IG01a – Information Governance Framework

Corby and Nene Clinical Commissioning Groups

Version 2

Document revision history

Date	Version	Revision	Comment	Author / Editor
08/05/2018	1.1	Review	Update for GDPR	Senior Internal and Assurance IG Manager
17/05/2018	1.1a	Prior to CCG review and adoption	Edited for use by Corby CCG Need to add Corby CCG's policies (section 2 and further reading at end), CCG roles & responsibilities (section 5)	John Geaney, IG Compliance Manager
18/05/2018	1.1b	CCG review	Edited to reflect joint working and minor revisions	Information Manager

Document approval

Date	Version	Revision	Role of approver	Approver
23/02/2017	1.0	Final	Policy approval Group	Governance Transition Group
July 2018	2	Final		Corby and Nene Audit and Risk Committees

Contents

1. Introduction

This Information Governance framework provides a solid basis upon which Information Governance and all its component parts will be implemented throughout Corby and Nene CCGs and inform the service we provide to our customers. The Framework outlines the roles and responsibilities of those who are tasked with overseeing that IG is appropriately supported and that all necessary guidance and advice is available in an effective and efficient manner as well as the responsibilities of all staff.

The Framework is based upon the legal requirements of the Data Protection Act (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), Common law duty of Confidentiality and Human Rights Act, the NHS Constitution and the Department of Health; NHS England and NHS Digital Information Governance assurance regimes, the NHS Information Governance toolkit. In particular, this framework also takes into account the requirement that the CCGs must be able to give assurance to NHS England, in line with the requirements of the NHS England IG Operating Model: https://www.england.nhs.uk/contact-us/pub-scheme/pol-proc/

This Framework will underpin the Information Governance policies, procedures and processes upon which the CCGs rely, in their duties to provide and support the business of its customers.

The law allows personal data to be shared between those offering care directly to patients but it protects patients' confidentiality when data about them are used for other purposes. These "secondary uses" of data are essential if we are to run a safe, efficient, and equitable health service. They include:

- Reviewing and improving the quality of care provided
- Researching what treatments work best
- Commissioning clinical services
- Planning public health services

Generally speaking, people within the healthcare system using data for secondary purposes must only use data that does not identify individual patients unless they have the consent of the patient themselves.

2. Purpose

All providers of NHS care are required by law to have effective arrangements in place to govern the use of information. They therefore have a legal responsibility to comply with the information governance requirements associated with this designation. There have been multiple changes in the NHS since the 2013, particularly within the information and data governance field, Specifically we must be able to support the NHS Planning Guidance[1], the implementation of the NHS Five Year Forward View[2] and the anticipated new EU Data Protection Regulations, therefore information sharing and processing has and will become increasingly complex.

[1] NHS England and NHS Improvement, NHS Operating and Contracting Guidance 2017 – 2019, 22nd September 2016 https://www.england.nhs.uk/ourwork/futurenhs/deliver-forward-view/ accessed 23rd January 2017.
[2] NHS, Five Year Forward View, 23rd October 2014, https://www.england.nhs.uk/wp-content/uploads/2014/10/5yfv-web.pdf accessed 23rd January 2013.

Overall, this information governance framework and the associated controls we intend to embed within the CCGs Directorates will enable a stronger focus and effective utilisation of information across health communities to support delivery strategies and removing barriers to information sharing, perceived and real, by effective and proactive information governance engagement across the Health and Care System for every customer.

Information governance covers the framework of law and best practice within which information is managed in a confidential, consistent and secure manner. Particular focus is placed on the management of personal data and other confidential information including commercially sensitive submissions from industry to ensure it is handled legally, securely and efficiently in accordance with business needs.

the CCG Information Governance Team will apply a risk based approach to all identified workstreams programmes and base implementation on provisions set out in legislation, national and local policy and information governance best practice.

Below is the list of the key documents produced and published on the CSU intranet Policies page and are available on request:

Further supporting documents specific to the CCG protocols will be made available on the CCG intranet where this is available and in the shared drive

Information Governance Policy	Information Management Policy	Information Security Policy	Information Quality Policy
IG01a CSU Information Governance Framework	IG02a CSU Information Management Policy	IG05 CCG Data Security and Protection Incident Reporting Procedure	IG07 Data Protection Impact Assessment Procedure
IG01b CSU Information Governance Policy	IG03 CCG Information Disclosure and Sharing Policy and Procedure	IG08a CSU Information Security Framework	IG10a CSU Information Quality Policy
IG06 CSU Confidentiality code of conduct	IG04 CCG Email and Internet Policy	IG08b CCG Information Security Policy	
IG07 CCG Data Protection Impact Assessment	IG10b CCG Records Management procedure	IG09 CCG Safe haven Policy	
	IG11 CCG Subject Access Request procedure (inc. AHRA)		
	IG12 FOI Policy		

3. Scope

General Information Governance Work plan

In order to ensure on-going assurance the CCG will undertake a series of checkpoints each year to ensure regular scrutiny of the use of information. This supports the submission of the Data Security and Protection Toolkit, NHS England assurance requirements and any other assurance model, should it be required. These are elaborated in more detail in the relevant IG Policy, Protocol or Procedure, but are these key check points:

- Information Flows (mapped and risk reviewed).
- Information Asset Register (risk review).
- Information Risks reviews and impact assessments.
- Confidentiality Audit and Staff Survey.
- Internal compliance assurance.
    - Facilitation of the required reporting to enable assurance.

These will be quality assured and supported via the Information Governance Working Group and the governance structure of the organisation.

The general work plan will co-ordinate with the specific work plans detailed below to complete an on-going assurance framework with a yearly assessment of standards and risks. The CCG will maintain a quarterly review cycle via the Information Governance Working Group to ensure appropriate scrutiny.

Specific Information Governance Work plan

To meet specific requirements of the assurance framework key tasks and evidence will be sought and evaluated from particular functions and providers. This will be elaborated in any contract or written agreement with customers or approved service providers to the CCG, which will outline the timeframe and particulars of quality assurance. Details of the evidence in place, schedule of delivery and evaluation will be maintained by the Governance Function for the CCG, supported by Information Governance – as required.

Information and Informatics IG Work Programme

The Informatics Lead will lead on the following areas:

- Secondary Use Assurance.
- Data Quality, benchmarking and auditing.
- Support the confidential use of patient information by leading, as appropriate, the use of pseudonymisation and anonymisation techniques.
- Identify and report Information Risks related to the secondary use of patient data for key business functions (such as commissioning, performance and informatics).

Information and Communications Technology IG Work Programme

The ICT Lead will lead on the following areas:

- Information Security Assurance and appropriate work-plan.
- Manage the requirements for assurance, scrutiny and performance monitoring in conjunction with the IG Team to achieve internal compliance requirements for the CCG and customer expectations – as defined by contract and the DSP Toolkit.
- Lead on the ICT elements of key Information Governance schemes to deliver assurance and meet quality of service expectations.
- Identify and report Information Risks related to information security as part of the ICT Risk register and Information Risk register.

4. Information Governance Framework Activities

The following information for the rest of the document will detail the activities which will need to be carried out for the implementation of the IG agenda for the CCG. Some guidance and examples have been provided.

Stakeholder engagement

4.1 The Information Governance team must be contacted at the initiation of any project where personal confidential data or commercially sensitive data is to be managed; to include design, implementation and understanding any challenges at the outset of the project.

4.2 Risks and issues identified by stakeholders should be documented within the data protection impact assessment for such projects.

4.3 The Information Governance team will:

4.3.1 Consider the opportunities that are emerging, e.g. those which might fall under the following headings: social, technological, environment, economic, political.

4.3.2 Identify threats which could or will present difficulties for the project. These might include new legislation requiring changes in practice, financial constraints, data sharing risks, etc.

4.3.2.1 Examples of NHS-related elements that may impact on activity are:

- Paperlite and Integrated Care Agenda
- Patient Access to Care Records
- Embedding the Data Protection Act 2018 rules and the EU General Data Protection Regulation
- Further establishment of STPs and ICS arrangements.

5. Accountability and Governance Structure

IG Assurance

5.1 Accountable Officer

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

5.2 Data Protection Officer

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 CCG and its 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 CCG.

5.3 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.

5.4 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is appointed by the Corporate 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.

5.5 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.

5.6 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.

5.7 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.

5.8 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.

5.9 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.

On-boarding Procedure

This allows a standard process to be followed in the event of new organisations signing up to the contract / agreements.

Check online registers to ensure that all new organisations have a compliant DSP Toolkit and are registered with ICO to process the appropriate Personal Data.

Ensure all new organisations sign up to Data Sharing documents.

Ensure all new organisations have agreed to mandatory training.

Where there is more than one Data Controller, ensure they all remain fully engaged throughout the process.

Data Risk Management

Data Protection Impact Assessment (DPIA)

A DPIA enables an organisation to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be identified through the gathering and sharing of data and consulting with stakeholders.

The DPIA identifies and assesses privacy implications where data about individuals is collected, stored, transferred, shared and managed. It enables organisations to identify the impact that any project might

have on the rights of the public / staff when processing their data. Systems can be designed to avoid unnecessary privacy intrusion or breaches, and features to reduce privacy intrusion can be built in from the outset.

The DPIA will assist in the mitigation of data risks and facilitate the modification of plans. A DPIA should be a process rather than output orientated.

A DPIA should be completed when the following activities occur:

- Developing or procuring any new programme, policy, procedure, service, technology or system ("project") that handles or collects data relating to individuals.
- Developing revisions to an existing programme, policy, procedure, service, technology or system which significantly change how data is managed.

The DPIA should be undertaken by the project team and identify areas for action in order to satisfy the statutory/mandatory framework for processing personal data, including identifying information risks to be added to the project risk register.

Privacy by design

Privacy by design means building privacy into the design, operation and management of a system specification.

There are security areas that should be considered when creating bespoke technology or engaging existing technology.

Further reading: Information Commissioner's Office (ICO) Privacy by Design.

6. Monitoring and compliance

This framework and the associated controls: Policies, Protocols, Procedures - will be monitored through the Risk Management system for the CCG. The Risk Register will be reviewed on a frequent basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information Risk Management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Information Risk Owners, assisted by Information Risk Administrators, will be required to routinely review the Risks and Information Flows associated with the Information Assets utilised to fulfil the business functions and activities within their remit.

7. 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 familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

8. Implementation and dissemination of document

The framework, once approved will be published within the CCG, made available publicly to meet publication scheme obligations and if requested via a Freedom of Information request and placed on the Policy register.

Further Reading/References

Corby and Nene CCG

CCG Policies and Procedures, forms and templates as available on the intranet where available or the shared drives

NHS England

Corporate Policies

Risk Stratification

Invoice Validation
Data Services for Commissioners

Caldicott

National Data Guardian

Information: To share or not to share? The Information Governance Review
Government Response to the Caldicott Review
Review of data security, consent and opt-outs

Information Governance Alliance (IGA)

Information Governance Alliance

NHS

The NHS Constitution - the NHS belongs to us all
NHS Confidentiality Code of Conduct

Health Research Authority (HRA)

Health Research Authority
Section 251 and the Confidentiality Advisory Group (CAG)

British Medical Association (BMA)

Principles for sharing local electronic patient records for direct patient care