South East Coast Ambulance Service NHS
NHS Foundation Trust

Data Protection Policy

Version:	V5.0
Approved by:	Senior Management Team
Date approved:	3 November 2017
Name of originator/ author:	Information Governance Manager
Date issued:	6 November 2013
Date next review due:	3 November 2019
Target audience:	All staff and contractors
Replaces:	V4.0

Document Control

Manager Responsible

Name:	Caroline Smart
Job Title:	Information Governance Manager
Directorate:	Quality & Safety

Committee/Working Group to approve	Senior Management Team	
Version No. 4.00	Final	Date: 05/09/2013
Version No. 5.00	Review	Date: 03.11.17

Draft/Evaluation/Approval (Insert stage of process)

Person/Committee	Comments	Version	Date
Senior Management Team	Review policy	V5.00	03.11.17
Joint Partnership Forum		V5.00	30.10.17
RMCGC	Approved	V4.00	05/09/2013
CWG	Recommended for approval. Further work to take place in future to help simplify the Policy for all staff members.	V3.02	19/06/2013
Corporate Information, Data Quality and Protection Manager	Reviewed and updated to reflect changes to Job roles and responsibilities	V3.02	11/06/2013
Corporate Records Administrator	Updated to reflect changes made following the Directorate restructure	V3.01	22/03/2013
RMCGC	RMCGC approval on 12 September 2011 for Trust Documents to be updated to reflect current workforce structure and Foundation Trust status, without the need to represent to Committee or Working Group for approval.	V3.00	12/09/2011
Corporate Records Administrator	Reformatted to reflect FT status and changes in roles following workforce review	V2.01	07/12/2011
RMCGSC Extraordinary meeting	Approved	V2.0	23/03/2009
IG	Reformatted	V1.3	17/02/2009

Head of IG	Reformatted and s3, 7, 8 and 10 added	V1.2	26/01/2009
IGWG	For review	V1.1	15/12/2008
IG Admin	Re-formatted	V1.1	24/09/2008
RMCGSC	Approved	V1.0	13/09/2007

Circulation

Records Management Database	Date: 06.11.17
Internal Stakeholders	
External Stakeholders	

Review Due

Manager	Information Governance Manager	
Period	Two years or sooner on system change, i.e. new legislation, codes of practice or national standards	Date: November 2019

Record Information

Security Access/Sensitivity	Public domain
Publication Scheme	Yes
Where Held	Records Management database
Disposal Method and date:	Non confidential waste, 3 years after replacement

Supports Standard(s)/KLOE

	NHS Litigation Authority (NHSLA)	**Care Quality Commission (CQC)**	**Auditors Local Evaluation (ALE)**	**IG Toolkit**	**Other**
Criteria/KLOE:	**1.1.8**	**13c**		**201, 202**	

Contents

1 Introduction

1.1. The South East Coast Ambulance Service NHS Foundation Trust ('the Trust') has a legal obligation to comply with all relevant legislation in respect of Data, Information and IT Security. It also has a duty to comply with guidance issued by the Department of Health, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

1.2. For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. A brief summary of the Data Protection Act 1998, associated legislation and guidelines is provided in Appendix 1.

2 Aims and Objectives

2.1. This Data Protection Policy aims to detail how the Trust 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 which is the key piece of legislation covering information security and confidentiality of personal information.

3 Definitions

3.1. **Data protection principles**: There are eight principles of good practice within the Data Protection Act 1998 which must be adhered to when processing personal data (see Section 5).

3.2. **Data controller:** means, "... 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"

3.3. **Personal data**: means "data which relate to a living individual who can be identified

3.3.1. From those data; or

3.3.2. From those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

3.3.3. And includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

3.4. **Sensitive personal data** means "personal data consisting of information" as to:

3.4.1. Racial or ethnic origin of the data subject,

3.4.2. Political opinions,

3.4.3. Religious beliefs or other beliefs of a similar nature,

3.4.4. Whether a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),

3.4.5. Physical or mental health or condition,

3.4.6. Sexual life,

3.4.7. The commission or alleged commission the individual of any offence, or

3.4.8. Any proceedings for any offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings".

4 Policy Statement

4.1. The Trust is committed to ensuring that it fully complies with the eight principles of good practice within the Data Protection Act 1998 when conducting its business, through adherence to robust procedures and the provision of guidance and training.

5 Arrangements

5.1. **Principle 1:** Personal data shall be processed fairly and lawfully.

5.1.1. **Publicising the Capture of Personal Data**

5.1.1.1. There is a requirement to make the general public, and those who use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. The Trust is obliged under the Data Protection requirements and Caldicott recommendations to produce patient information leaflets and posters which are customised to its own uses of patient information.

5.1.2. **Staff**

5.1.2.1. The Trust must notify staff, temporary employees (volunteers, locums) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed. This may occur during induction or by their individual manager.

5.1.3. **Patients**

5.1.3.1. Patients will be made aware of this requirement by the use of information posters and/ or information leaflets and verbally by those health care professionals providing care and treatment. They may also find information relating to this on the Trust website as defined by a Privacy Notice.

5.1.3.2. Patient information leaflets are available upon request from the Information Governance department.

5.2. **Principle 2:** Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

5.2.1. **Notification**

5.2.1.1. All databases that hold and/ or process personal information about living individuals must be registered with the Office of the Information Commissioner. This process is known as notification. If the Trust fails to complete this process and keep the information up to date it has committed a criminal offence and could face criminal prosecution.

5.2.1.2. The Information Governance Manager will ensure all relevant databases are registered. A nominated person will be responsible for each registered database and known as the data owner. A log of databases and nominated data owners will be maintained by the Information Governance Manager.

5.2.1.3. A database is any collection of personal information that can be processed by automated means (e.g. by machine/ computer). This could include patient, staff or contractor records; patient information used for research, e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this could be a spreadsheet or database;

5.2.1.4. If any system makes automated decisions it must also be noted in the log of databases. An automated decision is where the decision is made by automated means, not by human judgement. This could relate to a person's performance at work or where they are short listed for a job based solely on answers given by, for example, a touch tone phone. Where other information is used to base a decision, that is to say that other human factors are involved, it is not purely automated decision making. The reason for noting this here is that individuals have a right of access to their own personal information and if any decision is made by automated means, they have the right to know the logic used in the decision making process. More information can be found at: www.ico.gov.uk. and in the data protection subject access procedures.

5.2.1.5. It is also necessary to ascertain whether any identifiable personal information is disclosed to any country outside of the European Economic Area (EEA). This may occur where a software supplier based outside of the EEA has local offices within it, but sometimes needs to send personal data to its main office to rectify software issues. Where disclosures are likely to occur, further advice will need to be sought from the Information Governance Manager who may need to contact the Information Commissioner's office for guidance. Any identified disclosures will be presented to the Information Governance Working Group (IGWG) for consideration, to ensure no breaches of the Act occur.

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

5.3.1. Information collected from individuals will be complete and must all be justified as being required for the purpose it is being requested. It is sometimes necessary to justify information needs on an item-by-item basis.

5.4. **Principle 4:** Personal data shall be accurate and, where necessary, kept up to date.

5.4.1. The Trust will ensure that all information held on any media is accurate and up to date. The accuracy of the information can be determined by implementing validation routines, some of which will be system specific. Details must be provided of these validation processes to the system/information users.

5.4.2. Data owners are responsible for the quality (i.e. Accuracy, Timeliness, and Completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

5.4.3. Staff information must also be checked for accuracy on a regular basis by the Human Resources department.

5.5. **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.

5.5.1. All records are affected by this principle regardless of the media in which they may be held, stored or retained. An updated Records Management Code of Practice for Health and Social Care 2016 has been published by the Information Governance Alliance (IGA)and provides comprehensive guidance for all NHS organisations.

5.5.2. Details of how this affects the Trust, and the actions required to comply with it, are detailed in the Records Management Policy and the Records Management: Retention and Disposal Guidance.

5.5.3. If the information on the computer or manual record is not the main record, this is considered to be transient data, and procedures must be put in place to give guidance to these users that the information must be culled, archived or destroyed when no longer deemed to be of use.

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

5.6.1. **Individual's Rights – including Subject Access/ Right to Complain**

5.6.1.1. Under this principle, individuals have the following rights:

5.6.1.1.1. Right of subject access (for further information, see below);

5.6.1.1.2. Right to prevent processing likely to cause harm or distress;

5.6.1.1.3. Right to prevent processing for the purposes of direct marketing;

5.6.1.1.4. Right in relation to automated decision taking (see 5.2.1.4);

5.6.1.1.5. Right to take action for compensation if the individual suffers damage;

5.6.1.1.6. Right to take action to rectify, block, erase or destroy inaccurate data;

5.6.1.1.7. Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

5.6.2. The extent and nature of some of these rights have yet to be fully determined. Although guidance is available, this has not been tested by the courts.

5.6.3. **Subject Access**

5.6.3.1. Individuals whose information is held within the Trust have rights of access to it regardless of the media on which the information may be held/ retained. Individuals also have a right to complain if they believe that the Trust is not complying with the requirements of the Data Protection legislation.

5.6.3.2. The Trust must ensure an up to date procedure is in place to deal with requests for access to information. Further details are set out in the Trust's Data Subject Access Request Policy and Procedure.

5.6.3.3. The Access to Health Records Act 1990 provides access rights to personal representatives, or those who may have a claim, to deceased patients' manual/ paper records.

5.6.4. **Compensation**

5.6.4.1. Individuals have a right to seek compensation for any breach of the Act that may cause them damage and/ or distress.

5.6.5. **Complaints**

5.6.5.1. The Trust's complaints' procedures take account of complaints that may be received because of a breach or suspected breach of the Data Protection Act 1998.

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

5.7.1. **Security**

5.7.1.1. All information relating to identifiable individuals must be kept secure at all times. The Trust will ensure there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Details of how this occurs will be within the Information Security and Risk Management Policy. Other policies that pertain to this are listed in section 11.

5.7.1.2. Measures will be taken by the Head of IT to ensure that all software and data is removed from redundant hardware and media storage (e.g. tapes, disks) before the hardware is removed from the Trust.

5.7.1.3. Confidential paper waste will be shredded or collected and held in a secure area prior to shredding/ incinerating.

5.7.2. **Disposal of Non-Clinical Waste**

5.7.2.1. The Trust has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and Trust business. It is important that this information is disposed of in a secure manner.

5.7.2.2. All employees will be made aware of how easy it is to breach confidentiality by incorrect use of waste paper, by using examples of 'real life situations' during training sessions. Staff will be informed how to dispose of person-identifiable waste products.

5.7.3. **Data Owners**

5.7.3.1. The data owner is the person responsible for ensuring that a system and its users comply with the current Data Protection legislation. This will include responsibility for ensuring that the notification of the

system is kept up to date and that procedures are in place to achieve a high level of data quality. Each system will have a designated data owner who will ensure that:

5.7.3.1.1. The Data Protection notifications are up to date;

5.7.3.1.2. Users are set up on the system on a need to know basis;

5.7.3.1.3. Expert advice is available regarding Data Protection issues;

5.7.3.1.4. Disclosures of information are checked against the notifications;

5.7.3.1.5. Unusual requests for disclosure are scrutinised and advice taken from the Caldicott Guardian when necessary;

5.7.3.1.6. Their staff are aware of their responsibilities regarding security, data protection and confidentiality issues.

5.7.4. **Back-ups**

5.7.4.1. Each data owner will have responsibility for ensuring there is a procedure that outlines the media, frequency and retention period for back-ups of the data and programs for the systems within their control.

5.7.5. **Disclosure of Information/ Information in Transit**

5.7.5.1. It is essential that information about identifiable individuals (such as patients and staff) is only disclosed on a need to know basis. Strict controls governing the disclosure of patient identifiable information are also a requirement of the Caldicott recommendations.

5.7.5.2. All disclosures of person-identifiable information must be included in the relevant data protection notification document for the database from which the disclosure may be made.

5.7.5.3. Some disclosures of information may occur because there is a statutory requirement upon the Trust to disclose, e.g. with a Court Order; or because other legislation requires disclosure (for staff to the tax office, pension agency and for patients to the Department of Health if the patient has a notifiable disease).

5.7.5.4. If person identifiable information/ records need to be transported in any media such as: magnetic tape, compact disk etc or manual paper records, this will be carried out in a manner that maintains the strict security and confidentiality of this information.

5.7.5.5. Reliable transport couriers will be used at all times. Packaging must be sufficient to protect the contents from any physical damage during transit, and must be in accordance with manufacturers' specifications.

5.7.5.6. Contracts between the Trust and third parties will include an appropriate confidentiality clause that must be disseminated to the third parties' employees.

5.8. **Principle 8:** Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.8.1. If it is necessary to send person identifiable information to countries outside the EEA, it must be discussed with the Information Governance Managers the levels of protection for the information may not be as comprehensive as those in the UK. If the consent of the individual has been gained it is normally acceptable to proceed with the request: however, it is still best practice to seek advice before sending. It may also be necessary to check with software suppliers to ensure they conduct any development and bug fixes etc. within the UK or EEA. If the Trust wished to post person-identifiable information on their own web site, it is also necessary to consider the requirements of this principle.

5.8.2. Current guidance on this topic may be found on the Information Commissioner's website at: www.ico.gov.uk.

5.9. **Contracts of Employment**

5.9.1. Staff contracts of employment are produced and monitored by the Trust's Human Resources department. All contracts of employment will include a data protection and general confidentiality clause. Agency and non-contract staff working on behalf of the Trust will be subject to the same rules.

5.9.2. All Trust employees will be made aware of their responsibilities in connection with the Acts mentioned in this policy through their Statement of Terms and Conditions, and targeted training sessions carried out by data owners, managers and/ or other trainers/ specialists.

5.10. **Disciplinary**

5.10.1. A breach of the Data Protection Act may result in staff facing disciplinary action in accordance with Trust policy. A copy of the Trust's Disciplinary Policy is available from the Human Resources Department.

6 Responsibilities

6.1. The Chief Executive Officer (CEO) has overall responsibility for the Data Protection Policy within the Trust. The implementation of, and compliance with, this policy is delegated to the Director of Strategy

& Business Development (SIRO) Services and other designated personnel, including the Caldicott Guardian, Information Governance Manager and data owners.

6.2. The Freedom of Information Co-ordinator is the initial point of contact for freedom of information requests.

6.3. Requests from patients and their relatives for access to health records are managed by the Complaints and PALs Officers;

6.4. Requests from Solicitors, Insurance Companies, Police and Coroners will be handled by the Trust Legal Team through its Legal Administrators

6.5. Key responsibilities include:

6.5.1. Logging all information requests within the Trust's Risk Management database;

6.5.2. Forwarding them to the appropriate data owner/ manager for action auditing data protection compliance;

6.5.3. Providing guidance on the interface between data protection and freedom of information.

6.6. The Information Governance Working Group is responsible for bringing data protection issues to the Executive Management Team the Trust Board as appropriate. This role includes:

6.6.1. Maintaining accurate notifications with the Office of the Information Commissioner (including ensuring that all databases that require registration are registered in accordance with the Act's requirements and these registrations are reviewed on a regular basis);

6.6.2. Contributing content to induction and training sessions;

6.6.3. Providing guidance regarding any data protection issues that may arise within the Trust;

6.6.4. Assisting with complaints concerning data protection breaches;

6.6.5. Preparing reports for the Information Governance Working Group as required;

6.6.6. Providing guidance regarding any data quality issues that may arise within the Trust;

6.6.7. Assisting with complaints concerning data protection breaches.

6.7. Each computer system/ database must have a designated data owner, this forms part of an overarching Information Asset Register. A list of these nominated personnel will be maintained by the

Information Governance Working Group. They will have the day to day responsibility for enforcing this policy. Regular refresher training will be provided to them to ensure that they are aware of their responsibilities and the most effective way of ensuring adequate information security and confidentiality.

6.8. The Trust has appointed a Caldicott Guardian, who is currently the Medical Director. The Caldicott Guardian will provide advice and guidance where required, in line with the guidance in HSC 2002/2003, particularly in cases where a non-routine disclosure is in question.

7 Competence

7.1. All staff are required to complete Information Governance training as part of their induction on joining the Trust's employment and to undertake Statutory and Mandatory training on an annual basis through completing the IG training modules within SECAmb. The Trust will offer more specialised in-house training to those whose role indicates that this is required. The Information Governance Working Group is expected to provide expertise in the application of the Data Protection Act 1998 and will be able to provide advice and guidance.

7.2. Generic training will include:

7.2.1. Personal responsibilities;

7.2.2. Confidentiality of personal information;

7.2.3. Relevant Trust Policies and Procedures;

7.2.4. Compliance with the Data Protection Principles;

7.2.5. Compliance with Caldicott principles;

7.2.6. Individuals' rights (access to information and compliance with the principles);

7.2.7. General good practice guidelines covering security and confidentiality;

7.2.8. Awareness of managerial responsibility for Data Protection and contact points for all issues that may occur in the areas of security and confidentiality of personal information;

7.2.9. A general overview of all Information Governance components;

7.2.10. A brief overview of how the Data Protection and Freedom of Information Acts work and their differences;

7.2.11. How to report incidents/ learning events;

7.2.12. How the Trust manages Information Governance and who the main contacts are.

7.3. A register will be maintained of all staff attendance at the training sessions. Non-contract staff and those on short or fixed term contracts will also receive appropriate induction.

8 Monitoring

8.1. The Information Governance Working Group is alerted to pertinent information Governance issues or near misses through the incident reporting and complaints procedures. A log of such issues is presented to the bi-monthly Information Governance Working Group for review

9 Audit and Review

9.1. This policy will be reviewed every two years or more frequently if appropriate, by the Information Governance Working Group to take into account changes to national legislation that may occur, and/ or guidance from the Department of Health, the Information Commissioner and/ or any relevant case law.

9.2. When deemed appropriate, the Trust may commission internal audit to review compliance with these arrangements.

10 Equality Impact Appraisal

10.1. The Trust will undertake an Equality Impact Appraisal to determine whether any groups may be adversely affected by this policy; and if so, how this impact may be mitigated.

11 Associated Documentation

11.1. Data Subject Access Request Policy and Procedure

11.2. Information Governance Policy

11.3. Information Governance Strategy

11.4. Information Security and Risk Management Policy

11.5. Internet and E-mail Policy

11.6. Freedom of Information Policy

11.7. Records Management Policy

11.8. Records Management Retention and Disposal Guidelines

11.9. PALS and Complaints Policy

12 References

12.1. **Primary Legislation**

12.1.1. Access to Health Records Act 1990

12.1.2. Access to Medical Reports Act 1988

12.1.3. Caldicott Principles

12.1.4. Children Act 1989

12.1.5. Computer Misuse Act 1990

12.1.6. Copyright, Designs and Patents Act 1988

12.1.7. Crime & Disorder Act 1998

12.1.8. Data Protection Act 1998

12.1.9. Electronic Communications Act 2000

12.1.10. Freedom of Information Act 2000

12.1.11. Health and Social Care Act 2001

12.1.12. Human Rights Act 1998

12.1.13. Police and Criminal Evidence Act 1984

12.1.14. Public Records Act 1958

12.1.15. Regulation of Investigatory Powers Act 2000

12.2. **Secondary Legislation**

12.2.1. The Data Protection (Processing of Sensitive Personal Data) Order 2000 [SI 2000 No. 417]

12.2.2. The Data Protection (Subject Access Modification) (Health) Order 2000 [SI 2000 No. 413]

12.2.3. The Data Protection (Subject Access Modification) (Education) Order 2000 [SI 2000 No. 414]

12.2.4. The Data Protection (Subject Access Modification) (Social Work) Order 2000 [SI 2000 No. 415]

12.2.5. The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 [SI 2000 No. 419]

12.2.6. The Data Protection (Miscellaneous Subject Access Exemptions (Amendment) Order 2000 [SI 2000 No. 1865]

12.2.7. The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 [SI 2000 No. 191]

12.3. **NHS and Related Guidance**

12.3.1. Confidentiality: NHS Code of Practice (August 2003)

12.3.2. Employee Code of Practice (Information Commissioner)

12.3.3. HSC2000/009: Data Protection Act 1998: Protection and Use of Patient Information

12.3.4. HSC1999/053: For the Record (preservation, retention and destruction of records under the Public Records Act 1958) and records management strategy

12.3.5. HSC2002/3: Implementing the Caldicott Standard into Social Care

12.3.6. BS7799: British Standard for Information Management and Technology.

Appendix 1: Overview of Legislation and NHS Guidance

1 Data Protection Act 1998

1.1. This Act is the key piece of legislation and is therefore covered in detail. Summaries of other Acts mentioned above are shown at Appendix 2.

1.2. This Act applies to all person identifiable information held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records and other manual files such as microfiche/ film.

1.3. The Act dictates that information must only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty. Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

1.4. The Act also requires the Trust to register its data holdings (information held on computers and other automated equipment) with the Office of the Information Commissioner, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. The Trust also has to comply with the principles of good practice known as the Eight Data Protection Principles. Failure to register, an incorrect registration or an outdated registration is a criminal offence. This may lead to the prosecution of the Trust.

1.5. All applications/ databases required under law to be registered for Data Protection purposes will be registered under the Trust's global registration with the Information Commissioner and will comply with the Data Protection Act 1998. This will primarily be achieved by adhering to the policies of the Trust and following the Eight Data Protection Principles.

1.6. Under a provision of the Data Protection Act an individual can request access to their information regardless of the media this information may be held/ retained. The Trust will develop a Data Protection Subject Access Policy and Procedure for dealing with such requests.

2 NHS and Related Guidance

2.1. Confidentiality: NHS Code of Practice

2.1.1. This provides detailed guidance for NHS bodies concerning confidentiality and patients' consent to use their health information. It also details the required practice the NHS must take concerning

security, identifying the main legal responsibilities for an organisation and also details employees' responsibilities (www.dh.gov.uk).

2.2. **Employee Code of Practice**

2.2.1. This is guidance produced by the Information Commissioner detailing the data protection requirements that relate to staff/ employee and other individuals' information www.ico.gov.uk.

2.3. **HSC2002/003 Caldicott Guardians & Implementing the Caldicott Standard into Social Care**

2.3.1. Provides guidelines relating to sharing of patient identifiable information and promotes the appointment of a senior health professional to oversee the implementation of the guidance. It also re-iterates guidance produced in 1999 for NHS Caldicott Guardians (www.dh.gov.uk search by Confidentiality).

2.4. **NHS Records Management Code of Practice for Health & Social Care 2016**

2.4.1. Provides guidance to improve the management of NHS records, explains the requirements to select records for permanent preservation, lists suggested minimum requirements for records retention and applies to all information, regardless of the media, applicable to all personnel within the NHS such as patients, employees, volunteers etc. It aids compliance with the Data Protection and Freedom of Information Acts (www.dh.gov.uk search by circular details).

2.5. **ISO/IEC 17799 Information Security Standards**

2.5.1. This is the accepted industry standard for Information Management and Security. This standard has been adopted by all NHS organisations. It is also a recommended legal requirement under principle 7 of the Data Protection Act.

Appendix 2: Other Relevant Acts of Parliament

1 Access to Health Records 1990

1.1. This Act gives patients' representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons' records. All other requests for access to information by living individuals are handled under the access provisions of the Data Protection Act 1998.

2 Access to Medical Reports Act 1988

2.1. This Act allows those who have had a medical report produced for the purposes of employment and/ or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/ or prospective insurance company.

3 Human Rights Act 1998

3.1. This Act became law on 2 October 2000. It binds public authorities, including all Trusts and individual doctors treating NHS patients, to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and their right to expect confidentiality of their information at all times.

3.2. Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

3.3. Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

4 Freedom of Information Act 2000

4.1. This Act came into force on 1 January 2005. It gives individuals right of access to corporate information held by the Trust such as policies, reports and minutes of meetings. The Trust has a Freedom of Information Policy and a nominated officer to deal with requests and queries.

5 Regulation of Investigatory Powers Act 2000

5.1. This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

6 Crime and Disorder Act 1998

6.1. This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

6.2. The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/ exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There must be a Crime and Disorder Protocol governing the disclosure/ exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

7 The Computer Misuse Act 1990

7.1. This Act makes it a criminal offence to access any part of a computer system, programs and/ or data that a user is not entitled to access. Each organisation will issue users an individual user id and password which will only be known by the individual they relate to and must not be divulged/ misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

7.2. Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

Appendix 3: Disclosure of Personal Patient Information

1 Acts of Parliament that govern the disclosure/ sharing of personal patient information are detailed below:

1.1. Legislation to restrict disclosure of personal identifiable information

1.1.1. Human Fertilisation and Embryology (Disclosure of Information) Act 1992

1.1.2. Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992

1.1.3. Abortion Act 1967

1.1.4. The Adoption Act 1976

1.2. Legislation requiring disclosure of personal identifiable information

1.2.1. Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985

1.2.2. Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)

1.2.3. Births and Deaths Act 1984

1.2.4. Police and Criminal Evidence Act 1984

1.2.5. Sometimes a request may be received for patient information as part of a research project. Any such request would need to be assessed against requirements in the Data Protection Act 1998. In most circumstances it will be necessary to have any research proposal approved by the Local Research Ethics Committee (LREC). It is also necessary to obtain the patient's consent prior to using information for research purposes.

Appendix 4: Confidentiality Agreements for Contractors, Third Party Suppliers

1 Sample confidentiality agreements for third parties are set out below. Guidance is to be sought from the Senior Manager responsible for procurement and contracts before entering into an agreement.

1.1. Third party suppliers potentially affected could include the following:

1.1.1. Hardware and software maintenance and support staff (for all of the document);

1.1.2. Cleaning, catering, security guards and other outsourced support services (for general contractor clause and form on back page);

2 **General contractor clause** (based on clause from Introduction to Data Protection in the NHS (E5127) and BS7799).

2.1. The Contractor undertakes:

2.1.1. 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

2.1.2. 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

2.1.3. To ensure that they, their employees, agents and sub-contractors are aware of the provisions of the Data Protection Act 1998 and ISO/IEC 17799 and that any personal information obtained from the Trust shall not be disclosed or used in any unlawful manner; and

2.1.4. To indemnify the Trust against any loss arising under the Data Protection Act 1998 caused by any action, authorised or unauthorised, taken by them, their employees, servants, agents or sub-contractors; and

2.1.5. To comply, as required, with responsibilities under the Freedom of Information Act 2000. Specifically concerning the duty to disclose, where an exemption cannot be relied on when a request is received by the Trust. Also ensuring current and any new documentation between the supplier and the Trust complies with records management standards and the supplier is aware these documents could be made available to the general public, upon request.

2.1.6. All employees, 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 Trust sites where they may see or have access to confidential personal and/ or business information (see last page).

3 **Supplier Code of Practice** (based on example from Introduction to Data Protection in the NHS (E127) and ISO/IEC 17799).

3.1. The following Code of Practice applies where access is obtained to the Trust's personal data/ information, as defined within the Data Protection Act 1998, for the purpose of preventative maintenance, fault diagnosis, hardware or software testing, repair, upgrade, replacement or any other related activity.

3.2. The access referred to above may include:

3.2.1. Access to data/ information on the NHS organisations' premises;

3.2.2. Access to data/ information from a remote site;

3.2.3. Examination, testing and repair of media (e.g. fixed disk assemblies);

3.2.4. Examination of software dumps;

3.2.5. Processing using Trust data/ information.

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

3.4. The Supplier must undertake not to transfer the personal data/ information out of the EEA unless such a transfer has been registered, approved by the Trust's Information Governance Working Group and complies with the Information Commissioner's guidance.

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

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

3.7. Any data/ information sent from one place to another by or for the contractor shall be carried out by secure methods. These places will be within the supplier's own organisation or an approved sub-contractor (eg encrypted disk, secure file transfer etc).

3.8. Data/ Information that can identify any patient/ employee of the Trust must only be transferred electronically if previously agreed by the Trust's Information Governance Working Group. 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 ISO/IEC 17799. This will also apply to any direct-dial access to a computer held database by the supplier or their agent.

3.9. The data/ information must not be copied for any other purpose than that agreed by the supplier and the Trust.

3.10. Where personal data/ information is recorded in any intelligible form, it shall either be returned to the Trust on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to the Trust.

3.11. Where the contractor sub-contracts any work for the purposes in paragraph 3.1 above, the contractor shall require the sub-contractor to observe the standards set out above.

3.12. The Trust 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.

3.13. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party. These audits could include viewing the supplier's security policies, procedures and/ or controls to ensure they are complete and up to date, and cover Information Governance requirements.

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

3.15. Any security breaches and/ or other incidents made by the supplier's employees, agents or sub-contractors will immediately be reported to the Trust's Senior Information Risk Owner and particularly the Caldicott Guardian if this breach relates to patient identifiable information. The report will include the cause and actions taken to resolve the issue and how this has been reported to the supplier and the Trust.

4 Third Party Agreement

4.1. This agreement outlines your personal responsibility concerning security and confidentiality of information (relating to patients, staff and the business of the Trust).

4.2. During the course of your time within the Trust's 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 Trust and your employer. This condition applies during your time within the Trust and after that ceases.

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

4.4. The Data Protection Act 1998 regulates the use of all personal information and includes electronic and paper records of identifiable individuals (patients and staff). The Trust is registered in accordance with this legislation. If you are found to have misused any information you have seen or heard whilst working within the Trust you and your employer may face legal action.

4.5. If you are unsure of your responsibilities; have any doubt about how this affects you; or what you can or cannot do, please discuss this with your Trust's contact who will advise you or arrange a meeting with other appropriate personnel to give you advice and assistance. If necessary the Trust will invite you to attend an Information Governance training session.

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

Name of Organisation:	
Contract details:	
Print Name:	
Signature:	
Date:	

5 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 South East Coast Ambulance Service NHS Foundation Trust ('the Trust').

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

Signed: _____

Name of Individual: _____

Position in organisation: _____

Date: _____