NHS
Gloucestershire
Clinical Commissioning Group

OFFICIAL

Gloucestershire CCG

Data Security and Protection Policy

Version 2.0

DOCUMENT CONTROL

Document Name	Version	Status	Author
Data Security and Protection Policy	2.0	Final	SCW Information Governance Services
Document origin	This policy has been produced as a template Information Governance Policy by SCW as part of the service provided to Gloucestershire CCG. The CCG has adopted the template policy with appropriate CCG specific changes, including changing the name to Data Security and Protection Policy.		
Document objectives:	This policy supports CCG staff in compliance with Data Protection legislation, achieving best practice in the area of Data Security and Protection and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience:	All staff		
Committee/Group Consulted*:*	SCW Information Governance Steering Group		
Monitoring arrangements and indicators:	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.		
Training/resource implications:	All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet policy pages		
Approved and ratified by SCW:	SCW Information Governance Steering Group		Date: 07-06-18
	SCW Corporate Governance and Assurance Group		Date: 25-06-18
Approved and ratified by GCCG:	GCCG Data Security and Assurance Working Group		Date: 08-08-18
	GCCG IGQC		Date:
Equality Impact Assessment:	Yes		Date: 07-06-18
Date issued:			
Review date:	April 2020		
Author:	SCW Information Governance Team		
Lead Director:	SCW Head of Information Governance		

Contents

1. INTRODUCTION

The role of Gloucestershire CCG 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

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.

Data Security and Protection governs how 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:

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

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

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 mandatory for all staff

3. LEGAL COMPLIANCE

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

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.

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.

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

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).

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 confidentiality 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.

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

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).

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

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

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

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

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

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.

The CCG will adhere to the NHS Guidance for reporting, managing and investigating Data Security and Protection 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 IG SIRI Policy.

7. INFORMATION QUALITY ASSURANCE

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

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.

8. COMMISSIONING OF NEW SERVICES

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 Owners.

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.

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

9. ROLES AND RESPONSIBILITIES

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 is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Hierarchical Management Structure and associated roles is detailed in the Data Security and Protection Framework Document.

Governing Body

The Governing body is responsible for defining the CCG's Data Security and Protection Policy. The Governing Body is also responsible for providing sufficient resources for the implementation of policy requirements.

Integrated Governance and Quality Committee (IGQC)

The IGQC is responsible for the effective management, assurance and monitoring of the Data Security and Protection Agenda across the organisation.

Data Security & Assurance Working Group

The Data Security & Assurance Working Group will:-

- oversee day to day Data Security and Protection issues
- ensure development and maintenance of policies, standards, procedures and guidance
- promote Data Security and Protection best practice across the CCG

Accountable Officer (AO)

The AO of the CCG is responsible for the implementation of Data Security and Protection arrangements within the CCG. The AO will provide assurance that all information risks have been appropriately managed through the Statement of Internal Control.

Senior Information Risk Owner (SIRO)

The SIRO will:-

- act as an advocate for information risk on the Governing Body and in internal discussions, and will provide written advice to the AO on the content of the Annual Statement of Internal Controls (SIC)
- ensure that identified information security threats are investigated and incidents managed
- provide updates on information risk to the Governing Body and the AO

The role will be supported by the SCWCSU IG Team, the CCG Caldicott Guardian and a network of IAOs and IAAs, although ownership of the information risk assessment process will remain with the SIRO.

Information Asset Owners (IAOs)

IAOs will:-

- ensure that information assets are risk assessed and risk treatment plans are provided to the SIRO on a quarterly basis
- risk assess proposed new assets prior to acceptance and provide risk assessment reports to the SIRO

Information Asset Administrators (IAAs)

IAAs will support the IAO in the day to day management of records. IAAs are normally specially assigned individuals responsible for identifying risks to the information assets and ensuring policies and procedures are followed

Caldicott Guardian

The Caldicott Guardian will:-

- guide the CCG on matters of patient confidentiality
- act as the "conscience" of the organisation particularly in respect of the sharing and use of patient confidential information
- ensure that staff comply with the Caldicott Principles and the NHS Confidentiality Code of Practice
- advise the Governing Body on progress and major issues that may arise

10. TRAINING

All staff whether permanent, temporary or contracted are required to comply with the CCG Data Security and Protection Staff Handbook which stresses the importance of appropriate information handling and incorporates legislation, the common law and best practice requirements. Data Security and Protection is the framework drawing these requirements together therefore it is important that staff receive the appropriate training. On joining the organisation, CCG staff will receive a copy of the Data Security and Protection staff handbook and will be required to sign and return a receipt.

The CCG will ensure that all staff receive annual Data Security and Protection training appropriate to their role through the online E-Learning for Health training tool or face to face training delivered by the SCW Data Security and Protection Team. Managers are responsible for monitoring staff compliance. New starters and any temporary, contract or agency staff must also complete the Data Security and Protection Training when beginning their employment and annually thereafter.

11. PUBLIC SECTOR EQUALITY DUTY- EQUALITY IMPACT ASSESSMENT

An Equality Impact Analysis (EIA) has been completed. No adverse impact or other significant issues were found. A copy of the EIA is attached at Appendix A.

12. MONITORING COMPLIANCE AND EFFECTIVENESS

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.

The CCG Data Security and Protection action plan and regular progress reports will be monitored by the Data Security & Assurance Working Group.

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.

The CCG will ensure that Data Security and Protection is part of its annual cycle of internal audit. The results of audits will be reported to the Data Security & Assurance Working Group along with relevant action plans which they will monitor. Reports will also be provided to the Integrated Governance and Quality Committee.

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. Where non-compliance relates to partner organisations and third party organisations, this will be handled in accordance with contractual agreements and data sharing agreements.

13. REVIEW

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