NHS
Wiltshire
Clinical Commissioning Group

Document information

Document type:	Policy
Document reference:	
Document title:	**Information Security Policy**
Document operational date:	November 2013
Document sponsor:	David Noyes, Director of Planning, Performance & Corporate Services
Document manager:	Susannah Long, Governance & Risk Manager
Approving Committee/Group:	Audit & Assurance Committee
Approval date:	November 2013
Version:	1
Recommended review date:	November 2016
Internet location:	

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 has been created to describe how CCG information should be protected in order to ensure **confidentiality,** only available to those with a legitimate reason to see it, **integrity,** trusted to be of good quality and **availability,** available to those that need it, when they need it.

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.

Appendices

The following appendix forms part of this document:

Appendix 1: Evaluation Standard

Review Log

Version	Review Date	Reviewed By	Changes Required? (If yes, please summarise)	Changes Approved By	Approval Date

Acknowledgements

Standard Information Security Policy written and provided by Central Southern Commissioning Support Unit.

INFORMATION SECURITY POLICY

1.0 INTRODUCTION AND PURPOSE

Information is an asset which, like other important business assets, has value to an organisation and its stakeholders and needs to be suitably protected.

This information security policy sets out how CCG information should be protected in order to ensure its:

- **Confidentiality**
  That information is only available to those with a legitimate reason to see it.

- **Integrity**
  That information can be trusted to be of good quality.

- **Availability**
  That information is available to those that need it, when they need it.

If any of these are compromised, this can have a direct impact on the ability of the CCG to fulfil its objectives and may have consequences for individuals, for patient care, for the local health economy and to the reputation of the CCG.

The CCG has legal obligations to maintain security and confidentiality, notably under the:

- Data Protection Act (1998)
- Human Rights Act (1998)
- Copyright Patents and Designs Act (1988)
- Computer Misuse Act (1990).

In addition, the Caldicott Committee's Report on the Review of Patient-Identifiable Information, published in 1997, led to the establishment of a set of clear principles, reflecting best practice in the handling of confidential patient Information. The report called for regular and routine testing of information flows against these principles overseen by a network of Caldicott Guardians who would act, within each organisation, in a strategic, advisory and facilitative capacity.

Following a review, Caldicott 2 was published in May 2013 and featured 23 recommendations. The Caldicott principles inform this policy.

The policy aims to ensure that:

- Information systems, whether electronic or manual are properly assessed for security;
- Confidentiality, integrity and availability are maintained;
- Staff and managers are aware of their responsibilities; and

- Any risk to the information resource of the CCG is identified, recorded and effectively managed.

2.0 SCOPE AND DEFINITIONS

This Policy covers all information acquired and processed by the CCG.

The Policy covers all information systems utilised by the CCG.

The Policy covers all staff employed by or acting on behalf of the CCG.

3.0 PROCESS / REQUIREMENTS

3.1 GENERAL

The CCG will maintain an Information Security Policy supported by appropriate linked policies, codes of practice, protocols and guidance documents that reflect best practice. It will ensure that all staff have access to that Policy and its subordinate documents by cascading information to managers, briefing staff and posting copies on the intranet/internet as appropriate.

The CCG will comply with legislative requirements and seek to maintain compliance with national guidance and best practice.

The CCG will have procedures in place to evaluate security measures systematically with the greatest emphasis being given to areas where the potential impact of a security breach would be most serious.

The CCG will assign responsibility to key personnel to ensure a sound and robust security and information management infrastructure.

The CCG Governing Body will identify appropriate resources for information security. The Governing Body will carefully consider the likelihood and consequences of identified information security risks when contemplating risk mitigation.

3.2 PROCESS CHANGES

The CCG will ensure that when changes take place that may impact on information assets:

- A risk assessment is undertaken, with respect to information security best practice;

- The SIRO will be informed of the findings of the risk assessment; and

- Guidance will be sought from the CSU Information Governance Team.

3.3 THIRD PARTIES

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

- Identify where personal data is being received or sent out of the CCG (information flows);
- Confirm that the third party has robust processes in place to comply fully with the Data Protection Act;

The CCG will ensure that:

- Information Sharing Protocols (ISP) are in place where appropriate;
- There is adherence by both parties 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.
- Any transfer of personal information is Lawful.

3.5 ADVERSE EVENT AND RISK REPORTING

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

- Reported promptly to the SIRO (and Caldicott Guardian for patient information);
- Reported and recorded within a formal process, in line with the CCG Adverse Event Reporting and Investigation Policy, to ensure they can be learnt from or mitigated.

3.6 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 on a six monthly basis;
- Risk assessed again should any changes to processes or assets occur.

3.7 BUSINESS CONTINUITY

The CCG will ensure that:

- A tested Business Continuity Plan is adopted;

- The Business Continuity Plan covers all assets identified on the Information Asset Register;

- The Business Continuity Plan has a process for prioritising assets identified as high risk in terms of likelihood and consequence;

- The plan will be reviewed at least annually.

4.0 ROLES AND RESPOSIBILITIES

Governing Body
It is the role of the Governing Body to define the CCG policy in respect of Information Security, taking into account legal and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Chief Officer
The Chief Officer as Accountable Officer of the CCG has overall accountability and responsibility for Information Security 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 advice to the Chief Officer on the content of their Annual Governance Statement.

The SIRO will provide an essential role in ensuring that identified information security threats are managed and adverse events are reported and investigated. They will also ensure that the Governing Body and the Chief 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 and a network of Information Asset Owners and Information Asset Administrators, although the ownership of 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 information and acts 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.

Director Responsible for Information Governance

The Director responsible for the processes and procedures for the management of Information Governance (of which information security is a part) is the Director of Planning, Performance and Corporate Services. This Director will also oversee the support contract with CSCSU.

The Information Governance Group

The Information Governance Group is responsible for overseeing day to day information security issues, developing and maintaining policies, standards, procedures and guidance and for promoting Information Security best practice across the CCG.

Information Asset Owners

Information asset owners (IAOs) shall ensure that information risk assessments are performed at at least six monthly intervals on all information assets where they have been assigned “ownership”, following guidance from the SIRO. IAOs shall submit the risk assessment findings 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 and details of any residual risks.

Information Governance CCG Lead

The CCG Lead will support the SIRO, Caldicott Guardian and Lead Director in management of the information security process and the CSU support contract. The CCG Lead will facilitate reporting to the Information Governance Group.

Information Security Support

Support is also available from the Information Governance and FOI Team at the CSU.

All Managers

All Managers within the CCG are responsible for ensuring the requirements of this policy are recognised and local processes ensure compliance. All managers are expected to use the Evaluation Tool at Appendix 1 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. Managers shall promote a culture that supports information security.

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 responsible for:

- Alerting their manager should they identify information risks whilst undertaking their duties;
- Reporting all actual or suspected information security breaches to the CCG SIRO for investigation;
- Holding information securely and only sharing information in line with the principles of the Data Protection Act;
- Adhering to the Caldicott principles;
- Adhering to the NHS Code of Confidentiality;
- Alerting their line manager, should they feel they need additional training or guidance.

Failure to comply with this policy may result in disciplinary action.

5.0 TRAINING

The CCG will ensure that all staff receive appropriate and relevant training. Mandatory training will be provided via the on-line Information Governance training supplied by Connecting for Health.

The CCG Information Governance Lead, SIRO and Caldicott Guardian will liaise with the CSU support team to ensure that any additional training and awareness raising material thought to be necessary is made available to all staff.

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 effects have been identified. The EIA will be published on the CCG internet.

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 an annual basis commission an audit to critically review the CCG assessment against the Information Governance Toolkit. 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 1 within this policy provides an Evaluation Standard which should be used corporately by the CCG Information Governance Lead 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 three years.

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
Data Protection Act Policy
Records Management Policy
Transfer of Personal Information Procedure
Learning & Development Policy
Policy on Management of Procedural Documents

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

Related Guidance:

Records Management: NHS Code of Practice

APPENDIX 1

EVALUATION STANDARD

Policy Name: Information Security Policy
Policy Reference: TBC

Standard statement

The CCG will ensure that CCG information will be protected in order to ensure confidentiality, integrity and availability.

Criteria

1. All information assets are recorded on the Information Asset Register.

2. All information assets are assigned an Information Asset Owner.

3. All contracts stipulate required security measures for information security.

4. All information flows are mapped and Information Sharing Protocols are in place where applicable.

5. Risks to information assets are assessed on a six monthly basis.

6. Any security breaches or adverse events and reported, recorded and investigated in line with the CCG Adverse Event Reporting and Investigation Policy.

7. Business continuity plans are in place and tested to ensure the availability of information.

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:	