NHS
South Sefton
Clinical Commissioning Group

NHS South Sefton Clinical Commissioning Group

Confidentiality and Data Protection Policy
2014 - 2016

Title:		Document Number		
NHS South Sefton CCG Confidentiality and Data Protection Policy				
Next Revision Due: October 2016		**Author**	**Consultation and Communication**	**Approved by**
Department responsible for this document:	Cheshire and Merseyside Commissioning Support Unit (North West CSU)	Senior Governance Manager (Information Governance)	Corporate Governance Support Group	SSCCG Quality Committee
DESIGNATION	**NAME**	**SIGNATURE**		**DATE**
Chief Finance Officer	Martin McDowell			October 2014

Version Control:

Version History:		
Version Number	**Reviewing Committee / Officer**	**Date**
1.0	Corporate Governance Support Group	8th October 2014
	SSCCG Quality Committee	18th December 2014

Table of Contents

Section **Page**

1. INTRODUCTION

1.1. The Clinical Commissioning Group (CCG) has a legal obligation to comply with all appropriate legislation in respect of Data Protection and Information / Information Technology Security. It also has a duty to comply with guidance issued by the Department of Health, and the Health and Social Care Information centre (HSCIC).

1.2. All legislation relevant to an individual's right to confidentiality and the ways in which that can be achieved and maintained are paramount to the CCG.

1.3. Penalties could be imposed upon the CCG, and / or CCG employees for non-compliance with relevant legislation and NHS guidance.

1.4. This Confidentiality and Data Protection Policy (Policy) aims to detail how the CCG meets 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.

1.5. For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. Associated legislation and further guidance are detailed in Appendicies A to D.

1.6. The NHS documents listed below are the main publications referring to security and or confidentiality of person identifiable data (PID).

- Information Security Management: NHS Code of Practice
- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Information to share or not to share: The Information Governance Review

2. POLICY STATEMENT

2.1. This document defines the Confidentiality and Data Protection Policy for the CCG.

2.2. The Confidentiality and Data Protection Policy applies to all personal information obtained and processed by and on behalf of the CCG.

2.3. This document:

- Sets out the organisation's Policy for the protection of all information obtained and processed.
- Establishes the responsibilities for Data Protection.
- Provides reference to the Data Protection Act 1998.

3. BACKGROUND

3.1. The purpose of this Confidentiality and Data Protection Policy is to lay down the principles that must be observed by all who work within the CCG and have access to person-identifiable information or confidential information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security.

3.2. All employees working in the NHS are 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 the common law duty of confidence and the Data Protection Act 1998. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

3.3. It is important that the CCG protects and safeguards person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

3.4. This Policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

3.5. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per current NHS Encryption Guidance.

3.6. Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes CCG confidential business and corporate information.

3.7. The CCG needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Information could be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, iPads, mobile phones, digital cameras, close circuit television or even heard by word of mouth.

3.8. Information can relate to patients and staff (present, past and prospective, including Governing Body members, temporary staff, secondees, work placed students and contract staff), and other business contacts however stored.

3.9. The information includes name, address, email address, data of birth, private and confidential information, and sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the Data Protection Act 1998 (the Act).

3.10. The lawful and proper treatment of personal information by the CCG is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that the CCG treats personal information lawfully and correctly.

3.11. The CCG fully supports and complies with the eight principles of the Act which are summarised below:

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained/processed for specific lawful purposes.

3. Personal data held must be adequate, relevant and not excessive.

4. Personal data must be accurate and kept up to date.

5. Personal data shall not be kept for longer than necessary.

6. Personal data shall be processed in accordance with rights of data subjects.

7. Personal data must be kept secure.

8. Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

3.12. A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

3.13. The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this Policy can be found in Appendix B.

3.14. How to report a breach of this Policy and what should be reported can be found in Appendix C.

3.15. Definitions of confidential information can be found in Appendix D.

4. PRINCIPLES

4.1. The objective of this Policy is to ensure the protection of information in accordance with the Data Protection Act 1998, that is:

- To ensure notification;
  Annually notify the Information Commissioner about the CCG's use of personal information.
- To ensure professionalism;
  All information is obtained, held and processed in a professional manner in accordance with the eight principles of the Data Protection Act 1998.
- To preserve security;
  All information is obtained, held and disclosed in a secure manner.
- To ensure awareness;
  Proper training and awareness is in place which informs all employees of their roles and responsibilities.
- To manage Subject Access Requests;
  Prompt and helpful response to any data subject access request.

5. SCOPE OF THIS POLICY

5.1. This Policy applies to all personal information processed, stored on computer or relevant filing systems (manual records), or Close Circuit Television and any extracts taken either printed, copied, or verbal, together with the staff working in or on behalf of the CCG (present staff, Governing Body members, temporary staff, secondees, work placed students and contract staff) who use the information in connection with their work.

6. DATA AND INFORMATION

6.1. The CCG needs to obtain data and process information about different people for many purposes, for example, but not limited to:

- Pay and Pension
- Work Management
- Staff Training
- Internal Telephone Directory
- Administration of access to information systems
- Smart Card applications
- Email management
- Claims processing
- Staff records and administrative records
- Matters relating to the prevention, detection and investigation of fraud and corruption in the NHS

6.2. Such information may be kept in either computer and/or manual records. In processing such personal data the CCG will comply with the Data Protection principles within the Data Protection Act 1998.

7. DATA PROTECTION RESPONSIBILITIES

Overall Responsibilities

7.1. The CCG permit staff to use computers and relevant filing systems (manual records) only in connection with their work. The CCG have legal responsibility for the notification process and compliance of the Data Protection Act 1998.

7.2. The CCG, whilst retaining their legal responsibilities have delegated Data Protection compliance to the nominated CCG Information Governance Lead.

i. CCG Managers

CCG Managers are responsible for:

- Ensuring that the Policy is implemented within their area of responsibility.
- Ensuring that the Policy is built into local processes and that there is on-going compliance.
- Ensuring that any breaches of the Policy are reported, investigated and acted upon.

ii. All Staff

- All staff (including Governing Body members, temporary staff, secondees, work placed students and contract staff) are subject to Data Protection compliance and this Policy. They are accountable via personal liability.
- All staff are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they adhere to the Policy on a day to day basis.
- All staff have a responsibility to inform the Data Protection Officer of any new use of Personal Data as soon as possible after it has been identified.
- Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality: NHS Code of Practice 2003. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

- Any breach of confidentiality, inappropriate use of health or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported.
- All staff will, through appropriate training and responsible management:

    - Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.
    - Understand fully the purposes for which the CCG uses personal information.
    - Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the CCG to meet its service needs or legal requirements.
    - Ensure the information is correctly input into CCG systems.
    - Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.
    - Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian.

iii. Caldicott Guardian

The Caldicott Guardian will:

- Ensure that the CCG satisfies the highest practical standards for handling patient identifiable information.
- Facilitate and enable appropriate information sharing and make decisions on behalf of the CCG following advice on options for lawful and ethical processing of information, in particular in relation to disclosures.
- Represent and champion Information Governance requirements and issues at Board level.
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.
- Receive training as necessary to ensure they remain effective in their role as Caldicott Guardian.

iv. Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) will:

- Take overall ownership of the organisation's Information Risk Policy.
- Act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the organisation's statement of internal control in regard to information risk.
- Understand how the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed.
- Implement and lead the NHS Information Governance Risk Assessment and Management processes within the CCG.
- Advise the Board on the effectiveness of information risk management across the CCG.
- Receive training as necessary to ensure they remain effective in their role as SIRO.

v. Data Protection Officer's Responsibilities

The internal CCG Data Protection Officer (CCG Information Governance Lead) responsibilities include:

- Ensuring that an appropriate Data Protection Act 1998 Policy for the CCG is produced and kept up to date.
- Ensuring that the appropriate procedures and practices are formulated and adopted by the CCG.
- Representing the CCG on Data Protection matters.
- Providing the appropriate leadership and direction for the Governance Team operating within the CCG.
- Setting the standard of Data Protection Act training for staff across the CCG.
- Ensuring the Data Protection notification is reviewed, maintained and renewed annually for all uses of personal information.
- Ensuring compliance with individual's rights, including subject access.
- Acting as a central point of contact on Data Protection within the CCG.
- Implementing an effective framework for the management of Data Protection.
- Monitor compliance with the Data Protection Act 1998, any infringement (i.e. unlawful disclosure of information or unlawful access) are investigated and appropriately dealt with.
- Audit appropriate systems in accordance with risk analysis reviews.
- Assisting with Counter Fraud and Security Management issues.

vi. Information Governance Senior Manager (from the CSU)

The Information Governance Senior Manager will:

- Maintain the currency of this Policy.

- Provide advice on request to any member of staff on the issues covered within it.

8. STAFF CODE OF CONDUCT

8.1. To ensure staff members are effectively informed of what is required of them, the CCG has a Staff Code of Conduct (code) that identifies legal requirements and best practice.

8.2. The code applies to all the different staff groups, e.g. for staff working with particularly sensitive information or those who have little access to confidential information.

8.3. The code is set out as follows:

a. The legal framework and the circumstances under which confidential information can be disclosed

National guidance includes NHS Codes of Practice on Confidentiality, Records Management and Information Security Management; the Caldicott Principles; and the NHS Care Record Guarantee for England. Care professionals must also comply with the codes of practice of their respective professions. These national guidelines also provide a basis for local codes which can focus on particular work areas or staff groups. The Caldicott Principles and the relevant extracts from the Care Record Guarantee are set out below.

b. The NHS and Social Care Record Guarantees for England

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. The Guarantee was first published in 2005 and is reviewed annually by the National Information Governance Board. The Social Care Record Guarantee - published in 2009 - explains to service users how the information they provide to social care staff is used and what control they can have over this. It complements the NHS Care Record Guarantee for England.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

c. The Caldicott Principles

The Caldicott Principles were devised by the Caldicott Committee, which reported in 1997 following a review of patient-identifiable information. They

represent best practice for using and sharing identifiable personal information and should be applied whenever a disclosure of personal information is being considered. should be applied whenever a disclosure of personal information is being considered. They were updated in the 2013 Caldicott Report:

1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

d. The systems and processes for protecting personal information

These include all safe haven procedures, e.g. for answering telephone queries or receiving confidential faxes, any information sharing protocols agreed with external organisations, encryption requirements for mobile devices and secure transfers of personal information.

e. Who to approach within the CCG for assistance and advice on disclosure issues

There are a range of individuals who can assist with difficult issues – the Information Governance lead, Caldicott Guardian, Senior Information Risk Owner, and Data Protection lead can be approached.

f. Possible sanctions for breach of confidentiality or data loss

The CCG will ensure that all staff members are aware of the possible disciplinary sanctions for failure to comply with their responsibilities, e.g. deliberately looking at records without authority; discussion of personal details in inappropriate venues; transferring personal information electronically without encrypting it, etc. Sanctions can include disciplinary action, ending a contract, dismissal, or bringing criminal charges. Since April 2010, the Information Commissioner's Office (ICO) may order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998.

g. Staff Awareness

The CCG will ensure that staff are effectively informed about the code through awareness sessions, team meetings, briefing notes or a combination of these. The code must be accessible so it needs to be readily available – it will be published on the Internet. Understanding what is required should be supported through staff training, e.g. through the on-

line NHS Information Governance training modules, which all staff can access through the National Learning Management System (NLMS).

9. CORPORATE LEVEL PROCEDURES

9.1. Principles

All staff must ensure that the following principles are adhered to:

a) Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
b) Access to person-identifiable or confidential information must be on a need-to-know basis.
c) Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
d) Recipients of disclosed information must respect that it is given to them in confidence.
e) If the decision is taken to disclose information, that decision must be justified and documented.
f) Any concerns about disclosure must be discussed with either your Line Manager, the Caldicott Guardian or the SIRO.
g) The CCG is responsible for protecting all the information it holds and must always be able to justify any decision to share information.
h) Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.
i) Access to rooms and offices where terminals are present or person-identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.
j) All staff should clear their desks of confidential information at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.
k) Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes ,printouts and fax messages must not be left lying around but be filed and locked away when not in use.
l) Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

9.2 Disclosing Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- With consent.
- When effectively anonymised.
- When the information is required by law or under a court order.

Information can be disclosed in Child Protection proceedings, if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

If staff have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance staff.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail.

Transferring patient information by email to anyone outside the CCG network may only be undertaken by using encryption as per the current NHS Encryption Guidance or through an exchange within the NHS Mail system (i.e. from one NHS.net account to another NHS.net account or to a secure government domain e.g. gsi.gov.uk), since this ensures that mandatory government standards on encryption are met. Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, and they have given their consent.

9.3 Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst 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 paper documents.

Taking home/ removing paper documents that contain person-identifiable or confidential information from the CCG premises is discouraged.

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

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

Staff must minimise the amount of person-identifiable information that is taken away from the premises.

If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of the CCG building.
- Confidential information is kept out of sight whilst being transported.

If staff do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information 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.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person-identifiable or confidential information on a privately owned computer or device.

9.4 Carelessness

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

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

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

Passwords must be kept secure and must not be disclosed to unauthorised persons. 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. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

9.5 Abuse of Privilege

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 of the Data Protection Act.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the CCG.

If staff have concerns about this issue they should discuss it with their Line Manager or Information Governance staff.

9.6 Confidentiality Audits

Good practice requires that all organisations that handle person-identifiable or confidential information 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 Information Governance staff through a programme of audits and spot checks.

10. MONITORING

10.1. Compliance with this Policy will be monitored via the CCG SIRO, CCG Caldicott Guardian, the Information Governance Senior Manager (CSU), together with independent reviews by both Internal and External Audit on a periodic basis.

10.2. The Information Governance Senior Manager is responsible for the monitoring, revision and updating of this Policy on a 2 yearly basis or sooner if the need arises.

11. EQUALITY IMPACT ASSESSMENT

11.1. This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

11.2. As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

12. ASSOCIATED DOCUMENTS

The following documents will provide additional information:

- Information Governance Strategy
- Information Governance Policy
- Freedom of Information Policy
- Corporate Records Management and Retention Policy
- The suite of ICT security policies

Appendix A - Confidentiality Dos and Don'ts

Do

• Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of the CCG.

• Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

• Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.

• Do ensure that you cannot be overheard when discussing confidential matters.

• Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.

• Do share only the minimum information necessary.

• Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.

• Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.

• Do report any actual or suspected breaches of confidentiality.

• Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don’ts

• Don’t share passwords or leave them lying around for others to see.

• Don’t share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.

• Don’t use person-identifiable information unless absolutely necessary, anonymise the information where possible.

• Don’t collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B - Summary of Legal and NHS Mandated Frameworks

The CCG is 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. 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 Report (2014) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

1. Justify the purpose for using patient-identifiable information.
2. Don't use patient identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient-identifiable information.
4. Access to patient-identifiable information should be on a strict need to know basis.
5. Everyone should be aware of their responsibilities.
6. Understand and comply with the law.
7. 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

The NHS Confidentiality Code of Practice (2003) outlines for 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 – "intra vires". 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.

Appendix C - Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to line managers, and recorded on Datix. If staff are unsure as to whether a particular activity amounts to a breach of the Policy, they should discuss their concerns with their Line Manager or Information Governance staff. The following list gives examples of breaches of this Policy which should be reported:

- Sharing of passwords.
- Unauthorised access to CCG systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person-identifiable information in ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or Information Governance staff should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the CCG.

The information will enable the monitoring of compliance and improvements to be made to the Policy and procedures.

Appendix D - Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information as defined by the Data Protection Act 1998 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information such as contracts, trade secrets, procurement information, which should also be treated with the same degree of care.