NHS
Somerset
Clinical Commissioning Group

INFORMATION GOVERNANCE POLICY

Version:	1.0
Ratified by:	Information Governance, Records Management and Caldicott Committee
Date Ratified:	16 October 2018
Name of Originator/Author:	Information Governance Services
Name of Responsible Committee/Individual:	Kevin Caldwell, Information Governance and Data Protection Manager
Date issued:	16 October 2018
Review date:	16 October 2021
Target audience:	All Somerset CCG staff, including contractors and temporary staff

INFORMATION GOVERNANCE POLICY

CONTENTS

Section		Page
	VERSION CONTROL	i
1	INTRODUCTION	1
2	PURPOSE	1
3	LEGAL COMPLIANCE	2
4	SCOPE AND DEFINITIONS	2
5	PROCESSES/REQUIREMENTS	4
6	INFORMATION SECURITY	4
7	INFORMATION QUALITY ASSURANCE	4
8	COMMISSIONING OF NEW SERVICES	5
9	ROLES AND RESPONSIBILITIES	5
10	TRAINING	6
11	PUBLIC SECTOR EQUALITY DUTY – EQUALITY IMPACT ASSESSMENT	6
12	MONITORING COMPLIANCE AND EFFECTIVENESS	7
13	REVIEW	7
14	ADDITIONAL REFERENCES AND ASSOCIATED CODES OF PRACTICE	7

INFORMATION GOVERNANCE POLICY

VERSION CONTROL

Document Status:	Final
Version:	1.0

DOCUMENT CHANGE HISTORY		
Version	**Date**	**Comments**
1.0	16 Oct 2018	New Document

Equality Impact Assessment (EIA) Form OR EIA Screening Form completed. Date:	05/10/2018

Sponsoring Director:	David Freeman, Chief Officer
Author(s):	Kevin Caldwell, Information Governance and Data Protection Manager
Document Reference:	Information Governance Policy

INFORMATION GOVERNANCE POLICY

1 INTRODUCTION

The role of the Somerset Clinical Commissioning Group is to support the commissioning of healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will uphold the NHS Constitution. This policy is important because it will help the people who work for the CCG to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

2 PURPOSE

2.1 Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources and performance management. 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.

2.2 Information Governance looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and confidential information. Without access to information it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- Information Governance Management
- Confidentiality and Data Protection Legislation assurance
- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

2.3 The aims of this document are to maximise the value of organisational assets by ensuring that information is:

- Held securely and confidentially;
- Obtained fairly and efficiently;
- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared appropriately and lawfully

2.4 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the CCG will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured

- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff

3 LEGAL COMPLIANCE

3.1 The CCG regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

3.2 The CCG will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

3.3 In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

3.4 The CCG, when acting as a Controller, will identify and record a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ' processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller', the CCG will identify the official authority (legal basis) and record this on relevant records of processing.

4 SCOPE AND DEFINITIONS

4.1 The scope of this document covers

- All permanent employees of the CCG and;
- Staff working on behalf of the CCG (this includes contractors, temporary staff, and secondees).

4.2 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 information. The CCG also recognises the need to share information in a controlled manner. 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 managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

4.3 In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating 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 a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

5 PROCESSES/REQUIREMENTS

5.1 The CCG will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

5.2 Non-confidential information about the CCG and its services will be available to the public through a variety of media.

5.3 The CCG will maintain policies to ensure compliance with the Freedom of Information Act. Please refer to the Freedom of Information Policy.

5.4 The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

5.5 The CCG will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to the CCG Subject Access Policy in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

5.6 The CCG will maintain policies to ensure compliance with the Records Management Code of Practice for Health and Social Care (2016). Please refer to the CCG Records Management Policy.

6 INFORMATION SECURITY

6.1 The CCG will maintain policies for the effective and secure management of its information assets and resources.

6.2 The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training. Please refer to the CCG Information Security, Remote Working and Portable Devices and Network Security policies.

6.3 The CCG will adhere to the NHS Guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the organisation becomes aware of the incident. Please refer to the CCG incident reporting policy.

7 INFORMATION QUALITY ASSURANCE

7.1 The CCG Senior Leadership Team will maintain policies and procedures for information quality assurance and the effective management of records. Please see the Records Management Policy.

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

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

7.4 Wherever possible, information quality should be assured at the point of collection.

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

8 COMMISSIONING OF NEW SERVICES

8.1 The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the CCG SIRO and the Information Asset Owner's.

8.2 All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA and where required, seek review from the SCW IG Data Protection Impact Assessment Panel prior to approval or further work.

8.3 The CCG will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

9 ROLES AND RESPONSIBILITIES

9.1 The CCG has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. The CCG Senior Leadership Team is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

9.1.1 The Hierarchical Management Structure and associated roles is detailed in the Information Governance Framework Document.

Senior Leadership Team

9.2 It is the role of Senior Leadership Team to define agree ne policy in respect of Information Governance, taking into account legislative and NHS requirements. The Senior Leadership Team is also responsible for

ensuring that sufficient resources are provided to support the requirements of the policy.

Clinical Executive Committee

9.3 The annual audit of information governance shall be reported to the Clinical Executive Committee together with any recommendations identified and the associated improvement plans.

Information Governance, Records Management and Caldicott Committee

9.4 The Information Governance, Records Management and Caldicott Committee is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in the CCG and raising awareness of Information Governance.

Service Leads

9.5 Service Leads 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. Part of this obligation is to ensure that all staff are trained and made aware of confidentiality requirements and procedures. Data Custodians are responsible for carrying out annual audits and to implement local remedial actions in response to audit findings.

All Staff

9.6 All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy.

10 TRAINING

10.1 The CCG will ensure that all staff receives annual Information Governance training appropriate to their role through ConsultOD. New starters and any temporary, contract or agency staff must also complete the Information Governance Training when beginning their employment and annually thereafter.

11 PUBLIC SECTOR EQUALITY DUTY – EQUALITY IMPACT ASSESSMENT

11.1 An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found.

12 MONITORING COMPLIANCE AND EFFECTIVENESS

12.1 This policy will be monitored by the SCW Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.

12.2 The CCG IG action plan, along with regular progress reports will be monitored by, the IGRMCC.

12.3 Compliance with the Data Security and Protection Toolkit will be assessed by NHS Digital including a review of evidence, as part of the CCG performance assessment.

12.4 The CCG will ensure that information governance is part of its annual cycle of internal audit. The results of audits will be reported to IGRMCC along with relevant action plans which they will monitor. Reports will also be provided to the CEG.

12.5 Compliance with the CCG policies is stipulated in staff contracts of employment. If staff members are **unable** to follow the CCG policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with the CCG policies or failure to report non-compliance may be treated as a disciplinary offence.

13 REVIEW

This policy will be reviewed annually by the SCW IG team, or if required by law.

14 ADDITIONAL REFERENCES AND ASSOCIATED CODES OF PRACTICE

- NHS Digital Codes of Practice
  https://digital.nhs.uk/codes-of-practice-handling-information/confidential-information

- Department of Health Code of Practice
  https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

- CQC Code of Practice
  http://www.cqc.org.uk/sites/default/files/20160906%20Code%20of%20practice%20on%20CPI%202016%20FINAL.pdf

- Health and Social Care (Safety and Quality) Act 2015 http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted
- NHS England Policy https://www.england.nhs.uk/publication/confidentiality-policy/

- All THE CCG Policies, procedures and guidance relating to the management and processing of information within the organisation