NCL Clinical Commissioning Groups
Information Governance Policy

Version 0.07

Document revision history

Date	Version	Revision	Comment	Author/Editor
19/09/2018	0.2	Review		Head of IG
27/09/2018	0.3	Review		SME Manager
10/10/2018	0.4	Review		Compliance Manager
07/11/2019	0.5	Review		Compliance Manager
09/01/2020	0.6	Review		Compliance Manager
10/01/2020	0.07	Review	Short review pending acceptance of tracked changes	NLP IG Lead
22/01/2020	0.8	Review		IG SME Manager

Document approval

Date	Version	Revision	Role of approver	Approver

Contents

1. INTRODUCTION 4
2. SCOPE 5
3. PURPOSE 6
3.1 OBJECTIVES 6
4. THE USE OF INFORMATION 7
4.1 USE OF PERSONAL DATA 7
4.2 USE OF INFORMATION TO IMPROVE PERFORMANCE 8
5. DATA QUALITY 8
6. DISCLOSURE AND SHARING INFORMATION 9
7. PUBLIC RIGHTS OF DISCLOSURE 9
8. TRANSFERRING OF INFORMATION 10
9. SAFE HAVENS 11
10. INFORMATION SECURITY 11
11. MONITORING AND COMPLIANCE 12
11.1 NON-COMPLIANCE 12
12. REVIEW 12
13. IMPLEMENTATION AND DISSEMINATION 12

1. Introduction

This policy relates to Barnet, Enfield, Camden, Islington and Haringey Clinical Commissioning Groups, hereafter they will be referred to as 'North Central London Clinical Commissioning Groups (NCL CCGs)'.

The role of each of the CCGs is to commission healthcare, so that valuable public resources secure the best possible outcomes for patients. In doing so, they will seek to meet the objectives prescribed in the Mandate and to uphold the NHS Constitution. This policy is important because it will help the people who work for the CCGs to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

This policy sets out the intentions of each of CCGs to manage the information governance agenda within its remit, to the standards required by law and regulation. Specifically, data protection legislation (the UK Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation). In doing so, it supports high-quality commissioning and healthcare, through accurate, accessible and appropriately governed information.

This document refers to information to encompass the terms information, data and records. The Cabinet Office defines data as *'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation'* and information as '*output of some process that summarises interprets or otherwise represents data to convey meaning'.* This definition will be used throughout this document.

The CCGs use information to support the commissioning and management of healthcare services for patients. Information is also used in the administration of the NHS. In addition to these functions are the statutory duties of NHS England and NHS Digital which form the wider governance structure within which the CCGs operate.

The NHS and the administration of the NHS are dependent on the appropriate use of personal data, and the management of secondary uses of this data and business sensitive data.

The aims of this policy are;

- To maximise the value of organisational assets by ensuring that data is:
    - Held securely and confidentially;
    - Obtained fairly and lawfully;
    - Recorded accurately and reliably;
    - Used effectively and ethically; and
    - Shared and disclosed appropriately and lawfully.
- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental.

  Each of the CCGs will ensure:

    - 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; and
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Governance Compliance Manager.

Each of the CCGs recognise that effective information management is fundamental to proper administration and operational effectiveness and that these are enablers to the achievement of our strategic goals. These are:

- Further integration of health and social care (where appropriate);
- Delivering improved health outcomes and reducing health inequalities;
- Improving service quality and patient safety;
- Delivering sustainable finances;
- Ensuring robust governance;
- Organisational competence; and
- Underpinning our business with patient and public engagement.

This policy is part of the collection related to information governance which set out the expected standards and controls around the use of information. The policies are:

- Information Governance;
- Information Quality;
- Non-clinical incident and Near-Miss Reporting Policy and Procedure;
- Information Management; and
- Information Security.

The concepts and standards within these policies are interrelated. Obligations and intentions are considered across the suite of policies. The policies sit under an overarching Information Governance Framework which sets out roles and responsibilities and information governance related work plans.

2. Scope

This policy applies to:

- All information and data held and processed by each of the CCGs must be managed and held within a controlled environment. These include the personal data of patients and staff, as well as corporate information. Additionally, it applies to information, regardless of format, and includes legacy data held by the organisation;

- All permanent, contract or temporary staff of the CCGs and any third parties who have access to the CCG's premises, systems or information. Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual or voluntary basis;

- Information systems, data sets, computer systems, networks, software and information created, held or processed on these systems, together with printed outputs from these systems; and

- All means of communicating information, both within and outside the CCGs (in both paper and electronic format) including data and voice transmissions, emails, post, fax, voice and video conferencing.

Each of the CCGs believe that its internal management processes will be improved by the greater availability of information that will grow by the recognition of information governance as a designated corporate function.

3. Purpose

Information governance ensures processes, confidentiality and security controls are in place and sets standards of quality and ethical use of personal data. Corporate records must also be managed appropriately and where possible provided to the public under the appropriate legislation (Freedom of Information Act 2000 and Environmental Information Regulations 2004) to ensure transparency and accountability.

Information forms a key component in affirming the NHS intention to ensure effective decision making, inform and, empower patients through the provision of accurate, accessible and coherent information.

Each of the CCGs must manage their statutory and organisational responsibilities. All staff are responsible and contribute towards effective and responsible governance of information in line with the organisation's aims and objectives.

3.1 Objectives

NCL CCG's Governing Bodies are committed to ensuring that all:

- Information that relates to patients and staff is processed, protected and disclosed appropriately to provide improved healthcare and decisions for patients.

- Information related to its functions, activities and decisions must be managed to the appropriate standards, (the right information, in the right format, to the right people at the right time).

Each of the CCGs aims for the management of information and associated risk includes:

- Effective and efficient management of information for the care of service users and the management of the care service;
- Actively advance the management of information to improve the provision of services, information and care of patients;
- Engage with partner organisations and where appropriate and lawful share information to support care and the public interest;
- Discharge its obligations to disclose information in response to lawful requests with due regard to its duties of confidence by following clear and systematic processes;
- Ensure that systems and processes are effective to ensure the confidentiality and security of personal and other sensitive information;
- Ensure that all information and data processed, held and managed is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness;
- Ensure that all information and data is held in a consistent and systematic manner that ensures its accessibility, accuracy and integrity throughout its lifecycle;
- To actively provide information in line with the Freedom of Information Act 2000 and other regulatory or organisation requirements;
- Ensure those working on behalf of the CCGs, are informed, trained and active in the appropriate management of information; and

  To ensure that change is undertaken in a structured and systematic manner that ensures information governance issues are dealt with in a timely, proportionate and appropriate way.

4. The use of Information

All information must be created, used and managed in a professional manner, as described in the Information Management Policy. It must be accessible to the organisation on a long-term basis and must be stored in a systematic and consistent manner.

Access to information systems (such as the email, the internet or network) and records of the organisation are provided to staff for business purposes and remain the property of the relevant CCG. All access to, and use must be appropriate and in line with the discharge of their duties.

As staff create information, they are doing so on behalf of the organisation, for example when sending emails, and are accountable for the information they create, for its appropriateness and accessibility.

4.1 Use of Personal Data

Personal data can relate to information about patients, service users and members of staff that describes an identifiable person. It does not have to include particular demographic information,

such as name and address but can consist of a combination of factors that would make it possible to identify the person. Information provided to the NHS, is done so on the expectation of confidentiality and often in a healthcare setting. If personal data is also subject to a duty of confidentiality, for example because it relates to a patient, we refer to this as personal confidential data. It is important for staff and working practice to account for this and to ensure that any secondary use of personal confidential data, for non-care purposes, is done in accordance with legal and organisational requirements.

Each of the CCGs have a Privacy Notice published on it's website, which details what personal data is held and processed, for what purpose it is used, who it is shared with, and what governs that process. Each service within the organisation must provide a clear Privacy Notice for their area of responsibility.

4.2 Use of Information to improve performance

Each of the CCGs will actively seek opportunities to improve the performance of the NHS across their customer bases by the better use of information and data. This includes:

- Use of anonymised or de-identified patient data to inform better health care decisions for individuals and the community;
- Review of processes and functions within the organisation to ensure efficient and effective data processing; and
- Engagement with partner organisations to identify appropriate information sharing which ensures that the patient and public can exercise choice and are kept informed.

All new projects or services undertaken by each of the CCGs must follow the standard required, as set out by the Change Management Policy, including the completion of a Data Protection Impact Assessment (DPIA) at the start of a project or procurement process. All staff managing change must ensure that they identify any potential information governance requirements when scoping the business case for any change.

5. Data Quality

In order to support effective commissioning and to support efficiency, all systems and standard working practice involved in the processing of information, must ensure the accuracy and quality of information.

Data quality requires:

- Accessibility – information can be accessed quickly and efficiently through the use of systematic and constituent filing.
- Accuracy – information is accurate, with systems that support this work through guidance.
- Completeness – the relevant information required is identified and working practice ensures it is routinely captured.
- Relevance – information is kept relevant to the issues rather than for convenience with appropriate management and structure.

- Timeliness – information is recorded as close to possible to being gathered and can be accessed quickly and efficiently.

6. Disclosure and Sharing Information

As a public body, the constituent parts of each of theCCGs can only share personal confidential data when it is legally permissible.

This includes:

- The common law duty of confidence, which extends after death.
- Data protection legislation.

Any basis of disclosure and sharing needs to be understood and clearly stated before it is undertaken. This decision must demonstrate that the disclosure or sharing is:

- reasonable and done in good faith for a clear intention;
- Lawful and relevant to the purpose intended;
- On the grounds that they are in the public interest.

Data sharing in the NHS is also governed by the Caldicott Principles which supports the legal framework.

Disclosure or sharing of personal confidential data requires one of the following conditions to be met:

- The informed and valid consent of the individual, balanced against any duty of care and consideration of capability to provide that consent;
- Disclosure is in the public interest, which must demonstrate consideration of the balance of public interest against the individual and provision of a confidential service; or
- Disclosure is in accordance with the law.

All routine sharing of information must be supported by a clear statement that can be made available to the public or patients. This fair processing or privacy notice must detail the type of information being shared, who is it is being shared with and to what purpose and benefit. In addition, all routine information sharing must be accompanied by a current data sharing agreement or legally binding agreement that sets out the all relevant issues, undertakings and processes for the sharing.

7. Public rights of disclosure

All staff are reminded that there are several pieces of legislation that require information to be released to the public This include the

- Freedom of Information (FOI) Act 2000 and Environmental Information Regulations (EIR) 2004: applies to information in all formats; this includes emails, voice recordings and images.
- EU General Data Protection Regulations 2016 and UK Data Protection Act 2018, both gives the data subject's right to access their data that are held by the organisation.
- Access to Health Records 1990 which permits disclosure of information to those with a claim to the estate of the deceased or lawful right

To meet this responsibility, all staff are responsible for ensuring that the:

- Records are Accessible – ensuring that they can be found within a systematic and consistent filing structure.
- Contents of the records are appropriate and relevant – this includes a professional and appropriate tone.
- Integrity of the records are protected and that the records are complete – so that they can be used in an ongoing basis.
- Confidentiality of the contents of the records are appropriately safeguarded with a clear statement of who has access to the information.
- Records are securely stored and marked with the correct security classification e – systems and staff should ensure that personal identifiable, sensitive, confidential and corporate information is clearly stored and marked as such.

Details of each CCG' policy on active disclosure and compliance with the Freedom of Information Act is outlined in their organisation's Freedom of Information Policy and associated protocols and procedures.

8. Transferring of information

All transfers of information within and outside all the CCGs must be managed, comply with the information security requirements and follow clear process. All teams must have a clear statement of their inward and outward flows of personal data and personal confidential data.

This process must identify:

- The appropriate method, and inherent risks, of the transfer;
- The contact point and details to which the information is routinely transferred. All contact points should identify a team and position, rather than an individual to which the information is being transferred; and
- How the transfer is confirmed and completed.

In addition, where the transfer of information involves personal or identifiable data:

- The purpose and justification for transferring the information; and
- Security standards of the method of transfer.

It is expected that most transfers of information will be routine and follow an identified process.

The transfers of information within the CCG and between external organisations must be managed in an appropriate manner and by secure methods with any risks identified and managed.

9. Safe Havens

- In order to support the appropriate transferring of personal confidential data, the organisation will identify appropriate safe haven locations. Safe havens answer the requirements of the Data Protection Legislation and The NHS Code of Practice: Confidentiality and the NHS Care Record Guarantee. Safe havens have arrangements and procedures in place to ensure personal identifiable or sensitive information can be held, received and communicated securely.

- Where safe haven locations are not available to staff the relevant safe haven procedure for the method of transmission should be applied, safe haven locations and procedures will be posted on the intranet.

- The CCG does not support the use of physical fax machines and has an appropriate electronic solution in place where a fax is required to be sent. Staff must make every effort to encourage those they communicate with to use secure email and/or software with secure and controlled access to communicate sensitive information.

10. Information Security

The purpose of information security is to ensure business continuity in order to minimise the impact of security-related incidents and to ensure the integrity of the information and data processed by the NCL CCGs, as described in the Information Security Policy.

Information security enables information to be processed and shared with appropriate safeguards in place. It ensures the protection of information and assets as well as identifying and acting on threats to security.

Information security is both the technical and physical. It ranges from the security of networks, to the use of appropriate passwords by staff and storage of confidential information in secure environments.

All staff contribute towards the security of information and Information Asset Owners are required to have a clear statement on the information security and risks in place for the assets within their remit.

Information security has three basic components:

- Confidentiality: assuring that sensitive information or data is accessible to only authorised individuals and is not disclosed to unauthorised individuals or the public.

- Integrity: safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.

- Availability: ensuring that information, systems, networks and applications as well as paper records are available when required to departments, groups or users that have a valid reason and authority to access them.

- Accountability – Users are held responsible for their use of information.

Further information is detailed in each CCG' Information Security Policy.

11. Monitoring and compliance

This framework and the associated controls: policies, protocols and procedures - will be monitored through the risk management system for the CCGs. The information governance risk register will be reviewed:

- on a regular basis at each CCG's Information Governance Group and
- in response to any information incident or enforcement action by the Information Commissioner's Office.

Information risk management is one of the key components of wider assurance and control in setting the priorities for the information governance work plan.

NCL CCGs Information Asset Owners, assisted by Information Asset Administrators, will be required to routinely review the risks and information with the information assets utilised to fulfil the business functions and activities within their remit.

11.1 Non-Compliance

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance and as such are responsible for as individuals. Failure to maintain these standards can result in criminal proceedings against an individual.

12. Review

Review will take place every three years or earlier until rescinded or superseded, due to legal or national policy changes.

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available in the policy register for the organisation. All staff are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

13. Implementation and dissemination

The updated policy, once approved by the CCG's Information Governance Group and Audit Committee in Common, will be shared with all staff through an emailed and physical staff briefing (to support this dissemination) and updated on the intranet.

Awareness of the policy will be checked through a staff survey and spot checks on at least an annual basis.For further information please contact your CCG Information Governance Lead.