NHS
West Essex
Clinical Commissioning Group

Data Protection and Confidentiality Policy

Policy Reference: IG02

Brief Summary: The CCG Data Protection and Confidentiality Policy aims to detail 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 1990 which is the key piece of legislation covering security and confidentiality of personal information.

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	01/02/2013	Draft	New Document	NHS Central Eastern Commissioning Support Unit, Information Governance Team
1.0	14/02/2013	Final	Approved by West Essex CCG Board	NHS Central Eastern Commissioning Support Unit, Information Governance Team
1.1	17/10/2014	Draft	Changes in guidance and reporting structure necessitates policy review	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.2	08/01/2015	Draft	Key Contacts Added	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.3	05/03/2015	Final	Approved by West Essex CCG Board	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West Essex CCG's Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7th October 2016
Next Review Date	March 2019

Responsibility for Review	CCG's Information Governance Team
Audience	All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

The Data Protection Act 1998 (DPA) first came into force on March 1st 2000. The DPA covers all personal data held both manually (on paper) and electronically (on a computer).

The DPA is closely linked to the Freedom of Information and Human Rights Acts. Its intention is to focus on promoting the rights of individuals in respect of their privacy and the right to confidentiality of their data. The responsibility to maintain the confidentiality of data resides with the Data Controller, even if an agent or subcontractor performs the processing.

NHS West Essex Clinical Commissioning Group (the CCG) has a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty under the establishment order to comply with guidance issued by The Department of Health, the NHS Executive and other advisory groups to the NHS and guidance issued by professional bodies. The CCG believes that an individual's right to confidentiality is of vital importance.

All legislation relevant to an individual's right of confidentiality and the ways in which that can be achieved and maintained are paramount to the CCG. This relates to roles that are reliant upon computer systems such as patient administration / payment, purchasing, invoicing and the planning of treatment. Recent legislation also regulates the use of manual records relating to patients, staff and others whose information may be held within the CCG.

This document is a statement of the policy and principles adopted by the CCG governing the processing of personal data as specified in the DPA (1998).

Conformance with the DPA is part of the CCG's overall duty of confidentiality towards its patients, staff and all other individuals with whom it may effectively work in collaboration.

Non-compliance with the relevant legislation could result in individuals, employees and the CCG being investigated and subsequently prosecuted for offences under the DPA such as:

- Processing personal data without notifying the Information Commissioner.
- Processing personal data for any purpose other than that covered by the CCG's notification.
- Unauthorised disclosure of personal data for example disclosure to a person / organisation not entitled to receive it.
- Failure to comply with the information / enforcement notice issued by the Information Commissioner.
- Modifying personal data that has been subject to a Data Protection Act subject access request.

A full copy of the Data Protection Act 1998 is held by the Information Governance Team and any queries or questions from staff, patients or public in relation to this policy, the DPA or any other confidentiality issues should be addressed to them.

2. Purpose

The purpose of the policy is to deliver fully the Principles of Data Protection, as stated in the DPA 1998. The Principles require that:

First Principle: Personal information shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

There is a requirement to make the general public, who may 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 CCG is obliged under the DPA and Caldicott Principles to produce a patient information leaflet.

A clear policy of consent is needed to ensure the first principle is addressed.

Second Principle: Personal information shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that (or those) functions.

The CCG is required to complete a notification with the Information Commissioner on all databases which hold and / or process personal information about living individuals. It is a criminal offence if this notification is not kept up to date.

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

Information collected from individuals should be complete and should all be justified as being required for the purpose they are being requested.

Fourth Principle: Personal information shall be accurate and, where necessary, kept up to date.

Users of software will be responsible for the quality of the data by carrying out quality assurance checks and participating in activities, as instructed by the Information Governance Steering Group. Staff information should also be regularly checked by line managers or by Human Resources Department.

Fifth Principle: Personal information shall not be kept for longer than necessary for that purpose or those purposes

All records are affected by this principle regardless of the media they be held within, stored or retained. Records Management: NHS Code of Practice parts 1 and 2 provides comprehensive guidance.

If the information on the computer or manual records is not the main record this is considered to be transient data. Procedures must be put in place to give appropriate guidance to users.

Sixth Principle: Personal information shall be processed in accordance with the rights of data subjects under the Act. Under this principle of the DPA individuals have the following rights

- Right of subject access
- Right to prevent processing likely to cause harm or distress
- Right to prevent processing for the purposes of direct marketing
- Right in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Information Commissioner for an assessment against an organisation to establish whether any part of the Act has been contravened

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

The CCG has a legal obligation to maintain confidentiality standards for all patient identifiable information. This includes the disposal of non-clinical waste.

The CCG must ensure that all information held on any format of media is accurate and up to date. The accuracy of the information can be achieved by implementing validation routines.

Eighth Principle: Personal information shall not be transferred to a country or territory outside the European Economic Area 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.

Patient identifiable information should not be sent to any countries outside of the EEA as these countries do not have the necessary legislation in place to adequately protect the data covered by the DPA 1998.

3. Scope

The policy covers all aspects of business relating to personal information within the CCG and is not solely patient related. It may include information held by all areas such as healthcare covering:

- Acute, Community and Intermediate Care
- Mental Health
- Learning Disabilities

- Primary Care
- Child Protection
- Human Resources – including Criminal Records Bureau checks on staff
- Payroll and Finance
- Procurement
- Estates
- Occupational Health

The policy covers all methods of holding information and all media used to store this including:

- Manually stored paper data for example card index files, medical records and so on
- Computer referenced paper data, for example, health records, personnel records, and so on.
- Computerised data held in computer applications and databases
- Tapes and other data from CCTV systems
- Data held offsite in archive storage
- Data held on CD ROMs, floppy disks, computer disks, memory sticks, printer ribbons or any other type of removable media and so on

For the purposes of this policy confidential information shall include any restricted data relating to the CCG, its agents, customers, prospective customers, suppliers or any other third parties connected with the CCG and in particular shall include, without limitation:

- service user information
- ideas / programme plans / forecasts / risks / issues
- trade secrets
- Business methods and business design
- Finance / budget planning / business cases
- Prices and pricing structures
- Sources of supply and costs of equipment and / or software
- Prospective business opportunities in general
- Computer programmes and / or software adapted or used
- Policy advice and strategy.

4. Definitions & Terms

BMA British Medical Association

CCG Clinical Commissioning Group

HSCIC Health & Social Care Information Centre (now NHS Digital)

CSU Commissioning Support Unit

CRB Criminal Records Bureau

CCTV Closed Circuit Television

CQRS Calculating Quality Reporting System

DPA Data Protection Act

EEA European Economic Area

IM&T Information Management and Technology

ICO Information Commissioners Office

IGT Information Governance Toolkit

IGTT Information Governance Training Tool

NHS Digital (formerly HSCIC)

PIA Privacy Impact Assessment

SIRO Senior Information Risk Owner

QOF Quality of Outcomes Framework

QMAS Quality Management and Analysis System

Data Controller is the person who in nominated by the CCG who determines the purposes for and the manner in which any personal data are, or are to be, processed.

Data Subject is the individual who is the subject of personal data.

Personal Data means data which relate to a living individual who can be identified –

(a) from that data, or

(b) from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

This 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. See Appendix 1.

Relevant filing system means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Processing, in relation to information or data, means obtaining, recording or holding the information or carrying out any operation or set of operations on the information, including:

- acquiring the data
- organising and managing the information or data
- retrieving and using the information or data
- disclosing or sharing the information or data by fax, letter, e-mail, or any other means of transmission or dissemination
- archiving, disposing of or destroying the information or data.

This term comprises not only individuals but also organisations such as companies and other corporate and unincorporated bodies of persons.

Data Processor – The Data Processor refers to any person or organisation (other than an employee of the data controller) who processes (including storing or otherwise managing) the data on behalf of the data controller.

Recipient The Recipient refers to any person or organisation to whom the data is disclosed, but does not include any person to whom disclosure is made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Countries in the European Economic Area (EEA) The European Economic Area (EEA) refers to the following European countries or territories: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark (excluding the Faroe Islands), Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom (excluding the Isle of Man and the Channel Islands).

5. Roles & Responsibilities

5.1 Accountable Officers for NHS West Essex CCG

The Chief Officer (CO), as the Accountable Officer, has overall responsibility for information governance within the CCG. The CO is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

The CO has delegated operational responsibility for information governance to the Director of Finance, Contracting and Performance

5.2 Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. The SIRO has overall responsibility for the implementation and delivery of the DPA 1998, on behalf of the CCG with devolved responsibility to the Information Governance Lead. The SIRO is responsible for facilitating the implementation of the policy and supporting CCG staff to understand their responsibilities. This includes oversight of information security incident reporting and response arrangements.

5.3 Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service users information and enabling appropriate information sharing. For the CCG, this is an executive, the Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

5.4 All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.

The CCG policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.
All staff associated with the CCG have a responsibility to ensure compliance with the DPA 1998 and to actively respond to any concerns relating to confidentiality

5.5 Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate these.

5.6 Information Asset Administrators (IAAs)

Information Asset Owners can appoint Information Asset Administrators (IAAs) to support in the delivery of their information risk management responsibilities. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their Information Asset Owner on incident management and ensure that information asset registers are accurate and up to date.

5.7 CCG Clinical Leads and Operational Managers of Departments

The clinical leads and operational managers of departments have a responsibility to understand the Act and other related guidance, to ensure that appropriate procedures are in place to control and manage information accordingly, and to ensure that these procedures are followed.

6. Specific DPA Compliance Requirements

The CCG will fully conform to the rules for notification. These include:

- That a notification is lodged in its name with the Information Commissioner
- That the notification is lodged within the stipulated time period
- That the notification is full, correct and up-to-date
- That any changes are notified within the stipulated time period
- The CCG will fully discharge its responsibilities implied by the Principles contained with the DPA by putting in place procedures and by monitoring these through annual audit
- To fully observe conditions regarding the fair collection and use of information
- To meet its legal obligations to specify the purposes for which information is used
- To collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement
- To ensure the quality of information used
- To apply strict checks to determine the length of time information is held
- To ensure that the rights of people about whom information is held can be fully exercised under the Act, this includes monitoring the management of “rights of access”
- To take appropriate technical and organisational security measures to safeguard personal information
- To ensure that the necessary measures are taken to safeguard all sensitive personal data
- To ensure that the necessary measures are always taken to ensure the proper disclosure of information between agencies

- To ensure that personal information is not transferred abroad without adequate and suitable safeguards being implemented prior to the transfer.

7. Individual Rights

Individuals have rights under the DPA 1998 in respect of their own personal data held by others. The CCG will ensure that all individuals are aware of their rights under the Act and will fully comply with the delivery of these rights to individuals.

The rights of the individual are:

- To be informed about the use made of personal data
- To be informed about the purpose of processing, the source and the recipients of the data
- To be informed of any logic used in automated decisions
- To be provided with a copy of this record, where the effort to provide such is reasonable
- To have incorrect data corrected, blocked, erased or destroyed
- To have previous recipients of such data informed
- To object where substantial damage or distress may be caused
- To object to direct marketing where personal data is used
- To apply for compensation if an individual suffers damage
- To make a request to the Commissioner for an assessment to be made regarding whether any provision of the Act has been contravened.

The CCG will ensure that every individual is aware of his / her rights and of how to exercise these.

8. Subject Access Requests

All data subjects, or someone acting on their behalf, can request to view their personal data held by the CCG.

All applications regarding patient personal data must be made in writing to the IG Team as outlined in the Subject Access Requests and Access to Health Records Requests Policy and Procedure.

If a member of staff requires a copy of their personal data, a request can be made via their line manager.

9. Disclosure to Others

The CCG may receive requests to obtain personal data from sources other than the individual.

Important: Please refer to the CCG Safe Haven Procedures for guidance on how to handle person identifiable information.

Statutory Requests – All statutory requests from courts or coroner's offices and so on will be complied with by the CCG via the IG Team if appropriate. The patient concerned may be informed that the data has been disclosed unless this would prejudice criminal investigations.

Medico-Legal – All requests from solicitors and healthcare providers will only be complied with if the CCG is in receipt of the written consent of the patient or their representative, again all of these requests will be managed by the IG Team.

GPES (General Practice Extraction System) –GPES is a service that securely collects information, with consent, from GP systems, and delivers it to approved organisations with the aim of directly improving patient care.

Information collected for the NHS Diabetic Retinopathy Screening Programme, for example, will help improve screening and prevent people from developing this condition and losing their sight. Information collected for the Learning Disabilities Observatory will help drive practical improvements in the way services are delivered for patients with learning disabilities. GPES is not a data warehouse. Information is deleted once it has been transferred.

Key Functions of GPES:-

- Replaces QMAS (Quality Management and Analysis System)
- To Support QOF
- To extract anonymised and person identifiable data for use in other programmes that aim to improve patient care and to reduce health inequalities

GPES does have strict IG processes in place. These processes have been developed following many discussions that took place between the BMA and Royal College of General Practitioners. It is fully compliant with law and ensures that the practice is still in control of its data. Patients do have the option to opt out. Read codes have been developed so that a patient can dissent or withdraw their dissent from extraction of their data from taking place.

All clinical commissioning groups are bound by legal duties to promote research and the use of evidence to support commissioning, they may also wish to seek advice and support in order to be able to efficiently carry out these roles.

In planning how functions are transferring between organisations as part of the transition local health communities, may wish to review any locally based primary care trust research services. They are encouraged to consider retaining and finding a suitable host for skilled teams that can offer supportive services to primary care providers and to NHS commissioners with their future duties and activities.

Such teams may be independent or they may be hosted, for example:

- within a provider (acute, mental health, community)
- by a commissioner (clinical commissioning group, NHS England local area team or a commissioning support service)
- by the Clinical Research Network of the National Institute for Health Research or an Academic Health Science Network

CQRS (Calculating Quality Reporting System) – Has been developed to support organisation restructures and commissioning arrangements. Effectively it will replace QMAS, the current system in place to calculate payments to the GPs, under the Quality of Outcomes Framework (QOF). It will also calculate achievements made by CCGs against outcome indicators and quality rewards. The data used for CQRS will come from the Health and Social Care Information Centre, including *GPES*.

Police – All requests from the Police for personal data will be viewed on a 'case-by-case' basis via the IG Team and Caldicott Guardian (if necessary), who will decide if the information can be disclosed. All requests must be in writing using the documentation provided by the Police Authority.

The most likely legal bases for disclosure (without the patient's consent) to the Police are:

- Prevention of Terrorism Act 1989 and Terrorism Act 2000 – it is a statutory duty to inform the Police about information gained (including personal information) about terrorist activity.
- The Road Traffic Act 1988 – It is a statutory duty to inform the Police, when asked, the name and address (not clinical information) of drivers who are allegedly guilty of an offence.
- Court order – where the courts have made an order the information must be disclosed unless the CCG decides to challenge the order of the court.

10. Exemptions

There are specific reasons why access to personal data may be denied including:

- Where the data released may cause serious harm to the physical or mental condition of the patient, or any other person.
- Where access would disclose information relating to or provided by a third party (where consent had not been received by the third party to release their data). N.B. this does not include information recorded by CCG employees as part of their normal duties.
- Where it is assessed that a patient under the age of 16 cannot understand the implications of accessing their records.

11. Cost and Timescales

An application for data access can cost up to a maximum of £50 and a period of 40 days is allowed for the CCG to provide the data.

12. Human Resources

All contracts of employment include a data protection and general confidentiality clause, agency and contract staff are subject to the same rules.

Any member of staff current, past or potential (applicants) who may wish to have a copy of their information under the subject access provision of the DPA have the right to access data held about them.

A breach of the Data Protection requirements could result in disciplinary action being taken (including dismissal). A breach of the DPA could also result in legal action being taken against those found in contravention. A copy of the CCG disciplinary procedures is made available to all staff via the approved Human Resource policies on the intranet.

The CCG is required to undertake criminal records checks on certain groups of staff. The CRB 'check' is fully complaint with the DPA 1998 and the Freedom of Information Act 2000.

13. Privacy Impact Assessments

The clinical commissioning group recognises that the protection of an individual's confidentiality and not infringing on their privacy is an essential consideration for the CCG. With the development of new technologies and increased public concerns about intrusion into individuals' privacy, the Information Commissioner's Office in conjunction with NHS Digital (formerly Health and Social Care Information Centre -HSCIC), via the Information Governance Toolkit, has identified Privacy Impact Assessment (PIA) as a key tool in addressing confidentiality and privacy concerns.

Privacy Impact Assessment (PIA) is a process which enables organisations to anticipate and address the likely impacts of new initiatives on an individual's privacy. It is important to note that the individuals referred to are patients / service users and staff.

Please refer to the Privacy Impact Policy for more information with regard to how and when to complete a Privacy Impact Assessment.

14. Audit and Monitoring Compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents
Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has responsibility to provide assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect it. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programmes and progress reports
- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external assessments or other sources of information and advice.

15. Dissemination and Implementation

The policy will be published on the intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example e.g. through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

16. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

The SIRO has overall responsibility for ensuring that all staff are aware of the requirements of the DPA. This will be carried out by the regular mandatory training sessions covering the following elements:

- Patients are aware of the policy and of their rights
- Staff are aware of the policy and of their rights and obligations
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows whom to approach
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are clearly described
- A regular review and audit is made of the way personal information is managed
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated
- Ongoing awareness raising sessions for staff.

As well as mandatory training for existing staff, all new starters to the CCG will be provided with data protection and general IT security training as part of the induction process.

All training provided with regard to data protection will be recorded on the CCG training database.

Agency and contract staff are subject to the same rules.

In addition, staff members are bound by their professional codes of conduct where applicable.

17. Related documents & Acts

Acts & Legislation:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Police Act 1997
- Health & Social Care Act 2012
- Legislation to restrict disclosure of personal identifiable Information
- Human Fertilisation and Embryology (disclosure of information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1984
- The Adoption Act 1976

- Legislation requiring disclosure of personal identifiable information
- Public Health (Control of Diseases) Act 1984 and Public Health (Infectious Diseases) Regulations 1985
- Education Act 1944 (for immunisations and vaccinations to the NHS Trusts from Schools)

- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984

Policies:
- Information Governance Policy
- Information Sharing Policy
- Safe Haven Policy
- Information & Cyber Security Policy
- Information Lifecycle Management Policy & Strategy
- Information Risk Policy
- Access to Information Policy
- Privacy Impact Assessment Policy

18. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010.

This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.

19. Key Contacts

Within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net

Appendix 1

What constitutes Person Identifiable Information?

Any of the following information collected in the course of a service user's care will / could constitute person identifiable information:

- Name
- Address
- Post code
- Date of birth
- NHS Number
- National Insurance Number
- Carer's details
- Next of kin details
- Contact details
- Bank details
- Lifestyle
- Family details
- Voice and visual records (for example photographs, tape recordings)

This list is not exhaustive.