NHS
Buckinghamshire
Clinical Commissioning Group

Information Governance Policy Version 2.1

Buckinghamshire CCG

DOCUMENT CONTROL

Document Name	Version	Status	Author
Information Governance Policy	2.1	GDPR Update	SCW Information Governance Services

Document objectives:	This policy supports BCCG staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance 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 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 IG team pages	
Approved and ratified by:	Buckinghamshire CCG IG Steering Group BCCG Audit Committee	Date: March 2019 Date: 27.03.19
Equality Impact Assessment:	Yes	Date: 13.03.18
Date issued:	January 2019	
Review date:	**January 2021**	
Author:	SCW Information Governance Team	
Lead Director:	Head of Information Governance	

Change Record

Date	Author	Version	Page	Reason for Change
13.03.18	SCW CSU Information Governance	V2.0 Draft Legislative update	Throughout document	Draft amendments in line with GDPR and the Data Protection Act 2018
March 2019	Russell Carpenter/ Paul Antony	V2.1	Consent (section 9)	Inserted following recommendations from IG Audit Edits to reflect local arrangements

			Throughout	

Contents

1. INTRODUCTION

The role of Buckinghamshire Clinical Commissioning Group is to commission 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.

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

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 available to 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, those with honorary contracts 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 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.

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 BCCG 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 policies to ensure compliance with the Freedom of Information Act. Please refer to the Freedom of Information Policy.

The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media. Please refer to the Communications Strategy**.**

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 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 IG SIRI Policy.

7. INFORMATION QUALITY ASSURANCE

The CCG Audit Committee 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 Owner's.

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. CONSENT

In some circumstances the CCG may require explicit or implied consent to legitimise certain forms of data processing. This may relate to the common law duty of confidentiality where the request for consent relates to direct patient care, or to the General Data Protection Regulation (GDPR) where the request for consent does not relate to direct patient care.

The table below indicates common scenarios where a distinction would likely apply.

Distinction between common law duty of confidentiality and GDPR in requesting implied or explicit consent

CCG requests consent under common law duty of confidentiality ***Note: As each of the requests below relate to direct patient care, this means that no other legal basis is required and therefore no further evidence required for compliance with GDPR.***	**CCG requests consent under the General Data Protection Regulation (GDPR)**
Continuing Healthcare – to request explicit	Model Release – to request consent for use

consent in order to complete the assessment for NHS Continuing Healthcare (NHS CHC) with personal information gathered, collated and shared where appropriate with relevant parties as part of the assessment and on-going review process.	of photographs of patients and/or the public in corporate publications
Individual Funding Requests – to request implied consent through a primary care clinician for referral for a procedure not otherwise routinely funded by the NHS. This specifies that personal and clinical information will be provided to the IFR service via all means, including electronic and automated approvals, to enable full consideration of the funding request. Where NHS Buckinghamshire CCG does use automated individual decision-making, it is specifically in relation to matching clinical need against pre-defined criteria.	
Individual Rights/Right of Access (Subject Access Request) – by the very nature of a SAR the data subject is requesting their information related to direct care, with consent therefore implied. If the requester is acting for a third party, proof is also requested.	
Complaints – to request explicit consent in order to manage a case with any appropriate organisation for the purposes of investigating the complaint. This is deemed to fall under common law duty of confidentiality on the basis that a compliant is highly likely to relate to direct care a patient has or has not received.	

Managing consent under GDPR

Where data processing is legitimised under GDPR, CCG staff must adhere to a number of subsequent specific requirements, including but not limited to:

- How to consider whether consent is the most appropriate lawful basis for processing;

- How a consent request should be written;
- What information a consent request should include;
- What methods can be used to indicate consent;
- How should consent be recorded;
- How consent should be managed; and
- How to manage the right to withdraw consent.

CCG staff members are signposted to separate guidance published by the Information Commissioners Office (ICO) for this purpose: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/

When may consent not be necessary?

CCG staff members are asked to declare their conflicts of interest which are published on registers on the CCG website. However, this process does not require consent to publish as declaration is a legal requirement under Section 14O of the National Health Service Act 2006 (as amended by the Health and Social Care Act 2012). As consent is not required, it cannot subsequently be withdrawn. CCG Staff members may give valid reasons of sensitivity for certain data to be withheld from publication. This means that no other legal basis is required and therefore no further evidence required for compliance with GDPR.

The CCG Fair Processing Notice further describes how patient and staff data is processed in relation to compliance with the General Data Protection Regulation (GDPR).

https://www.buckinghamshireccg.nhs.uk/public/about-us/publishing-information/fair-processing-notice/

10. 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 Audit Committee 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 Information Governance Framework Document.

Buckinghamshire Clinical Commissioning Group Audit Committee

It is the role of the Audit Committee to define the CCG policy in respect of Information Governance, taking into account legislative and NHS requirements. The Audit Committee is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Buckinghamshire Clinical Commissioning Group Information Governance Steering Group
The CCG Information Governance Steering Group 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.

Buckinghamshire Clinical Commissioning Group Head of Department
The heads of various departments / functions within the CCG (Heads of, Associate Directors and Deputies) 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.

Buckinghamshire Clinical Commissioning Group Staff
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.

11. TRAINING

All staff whether permanent, temporary or contracted are required to comply with the CCG IG Staff Handbook which stresses the importance of appropriate information handling and incorporates legislation, the common law and best practice requirements. Information Governance 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 Information Governance staff handbook and will be required to sign and return a receipt to the Data Protection Officer.

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

12. 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.

13. MONITORING COMPLIANCE AND EFFECTIVENESS

This policy will be monitored by the CCG Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated. The CCG IG action plan, along with regular progress reports will be monitored by, the CCG Information Governance Steering Group and Audit Committee. 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 information governance is part of its annual cycle of internal audit. The results of audits will be reported to the CCG Information Governance Steering Group along with relevant action plans which they will monitor. Reports will also be provided to the Audit 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

14. REVIEW

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

15. 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

APPENDIX A: EQUALITY IMPACT ANALYSIS

Equality Impact Analysis on the

Information Governance Policy

1 What is it about? *Refer to the Equality Act 2010*

a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve

The Information Governance Policy details how the CCG will meet its legal obligations and NHS requirements concerning the management of information and the governance arrangements in place to support this.

b) Who is it for?

All staff

c) How will the proposal/policy meet the equality duties?

The policy will have no adverse effect on equality duties as it considers the management of information to be of equal status across all groups of people.

d) What are the barriers to meeting this potential?

There are no barriers.

2 Who is using it? *Consider all equality groups*

a) Describe the current/proposed beneficiaries and include an equality profile if possible

The policy is applicable to all.

b) How have you/can you involve your patients/service users in developing the proposal/policy?

Patients and service users have not been involved in developing the policy as this is an operational policy.

c) Who is missing? Do you need to fill any gaps in your data?

There are no gaps.

3 Impact *Consider how it affects different dimensions of equality and equality groups*

Using the information from steps 1 & 2 above:

a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is?

It is not anticipated that any adverse impact will be created.

b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or

justified? This is not applicable.
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? Can you maximise the benefits for other disadvantaged groups? This policy is equal across all groups.
d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Angela Sumner** **angelasumner@nhs.net**	Date completed: **08-06-18** Proposed EIA review date: **01-04-19**
Signature of director/decision-maker **Add signature** Name of director/decision-maker **Insert Name and Position**	Date signed **Insert date**