NHS
Herts Valleys
Clinical Commissioning Group

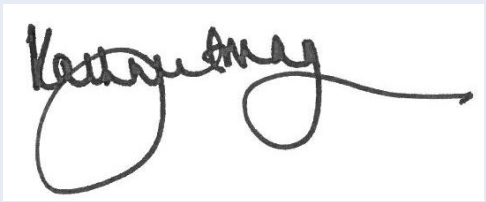
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		Data Protection and Confidentiality Policy
Could this policy be incorporated within an existing policy?	no	
Does this policy follow the style and format of the agreed template?	yes	
Has the front sheet been completed?		
Is there an appropriate review date?	yes	
Does the contents page reflect the body of the document?	yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	yes	
Are all appendices appropriate and/or applicable?	yes	
Have all appropriate stakeholders been consulted?	yes	
Has an Equality Impact Assessment been undertaken?	yes	
Is there a clear plan for implementation?	yes	Update to existing policy
Has the document control sheet been completed?	yes	
Are key references cited and supporting documents referenced?	yes	
Does the document identify which Committee/Group will approve it?	yes	

Plans for communicating policy to – staff; practice membership; public (as appropriate)	yes	Via weekly staff bulletin

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Chief Finance Officer (CFO)	Date	13 March 2018
Signature			

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Chief Executive	Date	13 March 2018
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

Data Protection and Confidentiality

Version Number	4.0
Ratified By	Information Governance Group, Senior Leadership Team and Executive Committee
Date Ratified	13 March 2018
Name of Originator/Author	Information Governance Manager
Responsible Director	Chief Finance Officer
Staff Audience	All Staff
Date Issued	March 2018
Next Review Date	April 2018

NHS
Herts Valleys
Clinical Commissioning Group

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
2.0		Reviewed 2013, 2016		
3.0		Complete review, put into new format DPA Guidelines, Statutory Restrictions on passing on information and definition of sensitive personal data, added as appendixes.	October 2016	IG Manager
4.0		Annual review Reference made to new General Data Protection Regulations (GDPR) which come into force May 2018 Approval by the Virtual Information Governance Group. Approved by Executive Team	December 2017 Jan 2018 March 2018	IG Manager

NHS
Herts Valleys
Clinical Commissioning Group

CONTENTS

Appendices:

NHS
Herts Valleys
Clinical Commissioning Group

Appendix 3 – Definition of Sensitive Data
Appendix 4 – Equality impact Assessment

1. INTRODUCTION

The Data Protection Act 1998 (DPA) covers all personal data held both manually (on paper) and electronically (on a computer) for living individuals. This will be replaced by the General Data Protection Regulations (GDPR) in May 2018.

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. (changes to data processors responsibilities will apply under GDPR)

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, 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.

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 e.g. 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 subject access request.
- There are also some offences around misinformation when registering with the Information Commissioner.

2. PURPOSE

The CCG Data Protection and Confidentiality Policy (This 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 DPA, which is the key piece of legislation covering security and confidentiality of personal information.

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.

3. DEFINITIONS (these may change slightly under GDPR)

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

- from those data, or

- from those data and other information that is in, 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.

Relevant filing system
What is a Relevant filing system?

- any set of information relating to individuals to the extent that, although the information is not processed 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
Processing, in relation to information or data, means obtaining, recording or holding or carrying out any operation or set of operations on the information, including:

- organising, adapting or alteration of the data,
- retrieving, consultation or use of 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.

Data Subject
The Data Subject refers to the individual to whom the personal data relates.

Data Controller
The Data Controller refers to the person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

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 are 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, Cyprus, Czech Republic, Denmark (excluding the Faroe Islands), Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom (excluding the Isle of Man and the Channel Islands),

4. ROLES AND RESPONSIBILITIES

Roles and Responsibilities within the Organisation

The SIRO has overall responsibility for the implementation and delivery of the DPA 1998, on behalf of the CCG with devolved responsibility to the Head of IM&T and the Information Governance Manager.

Responsibility for ensuring that personal information is processed in accordance with the rights of the individual resides at all levels within the CCG.

1. 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.

2. 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.

3. The SIRO is responsible for facilitating the implementation of the policy and supporting CCG staff to understand their responsibilities.

4. The Caldicott Guardian has responsibility for advising CCG staff and for ensuring adequate arrangements are effectively implemented to protect patient identifiable information.

5. The SIRO and Caldicott Guardian are jointly responsible for ensuring the effective integration of respective policies for control of clinical and non-clinical information. The SIRO is responsible for overseeing the development of the policy and its implementation.

6. 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 procedures through annual audit:

- To observe fully 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. The Data Protection Officer (new task under GDPR)

To inform and advise HVCCG and our staff about their obligations to comply with the GDPR and other data protection laws.
To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection privacy impact assessments; train staff and conduct internal audits.
To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, patients etc).

4.1 Consultation and Communication with Stakeholders

Policy will be reviewed by:

- Head of IM&T
- Information Governance Manager
- Senior Leadership Team
- Caldicott Guardian
- SIRO.
- Data Protection Officer

5. 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 their 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 his/her 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 where personal data are used for direct marketing, or where personal data are used inappropriately / illegally,
- To apply for compensation if an individual suffers damage,
- 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.

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

Subject Access Requests (NOTE: changes to charging and timescales under GDPR)

All data subjects, or someone acting on their behalf, can request a copy or 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 Policy and Procedure.

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

Disclosures to others

From April 2013, legislation as part of the Health and Social Care Act 2012 does not permit CCGs to access person identifiable data (PID). Instead CCGs will only be able to view pseudonymised data", i.

Need to Know

Sensitive information is only to be requested on a 'need to know' basis. This means only when the information is necessary to provide a service or to manage the delivery of care effectively, and then only in the best interest of service users or staff.

Some people may decide to refuse a service rather than give the personal information that would enable them to get the service. The CCG recognises this is a right to privacy.

Consent (the use of consent will change under GDPR)

Information that is confidential and restricted will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

Informed (or explicit) consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person.

Information about a deceased person may only be passed on with the informed consent of the executor, i.e. next of kin, Solicitor or someone with written confirmation that they are administering the deceased's estate, in line with Guidance to access information.
Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information.

A consent form is available from the Information Governance Manager.
Confidential information will not be discussed on the telephone unless the identity of the caller is established. This will be checked when necessary, e.g. with call-backs and/or security checks prior to the release of any information.

Circumstances where information can be disclosed

With the patient's/staff written consent for a particular purpose.

On a need to know basis if the person receiving the information is involved in the patient's treatment and requires the information for clinical reasons.

The information is to be used for one of the purposes listed in 'Disclosure of Information to others'.

The information is required by law or under a court order.

In Child Protection proceedings if it is considered that the information

required is in the public or child's interest. This is most likely to be justifiable in relation to the paramount of the child's interests.

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.

Disclosures without consent can occur in order to prevent serious crime. Request for information by the Police must be carefully considered. All Police information requests must first go to the Information Governance Manager who will liaise with the Caldicott Guardian.

Difficult decisions to releasing information may require legal advice prior to disclosure; this will be actioned by the Head of IM&T, Information Governance Manager, the Caldicott Guardian and the CCG Virtual Information Governance Group.

The CCG must be able to justify any decision when information has been disclosed.

Circumstances in which information cannot be disclosed

Where patient/staff have expressed a wish that information should be withheld. However, there may be overriding situations where, under the Data Protection Act , sensitive personal data may be processed. All of these instances are set out in paragraphs 2-10 of Schedule 3 of the Data Protection Act.

The consequences for their treatment (for example where non-disclosure will affect the CCG's ability to work with another agency such as Social Services Department) this must be explained to the patient and agreement sought on non-disclosure. This must be documented.

The patient's wishes must be communicated to other staff that need to know, and documented.

Patient information must not be disclosed under any circumstances for the purposes of fund raising or commercial marketing.

Disclosure of information on the following are restricted by law:

- HIV
- AIDS
- Sexually transmitted diseases
- Assisted conception
- Abortion

Such information must only be disclosed by one of the very limited number of people authorised to do so and in accordance with the relevant statutes

Storage of Data

No written document containing patient identifiable information must be left visible where it can be read by anyone. This includes telephone messages, computer screens, prints outs, letters and other documents.

All hardware containing data must be housed in a secure environment.

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 information 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 breach. A copy of the CCG disciplinary procedures is made available to all staff.

The CCG is required to undertake Disclosure and Barring Service checks on certain groups of staff. The DBS 'check' is fully compliant with the DPA 1998 and the Freedom of Information Act 2000.

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. Under GDPR the CCG has 1 calendar month in which to provide the data and a charge can no longer be requested.

6. MONITORING COMPLIANCE

Outline here the arrangements for monitoring and reviewing the policy, including the person responsible and the date of review. Monitoring tools must be built into all procedural documents in order than compliance and effectiveness can be demonstrated. The approach to be adopted will depend on the policy but could include

- Audits
- Patients views and experiences
- Benchmarking
- Staff surveys
- Environmental Impact Analysis
- Complaints monitoring
- Trend Analysis
- Incident Reporting and Monitoring
- Monitoring ethnicity/diversity access

7. EDUCATION AND TRAINING

All CCG staff are required to undertake annual mandatory information governance training via https://www.e-lfh.org.uk/ Or by contracting the information governance team.

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 regards 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.

9. REFERENCES

Data Protection Act 1998
General Data Protection Act (GDPR) – May 2018
Freedom of Information Act 2000

10. ASSOCIATED DOCUMENTATION

Information Governance Management Framework
Information Governance Policy
Information Risk Policy
IG - A Guide to Staff
Information Security Policy
Subject Access Request Policy
Safe Haven Policy

NHS
Herts Valleys
Clinical Commissioning Group

Appendix 1 - Data Protection Act - Guidelines

Data Protection

The 1998 Act covers information held on all media relating to living persons, it refers to: (The Access to Health Records Act 1990 covers deceased persons).

- Automatically processed information
- Information in manual filing systems where the information is filed such that particular information relating to particular individuals is readily available.
- Information which was recorded to be automatically processed under 1, or, will become part of a filing system under point 2.

The purpose of the Act is to protect individuals and the information stored about them. The Act requires that a valid purpose is declared for the retention and/or processing of such data by any system. The Act also places an obligation on the owners and users of such data to protect the accuracy and physical security as well as the confidentiality of the information.

The Act places responsibilities and legal liabilities on individual users of data as well as on the organisations that own the data and/or systems on which it is processed.

The Data Protection Act 1998 requires every data controller who is processing personal information in an automated form to notify, unless they are exempt. In addition to the purpose for which data will be stored and used, the notification covers the source of information and any parties to whom the information may be disclosed. Individuals have the right of access to information stored that relates to them, subject to certain conditions in the case of medical information. The user is obliged to correct any mistakes that might be identified. The individual must be supplied with an explanation of any "coded" information that is stored in relation to them.

The 8 Data Protection Principles are as follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions set out in schedule 2 of the Act is met. In the case of sensitive personal data, one of the conditions set out in schedule 3 of the Act must also be met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those

purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
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.

NHS
Herts Valleys
Clinical Commissioning Group

Appendix 2 – Statutory Restriction on Passing on Information

1. The **NHS (Venereal Diseases) Regulations (1974)** and the **NHS Trusts (Venereal Diseases) Regulations (1991)** prevent the disclosure of any identifying information about a patient with a sexually transmitted disease (including HIV and AIDS) other than to a medical practitioner (or a person employed under the direction of a medical practitioner) in connection with and for the purposes of the treatment of the patient, or to prevent the spread of the disease. The regulations do not prevent the normal notification of other communicable diseases in such patients.

2. The **Human Fertilisation and Embryology Act (1990)**, as amended by the **Human Fertilisation and Embryology (Disclosure of Information Act) 2008,** limits the circumstances in which information may be disclosed by centres licensed under the Act: see the Human Fertilisation and Embryology Authority's Code of Practice (HFEA, Paxton House, 30 Artillery Lane, London, E1 7LS).

3. The **Abortion Regulations (1991), as amended by the Abortion England Regs (2002)** made under the Abortion Act 1967, limit and define the circumstances in which information submitted to the Chief Medical Officer may be disclosed.

4. **Human Rights Act (1998)** – Article 8 of the Human Rights Act (1998) refers to the 'right to respect for private life'

NHS
Herts Valleys
Clinical Commissioning Group

APPENDIX 3

Definition of Sensitive Personal Data (Schedule 3 of the Data Protection Act 1998)

Sensitive personal data

The 1998 Act introduces categories of sensitive personal data, namely, personal data consisting of information as to:-

a) the racial or ethnic origin of the data subject;
b) their political opinions;
c) their religious beliefs or other beliefs of a similar nature;
d) whether they are a member of a trade union;
e) their physical or mental health or condition;
f) their sexual life;
g) the commission or alleged commission of any offence by the data subject; or
h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

NHS
Herts Valleys
Clinical Commissioning Group

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	HVCCG Data Protection Confidentiality Policy
What is it that is being proposed?	The CCG Data Protection and Confidentiality Policy (This 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 DPA, which is the key piece of legislation covering security and confidentiality of personal information.
What are the intended outcome(s) of the proposal	That all CCG staff are aware of their responsibilities and are aware of legal requirements and CCG processes.
Explain why you think a full Equality Impact Assessment is not needed	This policy sets the information governance requirements in relation to Data Protection and Confidentiality.
On what evidence/information have you based your decision?	The policy refers to information Data Protection Act 1998 and the new General Data Protection Regulations which come into force May 2018
How will you monitor	Via the IG Toolkit

NHS
Herts Valleys
Clinical Commissioning Group

the impact of policy or service?	
How will you report your findings?	To the Senior Leadership Team via toolkit action plans and compliance reports

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.	
Assessors Name and Job title Date 18/12/2017	Ruth Boughton Information Governance Manager