IG01b – Information Governance Policy

Corby and Nene Clinical Commissioning Groups

Version 4

Document revision history

Date	Version	Revision	Comment	Author/Editor
24/04/2018	3.1	Review	GDPR update	Senior Internal and Assurance Information Governance Manager
17/05/2018	3.1a	Prior to CCG review and adoption	Edited for use by Corby CCG Need to check roles (section 6), managed risks (section 9), clarify email address for CCG staff to report IG disclosures (section 13.2)	John Geaney, IG Compliance Manager
18/05/2018	3.1b	CCG review	Edited to cover both Nene and Corby CCGs and minor revisions	Information Manager

Document approval

Date	Version	Revision	Role of approver	Approver
July 2018	4.0	Final		Corby and Nene Audit and Risk Committees

Contents

1.0 Introduction

This policy sets out the intentions of Corby and Nene CCGs to manage the information governance agenda within its remit to the standards required by law and regulation. Specifically, Data Protection legislation (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, 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 commissioning of healthcare for patients for Clinical Commissioning Groups. Information is also used to support 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 that the CCGs operate within.

The NHS and the administration of the NHS is dependent on the appropriate use of Personal Data; the management of secondary use of this data and business sensitive data.

The CCGs recognise that effective information management is fundamental to good administration and operational effectiveness, and is an enabler to the achievement of our strategic values:

- Effective, Compassionate, Supportive & Safe

This policy is part of the suite related to Information Governance which set out the expected standards and controls around its use. They are: Information Governance, Information Quality, Information Management and Information Security. The concepts and standards are interrelated. It is important to consider all of our obligations and intentions across the suite of policies.

2.0 Scope

This policy is applicable to:

- All information and data held and processed by the CCGs must be managed and held within a controlled environment, including personal data of patients and staff, as well as corporate information. It applies to information, regardless of format, and legacy data held by the organisation.
- All permanent, contract or temporary staff of the CCGs and all third parties who have access to Corby CCG and Nene CCG 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 output from these systems, and

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

- Although this policy relates to patient/service user data and information, the principles included are applicable to any other data/information staff may encounter e.g. recording of minutes, etc.

The CCG also believe that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of information governance as a designated corporate function.

3.0 Purpose

Information Governance ensures processes, confidentiality and security are in place to ensure appropriate standards of quality and ethical use of personal data. Corporate records must also be managed appropriately and where possible provided to the public to ensure transparency and accountability.

Information is transferred to other organisations and the suppliers of services to support these functions and disclosed in accordance with statutory, regulatory or organisational requirements.

Information forms a key component of the Government's Information Revolution for the NHS. This restates the NHS intention to ensure effective decision making, inform and empower patients through the provision of accurate, accessible and coherent information.

The CCG 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.

This policy provides an overview of how information will be governed and used in the CCG and how the organisation will discharge it duties. This requires a systematic approach based on procedures owned, understood and supported by all those working on its behalf.

3.1 Objectives

The CCG Management Team is 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.

This policy sets out the CCGs aims for the management of information and associated risk. This 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 Corby CCG and Nene CCG, supporting 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.

4.0 Equality Analysis

This document demonstrates the organisation's commitment to create a positive culture of respect for all individuals, including staff, patients, their families and carers as well as community partners. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to use the Human Rights Act 1998 and to promote positive practice and value the diversity of all individuals and communities.

5.0 Definitions

All terms used in this policy are defined at the point of their use.

6.0 Responsibilities

Accountable Officer

The Accountable Officer has overall accountability for information governance. As the Accountable Officer they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

Data Protection Officer

The Data Protection Officer (DPO) the DPO reports to the SIRO. This ensures the DPO can act independently, without a conflict of interest and report direct to the highest management level. In

addition, depending upon the agreement with NEL, the DPO may deputise for the SIRO and Caldicott Guardian.

The Data Protection Officer is responsible for ensuring that the CCGs and their constituent business areas remain compliant at all times with data protection, privacy & electronic communications regulations, freedom of information act and the environmental information regulations (information rights legislation).

The Data Protection Officer shall: lead on the provision of expert advice to the organisation on all matters concerning the information rights law, compliance, best practice and setting and maintaining standards. Provide a central point of contact for the information rights legislation both internally and with external stakeholders (including the office of the information commissioner).

Communicate and promote awareness of information rights legislation across the CCGs.

Information Manager & Information Co-ordinator

The Information Manager has overall responsibility for Information Governance. He/she is responsible for the management of the organisation and for ensuring the implementation of appropriate mechanisms to support service delivery and continuity. Information Governance is key to this as it ensures appropriate, accurate information is available as required.

The Senior Internal and Assurance Information Governance Manager is responsible for the overall development and maintenance of information governance practice throughout the CCG, in particular for drawing up guidance for good management practice and promoting compliance with IG Policies in such a way as to ensure the easy, appropriate and timely retrieval of information.

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is appointed by the Management Team and is accountable to the Accountable Officer for the appropriate management of risk associated with the organisation's use and holding of information.

Caldicott Guardian

The Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

Information Governance Working Group

The Information Governance Working Group reports to the Audit and Risk Committee and is responsible for ensuring that this policy is implemented and that records management systems and processes are developed, co-ordinated and monitored.

Information Governance Service

The Senior Internal and Assurance Information Governance Manager is responsible for the overall development and maintenance of information governance practice throughout the CCG, in particular for drawing up guidance for good management practice and promoting compliance with IG Policies in such a way as to ensure the easy, appropriate and timely retrieval of information.

Information Asset Owners

All system managers (Information Asset Owners) must ensure that procedures are upheld for each personal confidential data system.

The responsibility for local information management is devolved to the relevant Directors, Service Leads and all managers. They have overall responsibility for the management of information and records generated by their activities, i.e. for ensuring that official records controlled within their unit are managed in a way which meets the aims of the Information Management Policy.

Senior managers are responsible for identifying and managing information risks in their remit. Staff nominated as Information Risk Owners (Information Asset Owners) and those responsible for operating Information Assets as Information Risk Administrators (Information Asset Administrators) are accountable to the SIRO for the appropriate identification and management of risks. Information Security risks form a vital part of the role and assurance required from these post holders.

All Staff

All staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the organisation and manage those records in keeping with this policy and with any guidance subsequently produced.

7.0 The use of Information

All information must be used, created 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 Corby CCG and Nene CCG. All access 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.

7.1 Use of Personal Data

Personal data relates to information about patients, service users and members of staff that makes the person identifiable. It does not have to include particular demographic information, such as name and address, and 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. It is important for staff and working practice to account for this and to ensure that any secondary use of personal data, for non-care purposes, is done in accordance with the legal and organisational requirements.

Corby CCG and Nene CCG each have a privacy notice published on their website, which details what personal data is held and processed, for what purpose it is processed and who it is shared with and what governs that process. Each service within the organisation must aim to provide a clear statement for their area of responsibility.

7.2 Use of Information to improve performance

The organisation will actively seek opportunities to improve the performance of the NHS across its customer base 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
- To review processes and functions within the organisation to ensure efficient and effective data processing
- To engage with partner organisations to scope appropriate information sharing which ensures that the patient and public can exercise choice and are kept informed

All change processes must follow the standard required, as set out by the Change Management Policy, including Data Protection Impact Assessments. All staff managing change must ensure that they scope potential information governance when scoping the business case for any change.

8.0 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 encompasses, as described in the Information Quality Policy:

- **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

The approach the CCGs adopt to manage risk and in providing assurance as described within this documentation will be reviewed annually by the CCG Group who will report to the CCG Governing Body upon its findings. An additional review relating to areas of best practice and practical application will be undertaken by the Information Governance team.

9.0 Transferring of information

All transfers of information within and outside the CCGs must be managed, comply with the information security requirements and follow a clear process. All teams must have a clear statement of their inward and outward flows of personal 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
- 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
- Ensure that the security standards of the method of transfer are appropriate

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.

9.1 Safe Havens

In order to support the appropriate transferring of information, 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 person 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 where this is available and on the shared drive.

Neither Corby CCG or Nene CCG supports 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.

10.0 Disclosure and Sharing information

As part of a public body, the constituent parts of Corby CCG and Nene CCG can only share information when it is legally permissible.

This includes:

- The common law duty of confidence, which extends after death
- Health Information is sensitive information and requires justification under article 6 and article 9 of the Data Protection Legislation which requires additional safeguards for its use.

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
- With grounds that 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 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
- 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 Information Sharing contract or legally sound agreement that sets out the all relevant issues, undertakings and processes for the sharing.

10.1 Public rights of disclosure

All staff are reminded that there are several pieces of legislation that require information to be released to the public (the Freedom of Information Act 2000 or Environmental Information Regulations 2004), or the subject of that data (Data Protection Legislation) or those with a claim to the estate of the deceased or lawful right (Access to Health Records 1990).

Access to information legislation applies to information in all formats, this includes emails, voice recordings and images.

In order to meet this responsibility, all staff are responsible for ensuring that the contents of records are:

- **Accessible** – ensuring that they can be found within a systematic and consistent filing structure
- **Appropriate** and **relevant** – this includes a professional and appropriate tone
- Have **Integrity** or completeness – so that they can be used in an ongoing basis
- **Confidential** – appropriately safeguarded to ensure confidentially with a clear statement of who was provided access to the information.
- **Identified** – systems and staff should ensure that person identifiable, sensitive, confidential and corporate information is clearly stored and marked as such.

Active disclosure of information in line with the Freedom of Information Act 2000

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

11.0 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 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 and storage.

All staff contribute to information security and have key responsibilities for its maintenance.

All staff contribute towards the security of information and all 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.

This subject is fully addressed in the CCGs Information Security Policy.

12.0 Training

All staff will be made aware of their responsibilities for information governance through generic and specific training programmes and guidance. Training requirements will be publicised via the Communications Department.

13.0 Monitoring and compliance

This policy and adherence to it will be audited regularly and will be monitored. Compliance with this policy and procedures are undertaken through the Data Security and Protection Toolkit (DSPT) annual self-assessment and an audit undertaken on the level of assurance provided by the submitted evidence.

The table below sets out how we will monitor implementation and utilisation of this Policy.

Table 1: Document Audit and Monitoring Table	
Monitoring requirements **"What in this document do we have to monitor"**	We will ensure that staff are aware of the Policy, the constituent aspects of the information governance strategy, and abide by legal, technical and mandatory IG requirements Performance in the DSPT and the completion of a Data Flow Mapping exercise
Monitoring Method	Quality Assurance criteria (Appendix A) to inform the DSPT annual assessment
Monitoring prepared by	Information Governance Manager
Monitoring presented to	IG Working Group
Frequency of presentation	Annual independent audit, submissions in line with Department of Health Guidance

13.1 Monitoring of compliance

Compliance with all aspects of Information Governance will be undertaken as part of the Information Governance work plan or at the direction of the Corby CCG and Nene CCG IG Working Group, Senior Information Risk Owner or Caldicott Guardian.

13.2 Non-Compliance

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

These include but are not limited to:

- Data Protection Act 2018
- General Data Protection Regulation (EU) 2016/679
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Common law duty of confidentiality
- Human Rights Act 1998
- NHS Act 2006
- Health and Social Care Act 2012
- Care Act 2014

This is not an exhaustive list of legislation which interacts with Information Governance requirements, for advice on other legal obligations specific to work area contact the IG team: nccg.informationgovernance@nhs.net

14.0 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. Those to whom this policy applies are responsible for familiarizing themselves periodically with the latest version and for complying with policy requirements at all times.

15.0 Implementation and dissemination of document

The updated Policy, once approved, will be shared with all staff through the all staff email, and physical staff briefing to support this dissemination and updated on the intranet where this is available.
Awareness of the policy will be checked through a staff survey and spot checks on at least an annual basis.

Appendix A: Quality Assurance Criteria

Approach	Aim	Objective	Quality Criteria
External Audit	To provide independent scrutiny and challenge to the organisation's DSPT self-assessment.	To provide the organisation with a report highlighting areas of compliance, non-compliance and areas for improvement.	The CCG own self-assessment position and accompanying evidence will provide the baseline for the external audit review and subsequent report. The DSPT indicates what evidence is required as mandatory for each requirement so it is essential the evidence made available to the auditor is consistent with that detailed in the DSPT. It is possible that a customer (current or future) may commission such an audit.
Internal Review	To provide an internal but objective assessment of performance against an agreed scope, which may be defined by the DSPT or some additional criteria.	To 'drill down' on to a specific issue or area using a 'check and challenge' approach which does not assume compliance but actively looks for areas for further improvement.	The audit scope will define the quality criteria so will be defined alongside the scope. If the scope is defined by a particular requirement or set of requirements in the DSPT then the quality criteria will be similarly defined (e.g. is X policy in place and in date?).
Learning Lessons	To recognise that most incidents, events or near misses provide an opportunity to review current practices or behaviours and implement change to minimise the chance of recurrence.	To act on the outcomes and recommendations of investigations and other reviews that have been carried out with the intention of improving and/or changing the status quo with a positive change.	Evidence that lessons learnt have been implemented and assessed to ensure the original issue has been resolved and no new risks or concerns have been introduced.
Risk Management	To use risk assessment and management as a positive lever that reduces the likelihood of risks or issues escalating into incidents, breaches or other negative outcomes.	Actively utilise risk management as a discipline that contributes to effective clinical and corporate governance and reduces the organisation's overall risk profile.	Use of a recognised methodology for assessing and measuring risks. Action Plans arising from risk registers and evidence that high and moderate level risks are actively tackled. Risks will have an identified Owner who is accountable for managing the risk until it has been removed or reduced to a level considered acceptable by the organisation.

Approach	Aim	Objective	Quality Criteria
Benchmarking	To recognise that experience from elsewhere can be a useful measure of current organisational performance and source of future improvement planning.	By identifying performance against a range of peer organisations, significant variances from the 'norm' can be used to focus effort and prioritise the delivery of improvements working with these same organisations where possible for mutual benefit. Be willing to share examples of good practice with others.	Evidence that under-performing or 'outlier' activities or areas are targeted for improvement related action so that overall performance / compliance is increased.
Performance Reports	To use corporate intelligence systems to help direct, prioritise and feedback IG related actions and initiatives, making best use of resources. Particularly useful where there are clear data parameters that can be defined and measured consistently.	Provide the IG Team, and wider governance function, with a means to demonstrate progress, achievement of milestones and objectives, or cost v benefit/effort assessments when determining priorities and resource commitments.	Will be measured against the data parameters set by the IG Team with periodic 'in progress' updates to determine trajectory and 'actual v anticipated' delivery, enabling adjustments depending on performance.
Communication	To use a range of communication methods to educate, support and enable staff to understand the aims, objectives and applicability of information governance to their roles and responsibilities.	Raise the overall levels of understanding amongst staff so they can then apply that understanding to their working environment, thereby contributing to the IG risk management agenda and enhancing the governance maturity of the organisation. Secondly, to help demystify information governance and ensure it becomes part of 'business as usual' action and thinking.	Increased understanding of information governance, measured by items such as training completion, reduced numbers of incidents/breaches, inclusion of IG within projects, completed staff surveys, increased involvement of and support from IG staff across organisational boundaries and directorates to help deliver corporate objectives.