NHS
South Warwickshire
Clinical Commissioning Group

Information Governance Policy

VERSION CONTROL

Version:	3.0
Ratified by:	Governing Body
Date ratified:	20/06/2016
Name of originator/author:	Information Governance Officer – Arden & GEM Commissioning Support Unit
Name of responsible committee:	Clinical Quality and Governance
Date last issued:	30/01/2019
Review date:	January 2022

VERSION HISTORY

Date	Version	Comment / Update
03/04/2013	1.0	Approved by Governing Body.
18/03/2016	1.1	Minor proofreading amendments and role updates.
20/07/2016	2.0	Approved by Governing Body.
03/07/2018	2.1	Amendment made by Corporate Governance Manager to update year of Data Protection Act to 2018.
24/09/2018	2.2	Reviewed by Corporate Governance Manager - corrections requested.
05/11/2018	2.3	Corrected version provided by Information Governance Officer – Arden & GEM Commissioning Support Unit.
28/11/2018	2.4	Reviewed by Clinical Quality and Governance Committee. Minor amendments requested. Recommended to Governing Body.
23/01/2019	3.0	Approved by the Governing Body.

Contents

1. Introduction....4
2. Principles....4
3. Scope....6
4. Responsibilities....6
5. Legislation and the NHS....8
6. Equality and Diversity Impact Assessment....8
7. Monitoring Compliance and Effectiveness of the Policy....8
8. References and Further Reading....9

1. Introduction

1.1. This document outlines NHS South Warwickshire CCG's overarching Information Governance arrangements and the relationships between NHS South Warwickshire CCG and the Commissioning Support Unit. The Commissioning Support Unit is responsible for providing the CCG with Information Governance services, operating within the NHS framework for information governance and are formally appointed as data processors.

1.2. Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management.

1.3. Information Governance is concerned with the way NHS organisations handle information about patients/clients and employees, in particular personal and sensitive information. It allows organisations and individuals to ensure that personal information is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

1.4. Information Governance is a framework that brings together all of the requirements, standards and best practice that apply to the handling of personal information.

1.5. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

2. Principles

2.1. The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information. NHS South Warwickshire CCG also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

2.2. The CCG believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

2.3. The CCG is committed to ensuring that information in whatever its context is processed as determined by prevailing law, statute and best practice.

2.4. There are four key interlinked strands to the Information Governance Policy:

- Openness;
- Legal Compliance;
- Information Security;
- Information Quality Assurance.

2.4.1. In respect of Openness:

- Non-confidential information on the CCG and its services should be available to the public through a variety of media, in line with the CCG's code of openness;

- The CCG will establish and maintain policies to ensure compliance with the Freedom of Information Act;

- The CCG will undertake or commission annual assessments and audits of its policies and arrangements for openness;

- Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients;

- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media;

- The CCG will have clear procedures and arrangements for handling queries from patients and the public.

2.4.2. In respect of Legal Compliance:

- The CCG regards all identifiable personal information relating to patients as confidential;

- The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements;

- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;

- The CCG will establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the Common Law Duty of Confidentiality

- The CCG will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

2.4.3. In respect of Information Security:

- The CCG will establish and maintain policies for the effective and secure management of its information assets and resources;

- The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements;

- The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training;

- The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

2.4.4. In respect of Information Quality Assurance:

- The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records;

- The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements;

- Managers are expected to take ownership of, and seek to improve, the quality of information within their services;

- Wherever possible, information quality should be assured at the point of collection;

- Data standards will be set through clear and consistent definition of data items, in accordance with national standards;

- The CCG will promote information quality and effective records management through policies, procedures/user manuals and training.

2.5. In respect of Information Risk management:

- The CCG will appoint a Senior Information Risk Owner (SIRO) with responsibility to the Governing Body for reporting information risks. The Chief Transformation Officer for the CCG has been appointed to this role;

- The CCG will ensure that asset owners are established for all information assets. Asset owners will be at a senior level, and will understand how to assess and address risks associated with their assets;

- The assets owners will undertake annual online training. Their assets register will be updated annually and they will produce an annual information asset report for the SIRO;

- The CCG will apply the Information Risk Policy and its Risk Management Policies and procedures in accessing and addressing information risks.

2.6. In respect of Management of third parties:

- The CCG will ensure that contracts and protocols with partners and suppliers where necessary include suitable statements relating to Information Governance;

- The CCG will, where necessary, require that Agency workers, Volunteers and contractors are adequately trained in Information Governance prior to their gaining access to the CCG information;

- The CCG will establish a procedure and updated register of all third parties with whom Personal Confidential Data (PCD) has been shared eg: via databases. There will also be a data sharing agreement signed by all relevant parties for each instance of data sharing.

3. Scope

3.1. This policy applies to all CCG staff which for the purposes of this policy includes but is not limited to governing body members, contractors, agency and temporary staff, student, honorary and volunteer staff.

4. Responsibilities

4.1. **Governing Body** - It is the role of the CCG Governing Body to define the CCG's policy in respect of Information Governance, 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.

4.2. **Accountable Officer** - The Accountable Officer has ultimate responsibility for the legal, secure, effective and efficient processing of information.

4.3. **Caldicott Guardian** - The Caldicott Guardian will be the senior responsible person for providing advice on the lawful and ethical processing of the personal information of patients or service users and will ensure appropriate sharing/disclosure of information.

The Caldicott Guardian will be responsible for granting permission to access or disclose personal information.

4.4. **Data Protection Officer (DPO)** - The DPO is a natural, identifiable person that informs and advises the CCG and its data processors, monitors their compliance, and is a primary contact for data subjects and the Information Commissioner's Office (ICO). The DPO works with staff in Information Governance. CCG staff consult the DPO in when, for example, conducting a Data Protection Impact Assessment (DPIA) and when serious personal data breaches need to be reported to the ICO.

4.5. **Commissioning Support Unit Information Governance Consultant -** The Commissioning Support Unit Information Governance Consultant is responsible for overseeing day to day Information Governance issues or risks relating to this policy reporting into the Information Governance Steering group; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the CCG and raising awareness of Information Governance.

4.6. **Senior Information Risk Owner (SIRO)** - The SIRO is responsible for overseeing the development of an Information Risk Policy and a strategy for implementing the policy within the existing Information Governance framework. Ensuring the Governing Body is adequately briefed on Information Governance risk issues.

4.7. **Information Asset Owners/Administrators** - Information Asset Owners (IAOs) are accountable to the SIRO and will provide assurance that information risk is being identified and managed effectively for those information assets that they have been assigned ownership of. Information Asset Administrators (IAAs) will usually be staff who have day-to-day responsibility for management of information risks affecting one or more assets, and report these to the IAOs.

4.8. **Managers** - Managers within the CCG are responsible for ensuring that the Policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

4.9. **All Staff** - All staff, whether permanent, temporary or contracted, and all third party contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Staff must ensure where a breach of this policy has taken place it is reported to the line manager so that the CCG's Incident reporting process can be invoked.

4.10. **The Information Governance Steering Group (IGSG)** – The IGSR will be accountable to the Clinical Quality and Governance Committee. The group will support and drive the information governance agenda providing the Governing Body with assurance that effective information governance procedures, policies and best practice are implemented within the CCG.

The group will identify leads for the various standards of the NHS Digital Data Security and Protection Toolkit. These leads will be responsible for maintenance and improvement of their assigned initiatives.

Improvement Plan and Assessment: An assessment of compliance within the Data Security and Protection Toolkit will be undertaken each year by the Commissioning Support Unit.

5. Legislation and the NHS

5.1. Recent legislation is having a significant effect on Information Governance in NHS organisations. The CCG must ensure that all policies and procedures are fully compliant with legislation and NHS guidance on the management of information, including:

- Public Records Act 1958 and 1967;
- Access to Health Records Act 1990;
- General Data Protection Regulations 2016;
- Data Protection Act 2018;
- Freedom of Information Act 2000;
- HSC 1999/053: For the Record: Managing Records in NHS Trusts and Health Authorities;
- Records Management Code of Practice for Health and Social Care (Information Governance Alliance 2016);
- HSC 1999/012: Caldicott Guardians;
- Caldicott 2;
- NHS Litigation Authority Risk Management Standards;
- NHS Digital Data Security and Protection Toolkit;ISO 27001 Information Security Management.

6. Equality and Diversity Impact Assessment

6.1. In reviewing this policy, the CCG considered, as a minimum, the following questions:

- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so, is this planned?

6.2. Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy, race, religion or belief, sex, sexual orientation. No adverse impacts have been identified.

7. Monitoring Compliance and Effectiveness of the Policy

7.1. The Clinical Quality and Governance Committee will oversee implementation of the Policy.

7.2. The policy will be reviewed every three years by the Governing Body or earlier if appropriate, to take into account any relevant changes in legislation or guidance, organisational change or any other exceptional circumstance

7.3. An action plan will be developed against the NHS Digital Data Security and Protection to identify key areas for continuous improvement.

8. References and Further Reading

8.1. This policy should be read in conjunction with the following:

- Confidentiality and Data Protection Policy;
- Information Security Policy;
- Internet Usage Policy;
- Email Usage Policy;
- Records Management Policy;
- Safeguarding Children and Vulnerable Adults/Adults at Risk Policy;
- Incident Reporting Policy;
- Information Risk Policy;
- Serious Incident Reporting Policy and Management Policy and Procedure;
- Data Encryption Policy;
- Remote Working Policy;
- Subject Access Request Procedure.

Blank Page

End of Policy