Recognition Act 2004 says that:

> 'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.'

17.10 'Protected information' means information which relates to a person who has made an application under the Gender Recognition Act. This covers both the fact of the application itself and, if the application was successful, the fact that the individual was previously of the opposite gender to the one in which they are now legally recognised. See Appendix 1 for more information.

18.0 Working away from the office environment

18.1 There will be times when staff may need to work from another location or while travelling. This means that these staff may need to carry CCG information with them which could be confidential in nature e.g. on a laptop, USB stick or as paper documents.

18.2 Taking home/removing paper documents that contain personal confidential data from CCG premises should be discussed with your line manager to identify potential risks.

18.3 When working away from CCG locations, staff must ensure that their working practice complies with the CCG policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance.

18.4 Staff must not leave confidential information unattended whilst travelling and ensure that it is kept in a secure place if they take it home or to another location.

18.5 Staff must minimise the amount of person confidential data that is taken away from CCG premises.

18.6 If staff need to carry personal confidential data they must ensure that any personal information is transported in an appropriate and secure manner and is kept out of sight whilst being transported

18.7 Staff are responsible for ensuring that any information taken home is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information

18.8 Staff must not forward any personal confidential data via email to their home email account. Staff must not use or store personal identifiable or confidential information on a privately owned computer or device.

19.0 Staff Responsibilities

19.1 All staff have a legal duty of confidence to keep personal confidential data private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about personal confidential data in public places or where they can be overheard
- Leave any personal confidential data lying around unattended, this includes telephone messages, computer printouts, faxes and other documents
- Leave a computer logged on to a system where personal confidential data can be accessed

19.2 Steps must be taken to ensure physical safety and security of personal identifiable or business confidential information held in paper format and on computers

19.3 Passwords must be kept secure and must not be disclosed. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality under the Computer Misuse Act 1990 . This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

20.0 Abuse of Privilege

20.1 It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other

persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and the Data Protection Act.

20.2 Members of staff who would like access to their personal confidential information must submit a subject access request under the Data Protection Act 1998 to the CSU Information Governance Team.

21.0 Confidentiality Audits

21.1 Good practice requires that all organisations that handle personal confidential data put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the CCG Data Custodian through a programme of audits.

Appendix 1: Summary of Legal and NHS Mandated Frameworks

The CCG are obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the CCG, who may be held personally accountable for any breaches of information security for which they may be held responsible. The CCG shall comply with the following legislation and guidance as appropriate:

The **Data Protection Act (1998)** regulates the use of "personal data" and sets out eight principles to ensure that personal data is:

1. Processed fairly and lawfully.
2. Processed for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date.
5. Not kept longer than necessary, for the purpose(s) it is used.
6. Processed in accordance with the rights of the data subject under the Act.
7. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data
8. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

The Caldicott principles should be applied when considering personal confidential data:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

Article 8 of the **Human Rights Act (1998)** refers to an individual's "*right to respect for their private and family life, for their home and for their correspondence"*. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The **Computer Misuse Act (1990)** makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

    a. Making, supplying or obtaining articles for use in offences 1-3

The **NHS Confidentiality Code of Practice (2003)** outlines four main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

- Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

- Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers.

The NHS Care Record Guarantee

- The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: Patients' rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made.

  The most relevant are:
  Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and
- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of
- Practice and other national guidelines on best practice.

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Managing Protected Information about Transsexual People

Section 22 of the Gender Recognition Act 2004 says that:

> 'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.'

'Protected information' means information which relates to a person who has made an application under the Gender Recognition Act. This covers both the fact of the application itself and, if the application was successful, the fact that the individual was previously of the opposite gender to the one in which they are now legally recognised.

A person acquires information in an 'official capacity' if they are acting:

- In connection with the functions of a public authority like the CCG
- As an employer, or prospective employer, of the person to whom the information relates or as a person employed by such an employer or prospective employer, or
- In the course of, or otherwise in connection with, the conduct of business or the supply of professional services.

It is not an offence to disclose information obtained in these circumstances if:

- The information does not enable the person to be identified, or
- That person has agreed to the disclosure of the information, or
- The person making the disclosure genuinely does not know or believe that a full gender recognition certificate has been issued, or
- The disclosure is in accordance with an order of a court or tribunal, or
- The disclosure is for the purpose of instituting proceedings before a court or tribunal, or
- The disclosure is for the purpose of preventing or investigating crime, or
- The disclosure is made to the Registrar General for England and Wales, the Registrar General for Scotland or the Registrar General for Northern Ireland, or
- The disclosure is made for the purposes of the social security system or a pension scheme, or
- The disclosure is in accordance with provisions made through regulations which the Secretary of State is permitted to make under the Act.

The law does not apply to information about a person’s gender recognition application or gender reassignment history when the information originates outside of an official setting – through social contact, for instance.

CCG staff must be careful about what they record and file about a transsexual person (or what was recorded and filed in the past) so as to avoid others from seeing information which becomes protected as a result of a gender recognition application and legal recognition.

Further guidance is available

http://www.legislation.gov.uk/ukpga/2004/7/section/22
http://www.equalityhumanrights.com/advice-and-guidance/your-rights/transgender/
http://www.gires.org.uk/GRA.php.

Appendix 2 Confidentiality Agreement

Confidentiality agreement – NHS North East & Farnham Clinical Commissioning Group

Document name	NHS North East Hampshire & Farnham Clinical Commissioning Group Confidentiality Agreement	
Date:	03/02/2012	
Author	NHS North East Hampshire & Farnham Clinical Commissioning Group	
Version	1	

Confidentiality agreement for third party suppliers

Who are third parties covered by this agreement?

Third party suppliers granted access to NHS North East Hampshire & Farnham Clinical Commissioning Group data and information in order to perform tasks as required by NHS North East Hampshire & Farnham Clinical Commissioning Group. They could include the following:

- Hardware and software maintenance and support staff (for all of the document)
- Cleaning, catering, security guards and other outsourced support services (for general contractor clause and form on back page)

General contractor clause
(based on clause from Introduction to Data Protection in the NHS)

The Contractor undertakes:

- To treat as confidential all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the contractor or an employee, servant or agent or sub-contractor of the contractor as a result or in connection with the contract; and

- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his employees, servants, agents or sub-contractors; and

- To ensure that they, their employees, servants, agents and sub-contractors are aware of the provisions of the Data Protection Act 1998 and ISO/IEC 27002 and that any personal information obtained from the CCG shall not be disclosed or used in any unlawful manner; and

- To indemnify the CCG against any loss arising under the Data Protection Act 1998 caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

All employees, servants, agents and/or sub-contractors of the Contractor will be required to agree to and sign a confidentiality statement when they come to any of the CCG sites where they may see or have access to confidential personal and/or business information (see last page).

Supplier Code of Practice

The following Code of Practice applies where access is obtained to CCG information for the fulfilment of a required service.

The access referred to in paragraph 1 above may include:-

- Access to data/information on the CCG premises
- Access to data/information from a remote site
- Examination, testing and repair of media (e.g. fixed disc assemblies)
- Examination of software dumps
- Processing using CCG data/information

The Supplier must certify that his organisation is registered if appropriate under the Data Protection Act 1998 and legally entitled to undertake the work proposed.

The Supplier must undertake not to transfer any personal data/information out of the European Economic Area (EEA) unless such a transfer has been registered, approved by the CCG and complies with the Information Commissioners guidance on Safe Harbours.

The work shall be done only by authorised employees, servants, or agents of the contractor (except as provided in paragraph 12 below) who are aware of the requirements of the Data Protection Act 1998 of their personal responsibilities under the Act to maintain the security of the CCG's personal data/information.

While the data/information is in the custody of the contractor it shall be kept in appropriately secure means.

Any data/information sent from one place to another by or for the contractor shall be carried out by secure means. These places should be within the suppliers own organisation or an approved sub-contractor.

Data/Information which can identify any patient/employee of the CCG must only be transferred electronically if previously agreed by the organisation. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 1998 and BS7799. This will also apply to any direct-dial access to a computer held database by the supplier or their agent.

The data/information must not be copied for any other purpose than that agreed by the supplier and the CCG.
Where personal data/information is recorded in any intelligible form, it shall either be returned to the CCG on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to the organisation.

Where the contractor sub-contracts any work for the purposes in paragraph 1 above, the contractor shall require the sub-contractor to observe the standards set out in this agreement.

The CCG shall, wherever practical, arrange for the equipment or software to be maintained, repaired or tested using dummy data that does not include the disclosure of any personal data/information.

The CCG reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The CCG will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the suppliers employee and/or any agents and/or sub-contractors.

Any security breaches made by the supplier's employees, agents or sub-contractors will immediately be reported to the CCG Caldicott Guardian.

Certification form:

Name of supplier: _____

Address of supplier
prime contractor: _____

_____

_____

_____

Telephone number: _____

E-mail details: _____

On behalf of the above organisation I certify as follows:

The organisation is appropriately registered under the Data Protection Act 1998 and is legally entitled to undertake the work agreed in the contract agreed with the Organisation

The organisation will abide by the requirements set out above for handling any of the organisation personal data/information disclosed to my organisation during the performance of such contracts

Signed: _____

Name of Individual: _____

Position in organisation: _____

Date: _____

Agreement outlining personal responsibility concerning security and confidentiality of information (relating to patients, staff and the business of the organisation)

During the course of your time within the CCG buildings, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties as detailed in the contract between the CCG and your employer. This condition applies during your time within the CCG and after that ceases.

Confidential information includes all information relating to the business of the CCG and its patients and employees.

The Data Protection Act 1998 regulates the use of all personal information and included electronic and paper records of identifiable individuals (patients and staff). The CCG is registered in accordance with this legislation. If you are found to have used any information you have seen or heard whilst working within the CCG for any other purpose than that which it was shared with you both you and your employer may face legal action.

I understand that I am bound by a duty of confidentiality and agree to adhere to the conditions within the Contract between the organisations and my personal responsibilities to comply with the requirements of the Data Protection Act 1998.

NAME OF ORGANISATION:	
CONTRACT DETAILS:	
PRINT NAME:	
SIGNATURE:	
DATE:	