PLEASE DESTROY ALL PREVIOUS VERSIONS OF THIS DOCUMENT

NHS
Islington
Clinical Commissioning Group

INFORMATION GOVERNANCE FRAMEWORK AND STRATEGY

1	**POLICY DRAFTED BY:**	**NELCSU INFORMATION GOVERNANCE TEAM**
2	**ACCOUNTABLE DIRECTOR:**	**DIRECTOR OF QUALITY AND GOVERNANCE**
3	**APPLIES TO:**	**ISLINGTON CLINICAL COMMISSIONING GROUP STAFF**
4	**COMMITTEE & DATE APPROVED:**	**EMT 7th December 2016**
5	**VERSION:**	**1.0**
6	**RELATED DOCUMENTS:**	**CALENDAR, EMAIL AND INTERNET POLICY** **CONFIDENTIALITY AND DISCLOSURE OF INFORMATION POLICY** **INFORMATION GOVERNANCE POLICY** **INFORMATION GOVERNANCE FRAMEWORK AND STRATEGY** **INFORMATION MANAGEMENT POLICY** **INFORMATION SECURITY POLICY**
7	**DATE OF IMPLEMENTATION:**	**January 2017**
8	**DATE OF NEXT REVIEW:**	**OCTOBER 2018**

DOCUMENT CONTROL

Date	Version	Action	Amendments
07/09/2016	1.0	New IGF/ Strategy for Islington CCG in line with policies issued by NELCSU in accordance with SLA	

CONTENTS

Introduction

Information is a vital yet potentially vulnerable asset, both in terms of the clinical management of individual patients and the efficient commissioning and management of services and resources. It plays a key part in clinical governance, service planning and performance management.

It is therefore of importance to ensure that information is efficiently managed and that appropriate policies, procedures and management accountability and structures provide a robust information governance framework for information management.

The following document outlines how Islington Clinical Commissioning Group (CCG) will address the Information Governance (IG) agenda.

This strategy will be supported by an annual IG Toolkit improvement plan focussing on the changing compliance framework requirements, new legislation and areas specifically identified for CCG improvement.

The strategy is also supported by the Information Governance Policy which covers all aspects of holding, obtaining, recording, using, sharing and disclosing of data/information or records, held in a manual/paper or electronic format, by or on behalf of the CCG.

1. Information Governance (IG) defined

IG can be defined as the discipline of ensuring that the NHS complies with its statutory obligations to protect patient privacy including its obligation to ensure confidentiality in the collection, processing and management of information.

The components of the IG Toolkit Annual Assessment are summarised in the image below:

2. Objectives

An outline of the high-level IG organisational objectives that we aim to achieve is as follows:

- Comply with the relevant information privacy and confidentiality laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance via the IG Toolkit.

- Maintain information risk at acceptable levels and protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions.
- Address the increasing potential for civil or legal liability impact on the organisation as a result of information breaches through efficient and effective risk management, process improvement and rapid incident management.
- Comply with Caldicott 2 and the Department of Health Cyber Security requirements via the IG Toolkit. Through provision of evidence within the IG work plan 2016/17.
- Provide confidence in interactions with key external organisations – for example, Royal Free Hospital, Whittington Hospital, Community Providers, neighbouring CCGs including other North and East London Commissioning Support Unit (NEL CSU) customers, NHS England and NHS Digital.
- Create, maintain and continuously improve trust from customers and the public.
- Provide accountability for safeguarding patient and other critical information.
- Protect the organisation's reputation.

3. Implementation

The implementation of this IG strategy and the IG Toolkit plan will ensure that information is more effectively managed within the CCG. To support this strategy, Islington CCG will implement key IG policies and will ensure that staffs abide by these. These polices are:

- Information Governance Policy
- Information Security Policy
- Information Management
- Confidentiality and Disclosure Policy
- Calendar, Email and Internet Policy

Each year the IG strategy will be reviewed and a revised IG Toolkit plan will be developed against the IG Toolkit attainment levels and scores, thus identifying the key areas for a programme of continuous improvement.

4. Information Governance Plan

An overarching annual IG work plan will be overseen by the CCG IG Group. It will require active engagement with all areas of the organisation and to ensure this, quarterly reporting will also be to the CCG Executive Management Team (EMT).

The plan will ensure compliance with the Information Governance Toolkit assessment to level 2 (satisfactory) maintaining and building upon the previous submitted annual IG Toolkit score.

A summary of the activities required to be undertaken is contained within the 2016/17 IG work plan.

The IG Toolkit report will be submitted to the CCG EMT on a quarterly basis and the Governing Body will receive a 6 monthly IG update report.

5. Roles and Responsibilities

Role	Summary	Who
Accountable Officer	Has overall accountability and responsibility for governance within the organisation. **Is provided with assurance, that all risks to the organisation, including those relating to information, are effectively managed and mitigated.**	Chief Officer
Senior Information Risk Owner (SIRO)	Has overall responsibility for ensuring that effective systems and processes are in place to address the Information Governance agenda. • Foster a culture for protecting and using data. • Ensure information risk requirements are included in the Corporate Risk Management Policy. • Ensure Information Asset Owners (IAOs) undertake risk assessments of their assets. • Take ownership of the annual review of information flows and information asset register and any advised recommendations. • Ensure IAOs and Information asset Administrators have carried out their annual online Information Governance training. Be responsible for the Incident Management process ensuring identified information security risks are followed up, incidents managed and lessons learnt. • Provide a focal point for the management, resolution and/or discussion of information risk issues. • Ensure that the CCGs approach to information risk is effective in its deployment in terms of resource, commitment and execution and that this is communicated to all staff. • Ensure the organisation is adequately briefed on information risk issues. • Be accountable for information risk. • Has delegated authority to review and approve the IG Toolkit submission in cases where the Quality committee cannot meet to approve the pre- toolkit submission. The SIRO roles and responsibilities are defined in Appendix 1 of the NHS Information Risk Management Guidance. The role holder will be supported and advised by the IG Team at NEL CSU.	Director of Quality and Governance/ Head of Corporate Affairs
Caldicott Guardian	The role of the Caldicott Guardian is an advisory role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality & information sharing issues. It should be noted this is limited to where the CCG owns the data. • The Caldicott Guardian is supported in this role by the NEL CSU IG Team. • The Caldicott plan will be mapped into the existing IG work plan for 2016 – 17.	GP Lead for Clinical and Quality

Role	Summary	Who
Information Asset Owners (IAOs)	All senior staff at Director level are required to act as Information Asset Owners (IAOs) for the information assets within their remit. They will: • Provide assurance to the SIRO that information risk is managed effectively for the information assets identified as within their remit. • Ensure all Information Assets and flows of data within their remit are identified and logged ensuring each has a legal basis to be processed. • Identify, manage and escalate all information security (for example, dependencies and access control) and information risks as appropriate. • Complete mandatory annual IG online additional training related to the IAO role. The IAOs will be supported by Information Asset Administrators who will ensure the above takes place. The detailed roles and responsibilities are defined in Appendix 1 of the NHS Information Risk Management Guidance	Directors
Information Asset Administrators (IAA)	Information Asset Administrators (IAAs) are the most senior individual user or direct users of systems and have an understanding as to how it works and how it is used. • They will ensure there are procedures for using them, control access to them and understand their limitations. • Complete mandatory annual and additional IG training online. • Review the information assets and flows of data relating to their area of work. The detailed roles and responsibilities are defined in Appendix 1 of the NHS Information Risk Management Guidance	Senior Managers
Information Governance Lead at the CCG	CCG IG Lead working with CSU IG Advisor to jointly cover and deliver the IG Agenda and IG Plan for the CCG. The IG Lead at the CCG acting as the first point of call for the CSU IG Advisor and responsible for cascading information to colleagues in the CCG and for improving IG awareness and compliance in the CCG. • IG Lead at the CCG responsible for helping co-ordinate Data Handling Review (covers Data Mapping) and for delivering key IG messages within CCG • Complete mandatory and additional online IG training.	Head of Corporate Affairs/ Governance and Risk Manager
All Staff	All those working for the CCG have legal obligations, under the Data Protection Act, Common Law of Confidentiality, and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct. These are in addition to their contractual obligations with the CCG which include adherence to policy, and confidentiality clauses in their contract. To complete mandatory annual IG online training.	All Staff

Role	Summary	Who
Third parties	The same responsibilities apply to those working on behalf of the CCG whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of the CCG are required to sign a third party agreement outlining their duties and obligations.	All third parties
CSU IG Team	As part of the IG Service Level Agreement, the CSU IG Team members work with the CCG internal IG lead to support the CCG in delivering the IG Framework and Strategy, IG Toolkit, compliance with the IG Policies and other IG-related initiatives, allowing the CCG to carry out business as a usual in a safe and secure manner. Where for example the CSU provides a service to the CCG, e.g. HR services, then the CSU IG Team provide the IG assurance related to the appropriate IG Toolkit areas.	CSU IG Team

6. IG Incidents

Islington CCG will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and procedure.

All information incidents must be reported as soon as the issue is detected in accordance with Islington CCG's policies and guidance.

Islington CCG will ensure that the IG agenda is addressed regularly by the IG Group responsible for oversight of IG matters and IG is embedded within working practices. The EMT will receive IG reports from the CSU on a quarterly basis.

Reporting IG Incidents

All information incidents must be reported as soon as the issue is detected **using Islington CCG's Incident reporting procedure**.

The template is based on the grading system used in the recently released NHS Digital IG incident reporting guidance – **NHS Digital – IG SIRI Checklist Guidance**

These IG incidents cover:

- Near misses of information incidents
- Suspected information incidents (such as losses of data or breaches of confidentiality)
- Information Incidents (data losses and breaches of confidentiality)
- Patient Identifiable Data sent to the wrong individual
- Cyber related incidents. These include for example spoof websites, cyberbullying and phishing emails. For more examples of cyber related incidents, please refer to the IG SIRI checklist Guidance in the references or further guidance section.

If the incident is assessed at level two or higher, it must be reported via **the IG Incident Reporting tool which is accessed via the IG toolkit website**.

The incident should be investigated in accordance with Islington CCG's Incidents and Serious Incidents reporting, Investigating and Management Policy.

Escalation of IG Incidents and Events

There is a requirement that certain incidents once assessed using the IG Incident assessment template be escalated to the Information Commissioners Office and Department of Health.

Other areas could potentially include customers, NHS England and other NHS organisations. This should be considered and continually reviewed in line with contractual requirements and the investigation process. Where this decision is to be taken it should be taken by the SIRO or where not available a director in conjunction with the Information Governance Team.

7. Training and Staff Support

Islington CCG will ensure that all staff are provided with relevant training and support to ensure that information risks are minimised. Islington CCG will achieve this by:

- Mandating that all staff, as a minimum, undertake appropriate information governance training.
- Training needs analysis will be conducted and any recommendations identified will be disseminated to staff.
- Keeping all staff informed of standards to support this strategy via staff bulletins and where necessary Information Governance specific messages.

In addition to the mandatory Introduction to IG or IG: The Refresher training module (depending on whether staff have previously successfully completed the Introduction to IG training)[1], identified staff (as set out in section 5 - Roles and Responsibilities) are also required to complete additional training appropriate to their duties.

The following staff will need to carry out additional IG online annual training as part of their respective roles s and responsibility.

- Information Asset Owners (IAOs)
- Information Asset Administrators (IAAs)
- Senior Information Risk Owner (SIRO)
- Caldicott Guardian (CG)
- CCG Internal IG lead

This will ensure that the CCG has the requisite IG awareness and controls in place to implement its IG Strategy and Framework.

8. Support and advice

As we build on relationships with organisations, harnessing and using data in new ways, it is important to recognise that guidance may not always be readily available externally. NEL CSU Information Governance Team will be a focal point and provide authoritative advice and guidance regarding the legal use of data in particular personal confidential data. They will be available via information.governanance@nelcsu.nhs.uk

9. Policy, Protocol and Procedure Distribution

All employee based policies, protocols and procedures will be made available on the CCG intranet and will be highlighted in staff briefings.
Knowledge of the key details of Information Governance related policies will be tested through the use of the online Information Governance training tool, and the use of staff surveys to test knowledge in particular areas.

[1] The online training tool will be decommissioned in December 2016. The replacement online training tool will be available from April 2017.

10. Monitoring and Review

Performance against this strategy will be monitored against the IG Toolkit requirements. These will be reported quarterly to the EMT.

This document will be reviewed on an annual basis, and in accordance with the following on an as and when basis:

- Legislative or case law changes;
- Changes or release of good practice or statutory guidance;
- Identified deficiencies, risks or following significant incidents reported;
- Changes to organisational infrastructure.

11. Key Legislation and Guidance

Access to Health Records Act 1990
Computer Misuse Act 1990
Data Protection Act 1998
Fraud Act 2006
NHS Act 2006
Regulation of Investigatory Powers Act 2000

References/Guidance

NHS Information Risk Management Guidance:

http://systems.digital.nhs.uk/infogov/security/risk/inforiskmgtgpg.pdf

IG Training tool (until December 2016):

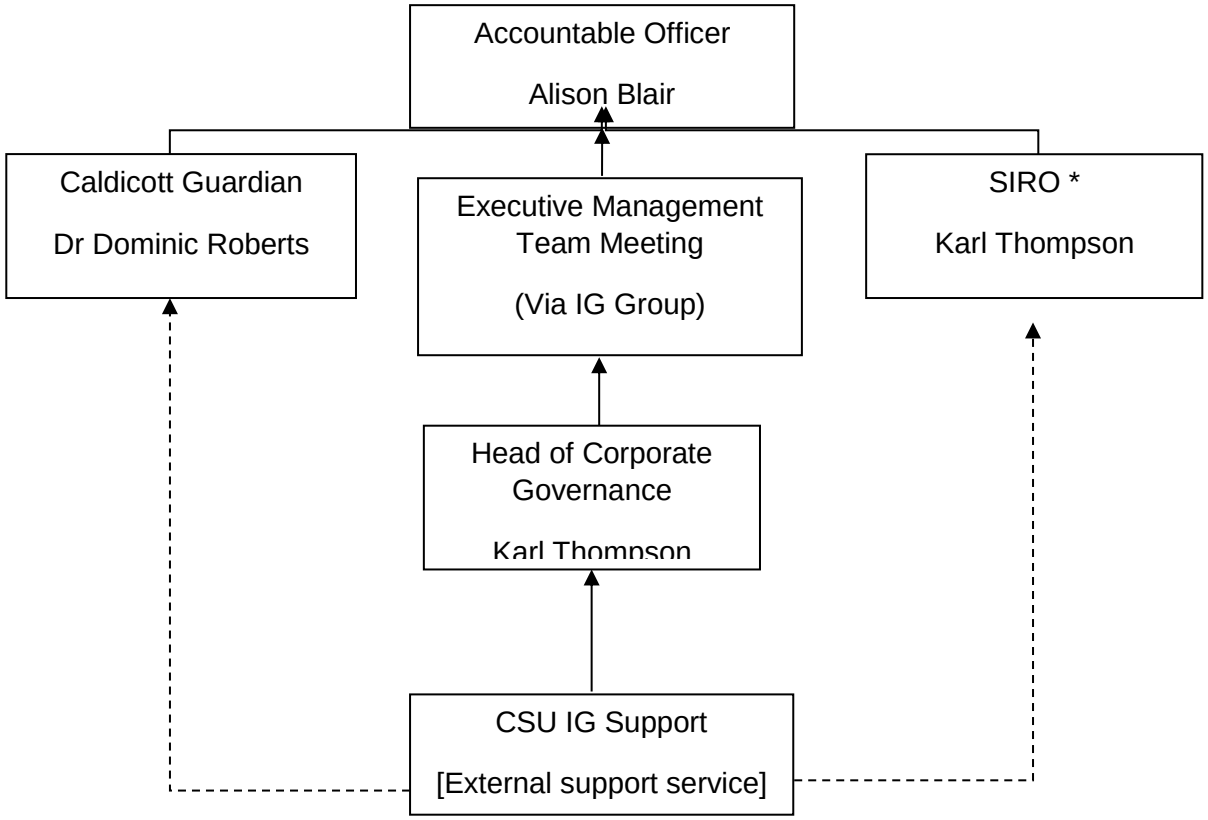
https://www.igtt.hscic.gov.uk/igte/index.cfm

IG SIRI Checklist Guidance:
https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf

IG Incident Reporting Tool User Guide (including IG SIRI assessment Tool):
https://nww.igt.hscic.gov.uk/resources/The%20Incident%20Reporting%20Tool%20User%20Guide.pdf

PLEASE DESTROY ALL PREVIOUS VERSIONS OF THIS DOCUMENT

Heading	Requirement	RAG	Compliance
Key Policies	Full suite of IG policies produced. To be ratified and disseminated November 2016.		The CCG currently have the following policies in draft: Information governance Policy Information Security Policy Information Management Policy Confidentiality and Disclosure Policy Calendar, Email and Internet Policy
Senior Roles and resources	The organisation should have in place at a minimum: Information Governance Lead Senior Information Risk Owner (SIRO) Caldicott Guardian		The CCG currently have nominated individuals acting in the official capacity as IG Lead, SIRO and Caldicott Guardian. The key roles are fulfilled by: • Caldicott Guardian – Dr Dominic Roberts • Senior Information Risk Owner (SIRO) – Karl Thompson • Information Governance Lead – Mr Karl Thompson These are supported by skills and experience though the SLA with the NEL CSU. <u>Information Governance Structure and Support:</u> The diagram below demonstrates how those roles are supported with adequate knowledge and skills and the line management and other reporting lines. All roles are required to complete relevant training modules in line with NHS Digital requirements.

Heading	Requirement	RAG	Compliance
	Information Governance Structure and Support		 * Information Asset Owners and Administrators will provide assurance relating to managed assets via the **Information Governance Steering Group** and place any risks on the **risk register.**
Key Governance Bodies	IG Group CCG EMT		Information Governance will be reported into the CCG via the Information Governance Group to the CCG EMT which meets every 2 weeks. The EMT will decide if issues need to be escalated to the CCG Governing body.
Governance Framework	Details of how responsibility and accountability for IG		All those working for the CCG have legal obligations, under the Data Protection Act, Common Law of Confidentiality, and professional obligations, for example the Confidentiality NHS Code of Practice and

Heading	Requirement	RAG	Compliance
	is cascaded through the organisation.		professional codes of conduct. These are in addition to their contractual obligations (with the CCG) – adherence to policy and confidentiality clauses in their contract. **All staff are responsible for the maintenance of confidentiality**, the protection and appropriate use of personal data in accordance with the Data Protection Act. These details are outlined in the contract that all staff are required to sign and adhere to. **The same responsibilities apply to those working on behalf of the organisations** whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of the organisation are required to sign a third party agreement outlining their duties and obligations. Islington CCG will adhere to these responsibilities and has developed additional guidance to support its policies.
Training & Guidance	Staff Code of Conduct Training for all staff Training for specialist IG roles		Intranet pages providing access to CCG policies - are accessible to all CCG staff. Policies on information governance issues, cover the following topics: ▪ Principles of Information Governance ▪ Information Management ▪ Data Protection ▪ Consent ▪ Confidentiality ▪ Records Management These pages will be supported by an active communication campaign to all staff to ensure staff receive clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. There will also be information governance at Induction and as part of annual mandatory training. All staff are required to complete and pass Information Governance training using the online information governance training module. Certain roles will be required to undertake further training as outlined in the organisations Information Governance Training Needs Analysis. All staff and those working on the organisation's behalf are expected to undergo the outlined training (including contractors, temporary staff, students, volunteers, work placements, etc.). Managers must ensure a local induction is completed that provides assurance that those working for the organisation are aware of their responsibilities under the law and policy, and how that impacts upon their day to day work.

Heading	Requirement	RAG	Compliance
Incident Management	Documented procedures and staff awareness		Clear guidance on incident management procedures is being developed and will be made available on the intranet. This systems will ensure that incidents will be collated centrally so that staff can be made aware of lessons that can be learned from internal, local and national incidents that may occur.