NHS
Dorset
Clinical Commissioning Group

NHS Dorset Clinical Commissioning Group

Data Protection Policy



Supporting people in Dorset to lead healthier lives

PREFACE

This document sets the policy for NHS Dorset Clinical Commissioning Group with regard to its legal obligation to comply with the Data Protection Act 1998.

All managers and staff (at all levels) are responsible for ensuring that they are viewing and working to the current version of this procedural document. If this document is printed in hard copy or saved to another location, it must be checked that the version number in use matches with that of the live version on the CCG intranet.

All CCG procedural documents are published on the staff intranet and communication is circulated to all staff when new procedural documents or changes to existing procedural documents are released. Managers are encouraged to use team briefings to aid staff awareness of new and updated procedural documents.

All staff is responsible for implementing procedural documents as part of their normal responsibilities, and are responsible for ensuring they maintain an up to date awareness of procedural documents.

A	SUMMARY POINTS
Policy for NHS Dorset Clinical Commissioning Group with regard to its legal obligation to comply with the Data Protection Act 1998.	

B	ASSOCIATED DOCUMENTS

- Information Governance Policy
- IT Security Policy
- Confidentiality: Staff Code of Conduct
- Confidential Corporate Information Policy
- Procedure for the Management of Adverse Incidents
- Procedure for the Management of Serious Incidents
- Remote Access and Homeworking Policy
- Network Security Policy
- Freedom of Information Policy

C	DOCUMENT DETAILS
Procedural Document Number	14
Author	Joyce Green
Job Title	Head of Information Governance/Customer Care
Directorate	Quality
Recommending committee or group	Information Governance Group
Approving committee or group	Information Governance Group
Date of recommendation (version 1)	12 March 2016
Date of approval (version 1)	October 2013
Version	1.2
Sponsor	Director of Nursing and Quality
Recommendation date	15 March 2016
Approval date	15 March 2016

Review frequency	Bi-annually
Review date	March 2018

D	**CONSULTATION PROCESS**		
Version No	**Review Date**	**Author and Job Title**	**Level of Consultation**
1.2	March 2016	Joyce Green, Head of Information Governance/ Customer Care	Information Governance Group

E	**VERSION CONTROL**				
Date of issue	**Version No**	**Date of next review**	**Nature of change**	**Approval date**	**Approval committee/ group**
March 2016	1.2	March 2018	This policy replaces the CCG Data Protection and Confidentiality Policy	15 March 2016	Information Governance Group

F	**SUPPORTING DOCUMENTS/EVIDENCE BASED REFERENCES**	
Evidence	**Hyperlink (if available)**	**Date**
Information Governance Review 2013		2013
NHS Code of Practice: Records Management	www.opsi.gov.uk	2006 updated 2009
NHS Code of Practice – Information Security Management	www.opsi.gov.uk	2009
NHS Code of Practice: Confidentiality	www.opsi.gov.uk	2003
HSG(96)18 – The Protection and Use of Patient Information		1996
HSC 1999/012 – Caldicott Guardians		
The Caldicott Principles		1997
The Caldicott 2 Review	www.gov.uk	2013
Data Protection Act	www.opsi.gov.uk	1998

Human Rights Act	www.opsi.gov.uk	1998
Freedom of Information Act	www.opsi.gov.uk	2000
Department of Health Guidance for Access to Health Records Requests		2010
Common Law Duty of Confidentiality	www.opsi.gov.uk	
Electronics Communications Act	www.opsi.gov.uk	2000
Computer Misuse Act	www.opsi.gov.uk	1990
Civil Contingencies Act	www.opsi.gov.uk	2004
Health and Social Care Act	www.opsi.gov.uk	2001 updated 2015
Protocol for Information Sharing between Health and Social Care Agencies		2006
Public Records Act	www.opsi.gov.uk	1958
NHS Constitution	www.gov.uk	2015
HSCIC Guide to Confidentiality in Health and Social Care: Treating Confidential Information with Respect	www.hscic.gov.uk	2013
HSCIC Code of Practice on Confidential Information	www.hscic.gov.uk	2014

G	**DISTIBUTION LIST**		
Internal CCG Intranet	**CCG Internet Website**	**Communications Bulletin**	**External stakeholders**
√	√	√	Tick as appropriate

1. RELEVANT TO

1.1 This policy is relevant to all staff:

- within NHS Dorset Clinical Commissioning Group (hereafter known as the CCG) whether operating directly or providing services under a service level agreement or joint agreement;

- including contracted employees, non-executive directors and contracted third parties such as bank, agency, volunteers, locums, student placements, staff on secondment, researchers, visiting professionals and suppliers.

1.2 Failure to adhere to this policy, and its associated procedures, may result in disciplinary action.

2. INTRODUCTION

2.1 This policy relates to the processing of personal information and to the management of personal information about members of the public/patients/service users and staff.

2.2 The CCG is required by law to comply with the Data Protection Act 1998 (DPA), which is concerned with the lawful processing of information relating to living individuals. To comply with the law staff, and/or others, who process personal information must ensure they follow the Data Protection Principles and the Caldicott Principles.

2.3 Like all NHS Organisations, the CCG holds and processes information about its employees, members of the public, patients and other individuals for various purposes (e.g. the effective provision of healthcare services, Continuing Healthcare or; for administrative purposes). To comply with the DPA personal identifiable information must be collected and used fairly, stored safely and not disclosed to unauthorised persons. The DPA applies to both manual and electronic data.

2.4 For the purposes of the DPA, the CCG acts as the data controller for personal and sensitive data. A data controller is an organisation who determines the purposes for which, and the manner in which, personal data is to be processed. Such processing may be carried out jointly or in common with other organisations.

2.5 The eight principles of the Data Protection Act 1998 determine how the CCG should collect, process, and retain personal data.

2.6 The CCG has a legal obligation to comply with all appropriate legislation in respect of data, information and information security. It also has a duty to comply with guidance issued by the Department of Health (DoH), the Information Commissioner (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

2.7 Compliance with the policy will provide assurance to the CCG, and to individuals, that all personal and sensitive information processed by the CCG is dealt with legally, securely, effectively and efficiently, in order to deliver the best possible care to patients.

2.8 The CCG will establish and maintain policies and procedures to ensure compliance with the requirements contained in the Health and Social Care Information Centre's Information Governance Toolkit.

3. SCOPE

3.1 To ensure that the CCG meets its legal requirements under the DPA this Policy applies to all staff within the CCG and Governing Body and Lay Members. It also applies to other personnel working for, and on behalf of, the CCG including agency staff, volunteers, students and contractors, third party partner organisations and suppliers This policy covers all:

- records held and processed by the CCG in any medium;
- information within the organisation, including (but not limited to)
    - General Public/Patient/staff/service user information
    - Personal information
    - Organisational information;
- aspects of handling information, including (but not limited to):
    - Structured and unstructured record systems – paper and electronic;
    - Transmission of information – fax, email, post and telephone;
    - Information systems managed and/or developed by, or used by the CCG;
    - Information sharing;
    - tapes and other data from CCTV Systems;
    - data held in offsite archive storage;
    - data held on CDs; memory sticks, laptops, IPads and any other type of mobile media.

4. PURPOSE

4.1 The purpose of this policy is to ensure that the CCG is compliant with the requirements of the DPA.

4.2 The CCG recognises its responsibilities to implement, in full, its duties in respect of the DPA and to ensure all its employees understand and implement the requirements.

4.3 This policy will underpin any operational procedures and activities connected with the implementation of the DPA, in particular those listed in the CCGs Information Governance Policy and IT Security Policy.

5. DEFINITIONS

5.1 See Glossary at Appendix A.

6. ROLES AND RESPONSIBILITIES

CCG Governing Body

6.1 The CCG Governing Body supports the eight Data Protection principles and the requirements of the Common Law Duty of Confidentiality and endorses this Data Protection Policy.

6.2 The CCG Governing Body, whilst retaining their legal responsibilities, has delegated Data Protection compliance to the nominated Data Protection Officer, Caldicott Guardian, Senior Information Risk Owner (SIRO), and the Information Governance Group (IGG).

Chief Officer

6.3 The Chief Officer has overall responsibility for the Data Protection Policy within the CCG.

6.4 The Chief Officer is the named officer with responsibility for ensuring that the CCG complies with its statutory obligations and Department of Health directives for Data Protection.

6.5 The Chief Officer will ensure that the CCG has access to specialist advice regarding the requirements of the DPA 1998. This will be provided by the CCG's Data Protection Lead in the first instance and then by the office of the Information Commissioner.

6.6 Responsibility for implementation of the DPA has been delegated to the Data Protection Officer.

Caldicott Guardian

6.7 The CCG has appointed a Caldicott Guardian, who oversees disclosures of patient information with particular attention being paid to those disclosures which are not routine.

6.8 The Caldicott Guardian ensures that the CCG and partner organisations protect the confidentiality of patient level information, and is responsible for advising the CCG and the Governing Body on confidentiality issues. This also includes establishing and maintaining procedures governing access to and the use of person confidential data held or processed within the CCG systems and the transfer of such data from the CCG to and from other bodies.

Senior Information Risk Owner

6.9 The Senior Information Risk Owner (SIRO) takes ownership of information risk and is responsible for:

- overseeing the development of an Information Security Policy;
- ensuring the Governing Body is adequately briefed on information risk;
- providing a focal point for the resolution and discussion of information risk issues.

Head of Information Governance/Customer Care (Data Protection Officer)

6.10 The Head of IG/Customer Care (Data Protection Officer) will provide specialist advice on data protection to the CCG, along with the Information Governance Team, overseen by the Information Governance Group and the Caldicott Guardian.

6.11 The Head of IG/Customer Care will also be responsible for:

- developing and maintaining policies, procedures and guidance as required by the DPA;
- maintaining and holding a record of the CCG's notifications of personal data held and the purposes under the DPA with the office of the Information Commissioner;
- periodically producing and distributing staff guides on Data Protection and Confidentiality;
- ensuring that all staff are aware of their personal responsibilities for compliance and adhere to organisational policies and procedures. This includes ensuring that training and written procedures are widely disseminated and available to all staff.
- dealing with subject access requests for the CCG;
- acting as an initial point of contact for any data protection and confidentiality issues which may arise and assisting with investigations into complaints about breaches of the Act;
- facilitating action in areas identified as non-compliant;

- the Head of IG and Customer Care has overall responsibility for co-ordinating the IG work programme and completion of the IGT annual assessment

Information Governance Group

6.12 The CCG has established an Information Governance Group (IGG) comprising of representatives from directorates within the CCG in order to promote a consistent approach to Data Protection/IG. The group is responsible for developing and sharing best practice across the organisation and ensuring that IG standards are included in other work programmes and projects.

6.13 The key authority and purpose of the Information Governance Group is to:

- ensure the CCG's approach to information handling, keeping personal information secure and respecting the confidentiality of service users, is communicated to all staff and made available to the public;
- offer support, advice and guidance to the Caldicott and Senior Information Risk Officer (SIRO) Function and Data Protection programme within the CCG;
- co-ordinates the review of the CCG's IG management and accountability arrangements and produces and monitors the annual IG work programme. The CCG recognises that other key staff will be involved in, and contribute to, this work programme;
- ensuring that the CCG has effective policies and management arrangements covering all aspects of data protection, confidentiality and information governance;
- reviewing, approving and monitoring Privacy Impact Assessments to ensure privacy considerations are taken into account when new projects are introduced or changes are made to existing services;
- advising the Governing Body on issues relating to data protection, confidentiality and Information Governance.

6.14 The IGG reports to the Audit and Quality Committee, and responsibility for the approval of related policies and procedures is delegated to the Directors Performance Group on behalf of the CCG Governing Body.

Managers

6.15 The day to day responsibility for enforcing this policy will be delegated to Line Managers. Managers will ensure that all staff:

- are made aware of the data protection policy;
- attend appropriate training;

- know how to deal with requests for person identifiable information;
- register all databases.

6.16 Managers will ensure that all systems and manual files that process personal data are recorded on the Information Asset Register and are managed by a nominated Information Asset Owner.

Information Asset Owners

6.17 The Information Asset Owner (IAO) must ensure that any system (and users) they are responsible for complies with the current Data Protection legislation.

6.18 The IAO is responsible for ensuring that:

- the system is recorded on the Information Asset Register;
- users are set up on the system on a need to know basis in line with access control procedures;
- expert advice is available regarding data protection issues;
- unusual requests for disclosure are scrutinised;
- there is a System Security Procedure which outlines the media, frequency and retention period for back-ups of the data and programs for the systems within their control.

Director of Engagement and Development

6.19 The Director of Engagement and Development is responsible for overseeing all staff requests for access to personal files, with support from the Information Governance Team.

6.20 The Director of Engagement and Development will ensure that appropriate clauses are in staff contracts to ensure that all staff are bound by the requirements of the DPA.

Staff

6.21 All staff are expected to adhere to this policy and associated documentation. Any breaches of this policy will be investigated in line with the CCG disciplinary procedures.

6.22 All staff are required to attend IG training on an annual basis.

6.23 All CCG employees are responsible for ensuring that all the personal data used and held by the CCG is secured from loss, corruption, damage and disclosure.

6.24 All staff who create, receive and use records have records management responsibilities. Staff:

- are responsible at law for any records they create and use;
- must be aware that any records they create are not their personal property, but belong to the CCG.

6.25 Staff are responsible for attending training as appropriate.

Information Commissioner's Office

6.26 The Information Commissioner's office (ICO) is the UK's independent public authority set up to uphold information rights. They rule on complaints, provide information to individuals and organisations and taking appropriate action when the law is broken.

6.27 The ICO enforces and oversees the following legislation:

- Data Protection Act 1998;
- Freedom of Information Act 2000;
- Privacy and Electronic Communications Regulations 2003;
- Environmental Information Regulations 2004;
- INSPIRE Regulations 2009.

6.28 The ICO maintains a public register of data controllers who process personal information.

6.29 Non-compliance with the DPA, and any breach of confidentiality, could result in the CCG being investigated by the ICO and ultimately fined up to £500,000 and/or prosecuted.

7. SUPPORTING POLICIES AND PROCEDURES

7.1 A summary of CCG key policies and procedures that support the Data Protection (IG) work programme are listed at Appendix B of this document.

7.2 This is a live document and as new legislation, guidance and policies are approved, amendments will be added to this document.

8. THE DATA PROTECTION ACT

8.1 The Data Protection Act 1998 came into force on 1 March 2000 and applies to all person identifiable information about living individuals held in manual files, computer databases, videos and other automated media. This includes personnel and payroll records, medical records, other manual files, microfiche/film etc.

8.2 The DPA dictates that information should only be disclosed on a need to know basis. Print outs 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.

8.3 The DPA also requires the CCG to register its data holdings 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. Failure to register or an incorrect registration is a criminal offence and may lead to the prosecution of the organisation.

8.4 Under a provision within the Data Protection Act an individual can request access to their personal information regardless of the media in which this information may be held / retained. The CCG has a Subject Access Procedure for dealing with such requests (please refer to the Information Governance Policy, http://intranet.dorsetccg.nhs.uk/WS-DCCG-Intranet/Downloads/Policies/Corporate/Information%20Governance%20Policy%202015%20.pdf).

8.5 The DPA defines eight principles of good practice to follow when obtaining, processing, holding/storing personal data relating to living individuals. These are referred to as the 'data protection principles'. The CCG must comply with these principles.

Data Protection Principles

Principle 1

8.6 Personal data shall be processed fairly and lawfully.

Principle 2

8.7 Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in a manner incompatible with that purpose or those purposes

Principle 3

8.8 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4

8.9 Personal data shall be accurate and, where necessary, kept up to date.

Principle 5

8.10 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6

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

Principle 7

8.12 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data".

Principle 8

8.13 Personal Data 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.

8.14 For full overview of the principles and their application see Appendix C.

9. CALDICOTT PRINCIPLES

9.1 Following a review of how confidential patient information was handled by the NHS the Caldicott report was published in 1997. The committee conducting the review recommended that each NHS organisation:

- identify a Board Member as the Caldicott Guardian;
- implement six principles (known as the Caldicott Principles) as good practice for all NHS organisations to adopt.

9.2 The Caldicott principles 'mirror' the requirements of the DPA 1998 and are good practice which staff in the NHS are required to adhere to.

9.3 Over recent years, there has been a growing perception that data protection/information governance was being cited as an impediment to sharing information, even when sharing would have been in the patient's best interests.

9.4 Dame Fiona Caldicott was asked to undertake a further review and on 26 April 2013 published a Report which includes revisions to the original Caldicott principles to emphasise the need to give greater focus to sharing information. A 7th principle was added.

9.5 For full overview of the principles and their application see Appendix D.

10. DATA SECURITY AND CONFIDENTIALITY

10.1 The CCG will ensure that personal data is held securely and adequately protected from loss or corruption and that no unauthorised disclosures of personal data are made.

10.2 All personal information relating to members of the public/patients/service users and staff must be kept secure at all times. The CCG has ensured there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Please refer to the following guidance contained within the CCG's IG Policy, http://intranet.dorsetccg.nhs.uk/WS-DCCG-Intranet/Downloads/Policies/Corporate/Information%20Governance%20Policy%202015%20.pdf:

- Procedure for Carrying out Privacy Impact Assessments and Privacy Impact Assessment Template Form;
- Guidance on Information Governance Forensic Readiness;
- Procedure for Information Governance Forensic Readiness;
- Guidance on the Introduction of Bring Your Own Device;
- Guidance on Managing Subject Access Requests and Associated Charges;
- Procedure for Managing Subject Access Requests;
- Guidance on the Management of Records;
- Procedure for the Management of Records;
- Guidance on Data Quality;
- Guidance on Passwords;
- Guidance on the Transmission of Information by Email;
- Guidance on Writing Business Emails;
- Guidance on the Encryption of Emails;
- Guidance on the Transmission of Information by Facsimile;
- Guidance on the Transmission of Information by Post;
- Guidance on the Communication of Information by Telephone;
- Guidance on Pseudonymisation;
- Guidance on Safe Havens;
- Guidance on Smartcards.

10.3 Further details can also be found in the IT Security Policy.

11. INFORMATION SHARING

11.1 Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them, and with other organisations providing related services, the public rightly expect that their personal data will be properly protected.

11.2 When sharing personal information, CCG staff must ensure that the Principles of the DPA 1998, the Human Rights Act 1998, the Caldicott Principles (including Caldicott 2) and the Common Law Duty of Confidentiality are upheld.

11.3 Information should only be shared for a specific lawful purpose or when appropriate consent has been obtained.

11.4 When identifiable information is to be used/shared for non-direct patient care the CCG must ensure that members of the public/patients/service users are aware of the use of the information and provide a means for the member of public/patient/service user to opt out.

11.5 The CCG has an information booklet which clearly informs members of the public/patients/service users why their information is collected, how it may be used and who it may be shared with. Staff must ensure that these booklets are provided to patients when their personal information is first collected. The booklets are available from the Information Governance Team.

11.6 Information sharing protocols (ISP) provide the basis for facilitating the exchange of information between organisations. Dorset CCG has a template ISP for use by staff which is available from the IG Team (contact details in Appendix E).

11.7 All ISPs must be agreed by the IG Group.

11.8 Some disclosures of information may occur because there is a statutory requirement upon the CCG to disclose e.g. with a Court Order, because other legislation requires disclosure (tax office, pension agency - for staff and notifiable diseases - for patients). See appendix F.

11.9 Before sharing information staff must:

- ensure there is a justifiable need to know;
- ensure there is a legal basis for sharing;
- anonymise/pseudonymise the data wherever possible;
- inform the member of public/patient/service user that basic information will be shared;
- seek the individual's consent to disclosure, as appropriate, in accordance with local protocols;

- keep disclosures to a minimum.

11.10 Please contact the Information Governance Team for further advice relating to any form of disclosure of personal information. Contact details available in Appendix E.

Health and Social Care Information Centre

11.11 Where data has been obtained from the Health & Social Care Information Centre (HSCIC) via a Data Service for Commissioners Regional Office (DSCRO) advice must be sought from them prior to release to ensure compliance with the terms of any Data Sharing Contract that may be in force.

Media

11.12 For all requests to share information relating to members of the public/patients/service users staff must contact the Public Relations Lead.

12. DATA PROTECTION CONTRACTUAL CLAUSES

12.1 The CCG is responsible for obtaining appropriate contractual assurance in respect of compliance with DPA (IG) requirements from all bodies that:

- have access to the CCG's information;
- conduct any form of information processing on its behalf.

12.2 This is particularly important where the information is about identifiable individuals as this is a legal requirement under the DPA.

13. PRIVACY IMPACT ASSESSMENT

13.1 In 2008 the Cabinet Secretary commissioned a review of Data Handling Procedures within government in recognition of public interest in the safe handling and sharing of personal data. The report following this review established Privacy Impact Assessments (PIAs) as a requirement for all government departments

13.2 There is no statutory requirement for the CCG to use PIAs however; the Information Commissioner's Office considers the use of a PIA to be good practice. The CCG accepts this recommendation and has introduced the use of a PIA procedure at the beginning of a new project/service and for changes to services.

13.3 A PIA helps assess and identify any privacy concerns, during a new project or change of service, and address them at an early stage.

13.4 The CCG has produced a PIA procedure to assist with the completion of PIA's, and this can be found at Appendix G in the CCG Information Governance Policy or on the CCG Intranet.

13.5 All PIAs must be approved by the IG Group.

14. COMPLAINTS

14.1 Any complaint which may be received because of a breach, or suspected breach, of the Data Protection Act 1998 will be dealt with under the CCG's Complaints Procedure.

15. TRAINING

15.1 It is recognised that the successful implementation of Data Protection Policy is dependent upon the input and commitment of staff at all levels of the organisation.

Induction

15.2 New staff will receive information governance training, delivered by the IG team, as part of their corporate induction. They will also be issued with a copy of the booklet 'Confidentiality: Staff Code of Conduct' at their induction.

Annual Training

15.3 Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. All staff are required to attend mandatory annual information governance training which is run by the IG team and tailored to individual staff groups.

15.4 Subsequent training needs for individual staff members will be identified through the appraisal process/individual performance review process.

15.5 Additional ad hoc information governance training will be provided by the IG team as required, for example following an incident relating to a confidentiality breach.

15.6 The Workforce Directorate and the IG team will monitor take up of the training and report to the IGG. Where there is a low take-up of training, this will be reported to Directors for action.

16. CONSULTATION

16.1 This policy is a legislative requirement and no consultation is required.

17. RECOMMENDATION AND APPROVAL PROCESS

17.1 Refer to Section C – Document Details at the front of this policy.

18. COMMUNICATION/DISSEMINATION

18.1 Refer to Section C – Document Details at the front of this policy.

19. IMPLEMENTATION

19.1 This policy does not require any new aspects to be implemented.

19.2 This policy will be made available to staff through the intranet as detailed in the CCG's policy for the management of procedural documents.

20. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE DOCUMENT

20.1 The Information Governance Group (IGG) takes overall responsibility for ensuring compliance with this policy and any procedures relating to Information Governance contained within the CCG's IG Policy.

20.2 Following each IGG meeting, a report summarising the issues discussed at the meeting is prepared and issued to the Governing Body, Audit and Quality Committee and the Directors Performance Group.

21. DOCUMENT REVIEW FREQUENCY AND VERSION CONTROL

21.1 This policy will be reviewed bi-annually or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Information Commissioner.

Appendix A

GLOSSARY

Phrase	Definition
Corporate Record	Record that relates to an organisation's business activities, processes, activities and transactions.
Corporate and operational records held in any format by the CCG	Administrative records; staffing records; complaints records; financial and accounting records; photographs slides and other images (non clinical); microform (microfiche and microfilm (non clinical records); audio and video tapes, cassettes and CD-ROMs and DVDs; emails; computerized records (databases, output and disks); scanned documents; material intended for short term or transitory use including notes and spare copies of documents; diaries; any other material which holds non clinical information.
Data Controller	A 'data controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is processed.
DPA	An acronym for Data Protection Act.
Data Subject	A 'data subject' means an individual who is the subject of personal data and must be a living individual. Organisations, such as companies and other corporate bodies of persons cannot, therefore, be data subjects. The 'data subject' need not be a United Kingdom national or resident. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject regardless of nationality or residence.
Disclosure	The divulging or provision of access to data.
Document	Not all documents are records. If for example, an email is sent asking the time of a meeting or forwarding a piece of information that is already in the public domain, the email is a document not a record. If, however, the email adds a new piece of information, supplies an appraisal on a member of staff or contributes to decision-making, then it becomes a record, because it is the only evidence of an action or activity.
HSCIC	Health and Social Care Information Centre
Information	A record comprises of information which is a corporate asset.

Phrase	Definition
Information Commissioner	The Information Commissioner is responsible for administering the DPA and enforcing its provisions through powers vested in him and through the courts. Further information is available at www.ico.gov.uk.
Information Governance	Information Governance
IGT	Information Governance Toolkit
NHS Record	An NHS record is anything which contains information, in any media, which has been created or gathered as a result of any aspect of the work of the NHS employees, including agency, temporary, students or bank staff.
Personal Data	The provisions of the DPA apply only to personal data. The term 'personal data' is defined, in section 1(1) of the act as "*data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller, 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".*
Personal Identifiable Data (PID)	Personal identifiable data refers to any data, or combination of data, that can be used to identify an individual.
Processing	Using information in the following ways: • Obtaining • Recording • Retrieving • Altering • Disclosing • Destroying • Using • Transmitting • Erasing.
Pseudonymisation	Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each identifiable patient data item. This allows patient linking analysis which is required within secondary uses.

Phrase	Definition
Record	Recorded information in any format of any type, in any location, which is created, received or maintained by the CCG in the transaction of its activities or the conduct of its affairs and is kept as evidence of such activity.
Sensitive Personal Data	Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.
Subject Access Request (SAR)	Subject Access Rights give individuals the right to make an application in writing to gain access to information held, or processed, about them.
Third Party	Any person other than: • The data subject • The data controller • Any data processor or other person authorised to process for the data controller.

Appendix B

KEY SUPPORTING POLICIES AND PROCEDURES

Policy/Procedure Name	**Approval Details**
Policy and Procedures for requests made under the FOI Act 2000 and the EIR 2004	IGG 15 March 2016
Information Governance Policy	IGG 16 December 2015
Data Protection Policy	IGG 15 March 2016
Confidentiality: Staff Code of Conduct Leaflet	IGG 10 October 2013 Reviewed 3 February 2015
IT Security Policy	IGG 15 March 2016
Procedure for the Management of Serious Incidents	Directors Performance Meeting 18 August 2015
Procedure for the Management of Adverse Incidents	Directors Performance Meeting 5 October 2015
Risk Management Framework	Directors Performance Meeting March 2015
Confidentiality: Patient Information Leaflet	IGG 22 October 2013

Appendix C

Data Protection Principles

1. Principle 1 – "Personal data shall be processed fairly and lawfully"

1.1 This requirement is concerned with making members of the public/patients/service users/staff aware of why the NHS needs information about them, how the information is used and to whom it may be disclosed. To comply, the CCG is required to produce patient and staff information leaflets to explain the use of information.

1.2 The CCG must ensure that the following information is made readily available:

- the identity of the data controller;
- the identity of any nominated representative for the purposes of the Act;
- the purpose(s) for which the data will be processed;
- any other information necessary to ensure fairness: such as the likely consequences of processing, and whether they envisage the data being disclosed to a third party.

1.3 The DPA makes specific provision for sensitive personal data. Any of the following data held by the CCG is considered to be sensitive data within the DPA:

- racial or ethnic origin;
- political opinions;
- religious or other beliefs;
- trade union membership;
- physical or mental health;
- sexual orientation;
- alleged offences;
- criminal proceedings or convictions.

1.4 Under the DPA, personal data shall not be considered to be processed fairly unless certain conditions in schedules 2 and 3 are met.

Schedule 2

1.5 Processing of personal data may only be carried out where at least one of the following conditions in schedule 2 of the DPA are met:

- the individual has given his or her consent to the processing;
- the processing is necessary for the performance of a contract with the individual;
- the processing is required under legal obligation;
- the processing is necessary to protect the vital interests of the individual or to carry out public functions;
- the processing is necessary to comply with any legal obligation to which the data controller is subject;
- the processing is necessary for the administration of justice;
- the processing is necessary for Crown, Ministerial or Government functions;
- the processing is in the functions of public interest.

1.6 Sensitive data can only be processed if one of the conditions in schedule 2 is met plus one of the conditions from schedule 3, which include:

- having the explicit consent of the individual;
- being required by law to process the data for employment purposes;
- needing to process the information in order to protect the vital interests of the data subject or another;
- dealing with the administration of justice or legal proceedings;
- for medical purposes;
- the information has been made public by the individual;
- to safeguard the rights and freedoms of the individual.

1.7 When identifiable information is to be used for non-direct patient care the CCG must write to the patient/service user explaining the use of the information and provide a means for the patient/service user to opt out.

1.8 The CCG has an information booklet which clearly informs members of the public/patients/service users why their information is collected, how it may be used and who it may be shared with. Staff must ensure that these booklets are provided to patients when their personal information is first collected. The booklets are available from the Information Governance Team.

2. Principle 2 – "Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in a manner incompatible with that purpose or those purposes"

2.1 Data can only be processed for the purpose or purposes for which it was originally obtained. When disclosing data, care must be taken to ensure that any person to whom it is disclosed is aware of the purpose or purposes for which the data was intended.

2.2 The Act requires that the CCG must specify the purpose of processing data (e.g. for the provision and administration of Health Care), what data is to be included in this purpose, whom it will be disclosed to and if it is to be transferred overseas.

2.3 In doing so the CCG has to consider that data that it requires. The CCG is legally obliged to notify and register its collection purposes with the Information Commissioner. The current purposes that the CCG has notified are:

- Staff Administration;
- Accounts and Records;
- Health Administration and Services;
- Research;
- Crime Prevention and Prosecution of Offenders;
- Public Health;
- Data Matching.

2.4 Should any member of staff be processing personal data for any purpose other than those listed then you should immediately inform the Data Protection Lead.

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

3.1 The Act requires that the CCG should only use the minimum amount of information required to fulfil the purpose. Staff should collect only data that is required for a specific purpose, and additional information should not be requested unnecessarily.

4. Principle 4 – "Personal data shall be accurate and, where necessary, kept up to date"

4.1 The CCG must take reasonable steps to ensure that all information held on any media, whether manual or electronic, is accurate and up to date. If data is out of date staff need to consider whether using it is likely to cause damage or distress to the individual.

4.2 Users of software will be responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

4.3 Patient/service user and staff information held by the CCG should be checked on a regular basis for accuracy.

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"

5.1 This principle applies to all records, regardless of the media in which they are held, stored or retained. Staff should review all data regularly and archive information that is no longer required. The CCG has a Records Management Policy which follows the Records Retention Schedule documented in the Records Management NHS Code of Practice. The storing and destruction of all records should be in accordance with this policy and retention schedule.

6. Principle 6 – "Personal data shall be processed in accordance with the rights of the data subjects".

6.1 Under this principle of the DPA, individuals have the following rights:

- right of subject access:

  * individuals whose information is held by the organisation have rights of access to it; regardless of the media in which the information may be held/ retained. Individuals also have a right to complain if they believe that the CCG is not complying with the requirements of the Data Protection legislation;

  * the CCG must ensure an up to date procedure is in place to deal with requests for access to information. This can be found in the CCG *Information Governance Policy*;

  * the Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased patients records;

  * once a request for information under the DPA has been received, no amendments or deletions to the data must be made that would not have otherwise been made. In other words, the data must not be tampered with in order to make it acceptable;

- if information is requested that would reveal personal data other than the applicants, the other individual(s) must give consent before it can be released;

- solicitors and insurance companies may make requests on behalf of clients. The client involved **must** sign a written consent form, which needs to be received before any information is released;

- 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:

  - individuals have a right to seek compensation for any breach of the Act which may cause them damage and/or distress;

- right to take action to rectify, block, erase or destroy inaccurate data;
- 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.

6.2 All patients/service users, or someone acting on their behalf, can request to have access to their information held by the CCG. All applications must be made in writing to the Information Governance team. Please refer to the CCG Information Governance Policy.

6.3 The CCG will ensure that the complaints procedures take account of complaints which may be received because of a breach or suspected breach of the DPA 1998.

7. Principle 7 – "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data".

7.1 All staff have a responsibility to ensure that data is kept securely. All information relating to identifiable individuals must be kept secure at all times. The organisation 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.

7.2 Measures should be taken 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 CCG;

- confidential paper waste is shredded or is collected and held in a secure area prior to shredding/incinerating.

7.3 The organisation has a legal obligation to maintain confidentiality standards for all information relating to patients, employees and organisation business. It is important that this information is disposed of in a secure manner. The NHS is most at risk in this area as there have been many occasions when personal information concerning patients has been discovered in public amenity waste disposal or in other public areas.

7.4 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 of how to securely dispose of person identifiable waste products.

7.5 Those systems which are 'run' for the users by the IT department will have their systems backed up on a regular basis as defined by the Information Asset Owner. The master copy of programs and back-ups of data will be kept secure.

7.6 It is important that information about identifiable individuals should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of patient identifiable information is also a requirement of the Caldicott recommendations.

7.7 Some disclosures of information occur because there is a statutory requirement upon the CCG to disclose e.g. with a Court Order, because other legislation requires disclosure - tax office, pension agency (for staff), and notifiable diseases (for patients).

7.8 When sharing identifiable information staff must make reasonable efforts to anonymise the information wherever possible. This particularly applies when sharing information for non-direct patient care purposes.

7.9 If person identifiable information/records need to be transported in any mobile media such as: encrypted CD, Data Stick, Laptop, Palmtop Devices, Magnetic Tape or iPad, then this should be carried out in accordance with the organisation's IT Security Policy.

7.10 All electronic information/records that need to be manually transported will be encrypted to NHS standard. The IT department can provide assistance with this.

7.11 Reliable transport couriers should be used at all times. Packaging should be sufficient to protect the contents from any physical damage during transit, and should be in accordance with manufacturer's specifications.

7.12 Contracts between the organisation and third parties should include an appropriate confidentiality clause which should be disseminated to the third party employees. The Information Governance Team can be contacted for guidance.

7.13 For further guidance please see the:

- Information Governance Policy
- Confidentiality: Staff Code of Conduct, and
- The Information Security Policy.

8. Principle 8 – "Personal Data 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".

8.1 Person identifiable information should not be sent to countries outside the EEA unless checks have been made concerning the levels of protection of the information. Advice should be sought from the Data Protection Lead before entering into any agreement to send information outside of the EEA.

Appendix D

Caldicott Principles

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients (or staff) to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix E

KEY CONTACTS

KEY CONTACTS Job Role	Job Title and Name	Contact Number
Information Governance Team Head of Information Governance and Customer Care (Data Protection Officer, CCG Records Manager, CCG Freedom of Information Lead)	Joyce Green	01305 361252
Information Governance and Customer Care Manager	Helen Williams	01202 541439
Information Governance Officer	Donna Adams	01305 368023
Information Governance and Customer Care Officer	Sandra Legg	01305 368941
Customer Care Officer	Judy Franek	01305 368914 / 8926
Freedom of Information Team	Joyce Green Donna Adams Sandra Legg	01305 361252 01305 368023 01305 368941
Caldicott Guardian Director of Quality	Sally Shead	01305 368053
Senior Information Risk Owner Governing Body Secretary	Conrad Lakeman	01305 361221
Information Risk Lead Patient Safety and Risk Manager	Susie Hawkins	01305 368049
Information Security Manager IM&T Infrastructure Manager	Duncan Pike	01305 368081

Appendix F

Disclosure of personal/sensitive information to the Police and other agencies

1.1 It is sometimes necessary for external agencies to have access to personal information without the consent of the individual.

1.2 If there is a legal duty on the CCG and/or the applicant then disclosure is mandatory and consent is not necessary. This is often the case in the instance of Child Protection issues.

1.3 If the applicant has a legal power to request the information, you can disclose it, but it is not mandatory. This is often the case with police enquiries. The applicant must be able to demonstrate that consent would not be appropriate because of the nature of the investigation. In the instance of the police, this would be done under an exemption of the DPA 1998. A **Section 29(3)** exemption is used when making enquiries which are concerned with:

- the prevention and detection of crime; or
- the apprehension or prosecution of offenders.

1.4 This exemption allows information to be provided by organisations without gaining consent. However, you do not have to supply information, even though the Police have made a considered judgement about their need for information.

1.5 Do not feel pressurised to give information because the police have requested it. It is reasonable to ask why it is needed and what is required before making a decision.

1.6 Staff should always check the identity of anyone requesting information, and only the minimum information to satisfy the request should be given.

1.7 It is recommended that staff should seek advice from colleagues and line managers before making a decision about disclosure. The decisions made and any reasoning should be recorded, as a judgement may have to be made as to whether disclosing information would cause fewer problems than withholding it.

Disclosure under Legal Duty

1.8 The most likely legal basis for disclosure to the police is legal duty, where you MUST disclose, even without consent:

- **Prevention of Terrorism Act (1989) and Terrorism Act (2000)** – if you have gained information about a terrorist activity you MUST inform the police.

- **Court Order** – where the courts have made an order, you must disclose the required information, unless the organisation decides to challenge the order in court.

Disclosure under Legal Power

1.9 The other likely legal basis for disclosure to the police is legal power:

- **The Police and Criminal Evidence Act (1984)** – you can pass on information to the Police, as the Act creates a power to do so if you believe that someone may be seriously harmed. This would be appropriate in the instance of a suspicion of offences such as murder, rape, kidnapping and causing death by dangerous driving, all of which are arrestable offences.

- **The Crime and Disorder Act (1998)** – Information may be required on an individual if there is a need for strategic cross organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in. A nominated officer deals with such requests.

- **Multi Agency Public Protection (includes the Probation Service)** – The Criminal Justice and Court Services Act 2000, sets the framework for sharing information about potentially dangerous offenders. 'Multi Agency Risk Conferences' may require information about individuals.

  If you are requested to provide information, you should consider gaining consent/informing the individual(s) unless this may cause more harm than good. If the risk presented by an individual(s) clearly cannot be effectively managed without information and gaining consent is inadvisable, then relevant information can be shared as it is in the interest of the public.

  If you suspect a child is being abused, you have a legal power to disclose information to Social Services (under 'vital interest' and 'medical purpose' conditions of the DPA) and/or the Police (under the Police and Criminal Evidence Act). You should consider whether gaining consent or informing the child and parents would be beneficial or detrimental to the situation. If detrimental then disclosure without consent is permitted.

- **Public Health (Control of Diseases) Act 1984** and **Public Health (Infectious Diseases) Regulations 1985** – it is a requirement to disclose information about individuals who have notifiable infectious diseases to various agencies.

- **Births and Deaths Act 1984** – It is a requirement to disclose all births and deaths to local government offices.

Other Acts Preventing Disclosure

1.10 There are also some Acts of Parliament that make it a legal requirement not to disclose information. These Acts are detailed below:

- Human Fertilisation and Embryology (Disclosure of Information) Act 1992;
- Venereal Diseases Act 1917 and Venereal Diseases Regulations 1974 and 1992;
- Abortion Act 1967;
- The Adoption Act 1976.