NHS
Wiltshire
Clinical Commissioning Group

## Document information

| | |
|---|---|
| Document type: | Policy |
| Document reference: | |
| Document title: | **Data Protection Act Policy** |
| Document operational date: | November 2013 |
| Document sponsor: | Steve Perkins, Senior Information Risk Officer |
| Document manager: | Susannah Long, Governance & Risk Manager |
| | |
| Approving Committee/Group: | Audit & Assurance Committee (Reviewed IGG December 2017) |
| Approval date: | January 2018 |
| Version: | 3.0 |
| Recommended review date: | January 2018 |
| | |
| Intranet location: | Policies |

*Please be aware that this printed version of this document may NOT be the latest version. Please refer to the internet for the latest version.*

## Summary

This policy explains the principles and processes which underpin the commitment of the Clinical Commissioning Group (CCG) to the protection of personal data. Personal data may relate to patients or staff.

## Consultation

This policy was developed in consultation with the Senior Information Risk Officer, Caldicott Guardian, Lead Director for Information Governance and the Central Southern Commissioning Support Unit Information Governance Team and has been reviewed and amended by the Information Governance Group.

## Appendices

The following appendices form part of this document:

Appendix 1: The 8 Data Protection Principles and 7 Caldicott Principles
Appendix 2: Evaluation Standard

**Review Log**

| Version | Review Date | Reviewed By | Changes Required? (If yes, please summarise) | Changes Approved By | Approval Date |
|---|---|---|---|---|---|
| 1.1 | Oct'16 | Senior IG Manager | Change reference to NHS Digital;<br>Change CSU name;<br>Update reference to Records Management Code of Practice for Health & Social Care 2016;<br>Recognition of on-line training availability;<br>Removal of annual audit. | IGG | Oct'16 |
| 2.1 | Oct'17 | Senior IG Manager | Update to Records Management Code of Practice for Health & Social Care<br>Remove Director Responsible for IG role | IGG | Dec'17 |
| | | | | AAC | Jan'18 |
| | | | | | |

**Acknowledgements**

Standard Data Protection Act Policy written and provided by Central Southern Commissioning Support Unit in 2013.

# Contents

# DATA PROTECTION ACT POLICY

## 1.0 INTRODUCTION AND PURPOSE

This policy explains the principles which underpin the commitment of the Clinical Commissioning Group (CCG) to the protection of personal data. Personal data may relate to patients or staff.

.

The CCG needs to collect and use certain types of information about people with whom it deals in order to operate. This will include information about patients, employees, suppliers, clients, customers, and others with whom it communicates. In some cases this information will be current, or it could be historical or prospective. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments for business data, for example. This personal information must be dealt with properly, however it is collected, recorded and used, whether on paper, in a computer, or recorded on other material and there are safeguards to ensure this in the Data Protection Act 1998.

## 2.0 SCOPE AND DEFINITIONS

This Policy covers all personal data processed by the CCG, including data relating to both Staff and Patients.

The CCG recognises the importance of correct and lawful handing of personal data, as specified in the Data Protection Act 1998.

This policy applies to all CCG staff including contractors and volunteers.

Personal data is data about a living individual who can be identified from that data or other data/information that is in the possession or likely to come into possession of the data controller. This includes any expression of opinion about the individual and any intentions of the data controller or any other person in respect to the individual. Data regarding a deceased person is covered by the Access To Health Records Act 1990.

## 3.0 PROCESS / REQUIREMENTS

### 3.1 Data Protection Principles

The Governing Body regard the lawful and correct treatment of personal information by the CCG as very important to successful operations and to maintaining stakeholder confidence in the CCG. The Governing Body will ensure that the organisation treats personal information lawfully and correctly.

To support this, the Governing Body fully endorse and adhere to the Principles of data protection, as enumerated in the Data Protection Act 1998.

Specifically, the Principles require that personal information:

1. shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met;
2. 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. shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. shall be accurate and, where necessary, kept up to date;
5. shall not be kept for longer than is necessary for that purpose or those purposes;
6. shall be processed in accordance with the rights of data subjects under the Act;
7. shall be protected by appropriate technical and organisational measures to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. 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.

## 3.2 Policy Statement

In order to meet the requirements of the Data Protection Act, the CCG will:

- Observe fully the conditions regarding the fair collection and use of personal data;
- Meet its obligations to specify the purposes for which personal data is used;
- Collect and process appropriate Personal Data only to the extent that it is needed to fulfil operational or any legal requirements;
- Ensure the quality of Personal Data used;
- Apply appropriate checks to determine the length of time Personal Data is held;
- Take the appropriate technical and organisational security measures to safeguard Personal Data;
- Ensure that Personal Data is not transferred abroad without appropriate safeguards.

In addition, the CCG will ensure that:

- All staff managing and handling personal information understand that they are contractually responsible for following good data protection practice;

- All staff managing and handling personal information are:

    - Appropriately trained;
    - Appropriately supervised;
    - Know who to contact, should they have any queries;

- Any requests from data subjects around how their data is being used will be answered promptly;

- The methods for handling personal data are regularly evaluated and assessed;

- Data sharing is carried out under written agreement, clearly setting out the scope, limits and conditions for sharing;

- Any disclosure of personal data will be in line with agreed procedures;

- The Data Protection Notification is regularly reviewed for accuracy;

- All staff are to receive Data Protection Act training annually.

### 3.3 Data Shared With Third Parties

The CCG will ensure that all contracts with third parties will:

- Identify where personal data is being received into or sent out of the CCG;

- Specify who is the Data Controller and who is the Data Processor, or whether data is Controlled jointly or in common;

- Confirm that the third party has robust processes in place to comply fully with the Data Protection Act;

- Adhere to the guidance provided by the CSU Information Governance Team on safe information sharing.

### 3.4 Transfer of Personal Information

The CCG will ensure that:

- All Staff follow the ‘Transfer of Personal Information’ Procedure;

- The transfer is lawful.

### 3.5 Subject Access Requests

The CCG will ensure that all Subject Access Requests are:

- Completed within 40 days, in line with the Data Protection Act;
- Passed to the CSU Information Governance Team on receipt in line with the Subject Access Request procedure for processing;
- Acknowledged on behalf of the CCG.

The response will be:

- Reviewed for references to third parties and potential for serious harm, in line with the Data Protection Act;
- Presented in such a way that the data subject can understand what information is being held, why is it being held and with whom it is or might be shared.

The CCG will not normally charge for managing the SAR and providing copy information.

### 3.6 Records Retention

The CCG will ensure that all personal data is stored only:

- For as long as is necessary;
- In line with the CCG Records Management Policy and the Records Management Code of Practice for Health & Social Care 2016.

### 3.7 Adverse Event and Risk Reporting

The CCG will ensure that all adverse events and risks are:

- Reported promptly to the Senior Information Governance Manager;
- Reported appropriately to the SIRO and Caldicott Guardian;
- Recorded within a formal process to ensure learning and/or risk mitigation;
- Reported to the Information Commissioner where appropriate.

### 3.8 Data Flow Mapping

The CCG will ensure that all flows of personal confidential information are:

- Formally recorded on the Data Flow Map;
- Formally risk assessed, referring to the risk management matrix in the CCG Risk Management Policy, with the SIRO informed of all risks;
- Reviewed annually;
- Risk assessed again should any changes to process or flows occur.

### 3.9 Information Asset Register

The CCG will ensure that all information assets are:

- Formally recorded on the Information Asset Register;
- Allocated an Information Asset Owner;
- Formally risk assessed with the SIRO informed of all risks;
- Reviewed annually;
- Risk assessed again should any changes to processes or assets occur.

### 3.10 Notification to the Information Commissioner

The Information Commissioner maintains a public register of Data Controllers. The CCG is registered as a Data Controller.

The Data Protection Act 1998 requires every Data Controller who is processing personal data, to notify and renew notification, on an annual basis. Failure to do so is a criminal offence.

Any changes to the register must be notified to the Information Commissioner, within 28 days and managers are responsible for notifying and updating the SIRO and Caldicott Guardian of the processing within their area of responsibility.

The CSU Information Governance Team will assist with and arrange the annual notification renewal.

## 4.0 ROLES AND RESPONSIBILITIES

### Governing Body

It is the role of the Governing Body to define the CCG policy in respect to the Data Protection Act. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

### Accountable Officer

The Interim Chief Officer, as Accountable Officer of the CCG, has overall accountability and responsibility for the implementation of the Data Protection Act within the CCG and is required to provide assurance, through the Annual Governance Statement that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

### Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is an Executive Director of the CCG Governing Body. The SIRO is expected to understand how the strategic business goals of the CCG will be impacted by information risk. The SIRO acts as an advocate for information risk on the Governing Body and in internal discussions, and will provide written advice to the Accountable Officer on the content of their Annual Governance Statement (AGS).

The Chief Financial Officer is the SIRO for the CCG.

The SIRO will provide an essential role in ensuring that identified information security threats are investigated and adverse events managed. They will also ensure that the Governing Body and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the CSU Information Governance Team, the CCG Caldicott Guardian, the CCG IG Lead Manager, and a network of Information Asset Owners and Information Asset Administrators, although the ownership of the information risk assessment process will remain with the SIRO.

### Caldicott Guardian

The Caldicott Guardian will guide the CCG on matters of confidentiality relating to patient and staff information and act as a ‘conscience’ on its use. The role is pivotal in ensuring the balance between maintaining confidentiality and the delivery of care.

The Caldicott Guardian has responsibility for ensuring staff comply with the Caldicott Principles and the NHS Confidentiality Code of Practice.

The role will advise the Governing Body on progress and major issues that may arise. The Caldicott Guardian for the CCG is the Director of Nursing and Quality.

**Data Protection Support**
Support is available from the Information Governance and Freedom of Information Team at the CSU. Support is also available from the CCG IG Lead Manager.

**The Information Governance Group**
The Information Governance Group is responsible for overseeing day to day management of Data Protection, developing and maintaining policies, standards, procedures and guidance, as appropriate, and promoting Data Protection best practice across the CCG.

**Information Asset Owners**
Information asset owners (IAO) shall ensure that information risk assessments are performed at least every six months on all information assets where they have been assigned 'ownership', following guidance from the SIRO. IAO shall submit the risk assessment results and associated plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions along with expected completion dates, as well as residual risks.

**Information Asset Administrators**
Information Asset Administrators (IAA) shall manage the information held within a department in line with the Data Protection Act 1998 and CCG Information Governance policies. IAA will carry out information risk assessments as directed.

**All Managers**
All Managers within the CCG are responsible for ensuring the requirements of this policy are recognised and local processes comply. This will include the nomination of departmental staff as Information Asset Owners or Administrators as necessary and release of staff for information asset audits. All managers are expected to use the Evaluation Tool at Appendix 2 to assess local compliance and take necessary remedial steps.

Managers are responsible for ensuring all staff undertake mandatory Information Governance on-line training and attend any awareness training. They are also responsible for addressing any training needs identified during process change or a change in duties.

Managers shall promote a culture of good information governance and will cooperate fully with any investigation into information governance breaches.

**All Staff**
All staff, whether permanent, temporary or contracted, are responsible for ensuring that they are aware of the requirements incumbent on them and for ensuring they comply with these on a day to day basis.

All staff are expected to alert their manager if they feel they need additional training or guidance and must alert the SIRO and Caldicott Guardian should they encounter information risks, whilst undertaking their duties.

**Failure to comply with this policy may result in disciplinary action and/or civil/criminal action.**

## 5.0 TRAINING

The CCG will ensure that all staff receives appropriate and relevant training to support their responsibilities under this policy. Mandatory training will be provided via the on-line NHS Digital tool, where available.

Successful completion of training will be monitored in accordance with the Learning and Development Policy.

## 6.0 EQUALITY, DIVERSITY AND MENTAL CAPACITY

An Equality Impact Assessment (EIA) has been completed for this policy and no adverse effect has been identified. The EIA will be available on request. This policy has been assessed and meets the requirements of the Mental Capacity Act 2005.

## 7.0 SUCCESS CRITERIA / MONITORING EFFECTIVENESS

The SIRO will, on occasion, commission Internal Audit to critically review the CCG assessment against the Information Governance Toolkit or review IG arrangements. Findings of this audit will be reported to the Audit & Assurance Committee. Implementation of any actions identified as necessary or recommended during the audit will be monitored, as a minimum, at the next annual assessment.

In addition, Appendix 2 within this policy provides an Evaluation Standard which should be used corporately by the CCG Information Governance Lead Director and by Department Managers to assess compliance with this policy. Results from any corporate assessment will be presented to the Information Governance Group.

Any non-compliance with this policy should immediately be reported using the Non-compliance Form contained within the Policy on Management of Procedural Documents.

## 8.0 REVIEW

This document may be reviewed at any time at the request of either staff side or management, but will be reviewed where there is any major change in legislation or NHS guidance and after one year.

## 9.0 REFERENCES AND LINKS TO OTHER DOCUMENTS

This policy should be read in conjunction with the NHS Code of Confidentiality and the following CCG policies:

Information Governance Framework
Information Governance Policy
Information Security Policy
Freedom of Information Act and Environmental Information Regulations Policy
Records Management Policy
Learning & Development Policy
Policy on Management of Procedural Documents

Other policies and procedures may become available during the lifespan of this policy.

**Related Guidance/Information:**

Records Management Code of Practice for Health & Social Care 2016
Data Protection Act 1998
Access to Health Records Act 1990

**APPENDIX 1**

**The 8 Data Protection Principles**

Data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specified and lawful purpose(s);
3. Be adequate, relevant and not excessive in relation to the purpose(s);
4. Be accurate and, where necessary, up to date;
5. Not be kept for longer than necessary;
6. Be processed in accordance with the rights of the Data Subject;
7. Be protected by appropriate technical and organisational measures against unauthorised/unlawful processing and against accidental loss, destruction or damage;
8. Not be transferred outside the EEA unless adequate protection of rights and freedoms are ensured.

**The 7 Caldicott Principles**

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

**APPENDIX 2**

# EVALUATION STANDARD

Policy Name: Data Protection Act Policy
Policy Reference: TBC

Standard statement

The CCG needs to collect and use certain types of information about people with whom it deals in order to operate. This will include information about patients, employees, suppliers, clients, customers, and others with whom it communicates. This personal information must be dealt with properly, however it is collected, recorded and used, whether on paper, in a computer, or recorded on other material and there are safeguards to ensure this in the Data Protection Act 1998.

Criteria - Corporate

1. The CCG registration as a Data Controller is in place and correctly reflects the activities of the CCG.

2. All Subject Access Requests are immediately sent to the CSU Information Governance Lead.

3. All Subject Access Requests are sent a formal acknowledgement.

4. All requests are responded to within the statutory timeframe of 40 days.

5. All departments have Information Asset Owners and Information Asset Administrators in place.

6. An Information Asset Register is in place.

7. A data flow map is in place.

8. Results of information asset audits are reported to the Information Governance Group.

9. Information Sharing Agreements are in place and have, where appropriate, been reviewed.

10. All relevant information asset adverse events are investigated.

Criteria - Departmental

11. All paper Subject Access Requests (SAR) are stamped with the date of receipt, and both paper and emailed SAR are passed to the Information Governance Lead within one working day to be processed by the CSU.

12. All document search requests for SAR received from the CSU by team members are identified as a high priority and responded to within the stipulated time frame.

13. All information assets within the Department are recorded on the Information Asset Register and have an associated Information Asset Owner and Information Asset Administrator.

14. All information flows and information sharing are identified and where appropriate Information Sharing Agreements are in place.

15. All staff have received and successfully completed appropriate training in line with the Training Needs Analysis (TNA).

16. All information adverse events (including breaches of the Data Protection Principles) are reported and, where appropriate, investigated.

17. Information is held no longer than is necessary and is disposed of appropriately in line with the Records Management Code of Practice for Health & Social Care 2016 Retention and Disposal Schedule.

Conclusion

Please explain any discrepancies below:

| |
|---|
| |

Please detail remedial action to prevent re-occurrence, giving details of monitoring arrangements to assess improvement:

| |
|---|
| |

| | |
|---|---|
| Date of assessment: | |
| Assessed by: | |