Information Governance Strategy

Number: 1	Version: 1

NHS
Tower Hamlets
Clinical Commissioning Group

Executive Summary	The Information Governance Strategy outlines the CCGs governance aims and the key objectives of its governance policies. The Chief Officer has the overarching responsibility for Governance. The Deputy Director of Strategy and Planning the named person with the responsibility for Governance and is the delegated Senior Information risk Owner (SIRO) for the CCG. The Principal Clinical lead on the governing body is (Dr Osman Bhatti) who is the Caldicott Guardian for the CCG.
Date of ratification	Senior Management Team on 28 January 2016
Document Author(s)	Mary Olubi – CCG IG Facilitator (NELCSU)
Who has been consulted?	All staff.
Was an Equality Analysis required?	No
With what standards does this document demonstrate compliance?	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 The Caldicott Principle

References and associated CCG documentation	Information Governance Policy Information Security Policy Records management Policy Confidentiality and Disclosure of Information Policy Calendar, Internet and Email Policy Information Risk Management Guidance		
List of approvals obtained	Senior Management Team Executive Team Committee		
Recommended review period	Annually		
Key words contained in document	Information Governance, Clinical Governance, Service planning, Performance management and Quality assurance		
Is this document fit for the public domain? Y / N	**Y**	**If No, why?**	

Document Control

Date	Version	Action	Amendments
05/11/2015	Draft	Mary Olubi Strategy reviewed to reflect current changes in legislation.	Reference to Caldicott 2 assurance compliance. Referenced the new Caldicott work tasks in the IG Toolkit requirements Reference to annual online IG training for Information Asset Owners (IAOs), Information Asset Administrator (IAA), SIRO, Caldicott Guardian and IG Lead Updated Guidance on IG Incident reporting and the need to report IG Serious Incidents within 24 hours via IG Toolkit Updated website link for IG Training website and IG incident reporting Reference to Cyber Security and the IG Toolkit

			Amendments and update to role and responsibility section of the document.

Contents

Information Governance Strategy 1

Introduction 4

1. Information Governance (IG) defined 4

2. Objectives 5

3. Implementation 5

4. Information Governance Plan 6

5. Roles and Responsibilities 7

6. IG Incidents 9

7. Training and Staff Support 11

8. Support and advice 11

9. Policy, Protocol and Procedure Distribution 12

10. Monitoring and Review 12

11. Key Legislation and Guidance 12

Introduction

In the NHS, 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 paramount 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 Tower Hamlet Clinical Commissioning Group (THCCG) will address the Information Governance (IG) agenda.

This strategy is in the second year of a 3 year long term vision for Information Governance. The NHS has gone through a period of radical change. As a result, this long term strategy will be supported by an annual improvement IG Toolkit plan focussing on changing compliance framework requirements, new legislation and areas specifically identified for improvement by the CCG.

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 of ensuring confidentiality in the collection, processing and management of data and information.

IG is defined by the requirements that the organisation is required to demonstrate compliance with as part of the IG Toolkit Annual Assessment, these include the following domains in the diagram below.

2. Objectives

An outline of the high-level IG organisational objectives that we seek 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 impacting the organisation as a result of information breaches through efficient and effective risk management, process improvement and rapid incident management;
- To comply with the Department of Health Caldicott 2 compliance levels. The assurance is currently linked to the CCG version13 (V13) IG work plan related toolkit requirements and will also be via the IG Toolkit submission at the end of March 2016. It is anticipated that detailed guidance may follow from the Department of Health on the CCG compliance with Caldicott 2 during 2015-16.
- To comply with the Department of Health Cyber Security compliance levels. This will be via the IG Toolkit. Through provision of evidence on the related Cyber Security IG Toolkit requirements within the IG work plan 2015/16.
- Provide confidence in interactions with key external organisations – for example, Royal Free Hospital, Royal National Orthopaedic Hospital, Community Providers and neighbouring CCGs such as North and East London Commissioning Support Unit (NEL CSU), customers, NHS England, the Health and Social Care Information Centre (HSCIC) and healthcare providers;
- Create, maintain and continuously improve trust from customers and the public;
- Provide accountability for safeguarding patient and other critical information ; and
- Protect the organisation's reputation.

3. Implementation

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

- IG Policy
- Information Security Policy
- Information Management
- Confidentiality and Data Protection Act

- Internet & Email

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 Executive Team. It will require active engagement with all areas of the organisation.

The plan will ensure compliance with the Information Governance Toolkit assessment to level 2 (satisfactory), as part of best practice and to maintain and build upon the previous submitted annual IG Toolkit score and link with Cyber Security requirements and Caldicott 2. It is anticipated that there will be some IG toolkit requirements that may therefore achieve level 3 IG Toolkit scores but this is subject to CCG local resources and local IG reporting within the CCG.

A summary of the activities required to be undertaken is contained within the IG work plan

VERSION 13 IG Toolkit Work Plan.doc

The IG Toolkit report will be submitted to the Executive Team on a quarterly basis and the Governing Body will receive a 6 monthly IG update report. Detailed planning will be included in the Information Governance Toolkit working documents and plans.

5. Roles and Responsibilities

Role	Summary	Who
Director for Quality & Governance	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.	Director of Quality and Governance
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 A 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

Role	Summary	Who
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. • There are some new additional IG areas of Caldicott work in IG Toolkit version 13 for example the Caldicott plan. These are mapped into the existing IG work plan for 2015-16	GP Lead for Clinical and Quality
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 assists 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 A 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 A of the NHS Information Risk Management Guidance	Senior Managers

Role	Summary	Who
Information Governance Lead at the CCG	CCG IG Lead working with CSU IG Lead 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 Lead 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.	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 which include adherence to policy, and confidentiality clauses in their contract. To complete mandatory annual IG online training.	All Staff
Third parties	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.	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 help support the CCG in delivering the IG Strategy and Framework, IG Toolkit, 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

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

All information incidents must be reported as soon as the issue is detected in accordance with Tower Hamlet CCG's Incidents and Serious Incidents reporting, Investigating and Management Policy.

Tower Hamlet CCG will ensure that the IG agenda is addressed and reported to Senior Management and Executive Committee responsible for oversight of IG matters and IG is embedded within working practices. The Executive Committee will request and receive IG reports from the CSU on a periodic basis.

Reporting IG Incidents

All information incidents must be reported as soon as the issue is detected using Tower Hamlet CCG's Incident reporting procedure and form and Incidents and Serious Incidents reporting, Investigating and Management Policy.

The template is based on the grading system used in the recently released HSCIC IG incident reporting guidance – see Appendix A. **HSCIC – 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, cyber bullying 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. This link opens the IG reporting tool guidance: https://nww.igt.hscic.gov.uk/resources/The%20Incident%20Reporting%20Tool%20User%20Guide.pdf

The incident should be investigated in accordance with Tower Hamlet 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 within NEL CSU, 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

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

Mandate that all staff, as a minimum, undertake the “Introduction to Information Governance” e-learning module once followed by the “Information Governance Refresher” on an annual basis. Undertake additional training needs analysis and any recommendations identified will be compiled by staff

Keep all staff informed of compliance and standards set to support this strategy via staff bulletins and where necessary Information Governance specific messages

In addition to the annual mandatory Introduction to IG or IG: The Refresher training module (depending on whether staff have previously successfully completed the Introduction to IG training), identified staff as set out in section 6 (Roles and Responsibilities) are also required to complete additional training appropriate to their duties. This will ensure that the CCG has the requisite IG awareness and controls in place to implement its IG Strategy and Framework.

The following staffs have 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

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.

10. Monitoring and Review

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

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

Appendix A of the NHS Information Risk Management Guidance

IG Training tool - https://www.igtt.hscic.gov.uk/igte/index.cfm

HSCIC – 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