Manchester Health & Care Commissioning
A partnership between Manchester City Council and NHS Manchester CCG

MANCHESTER CITY COUNCIL

NHS Manchester Clinical Commissioning Group

Framework Document

Information Governance Framework

Version: **1.4**

Date: **November 2016**

Document Control Sheet

Title of document:	Information Governance Framework
Placement in Organisation:	Corporate Services Framework

Consultation/Stakeholders	NHS North, Central & South Manchester CCG Information Governance City Wide Corporate Governance Team		
Author(s) name:	Shavarnah Purves Aliyah Ashraf		
Department/Team:	Information Governance Team		
Approved by:	NMCCG Corporate Governance Committee CMCCG Corporate Governance Committee SMCCG Corporate Governance Committee		
Approval date:	December 2015	Review date:	December 2017
Implementation Date:	October 2014		
Implementation Method:	CCG Website Staff Bulletin		
This document is to be read in conjunction with the following documents: *Information Governance Policy* *Records Management Policy* *Acceptable Use Policy* *Information Governance Procedures*			

Version Control

Version	Date	Brief description of change
V 0.1	May 2013	Amendments to reflect CSU Management of IG
V 0.2	August 2013	Amendments made by the Corporate Governance Committee
V 1.1	Oct 2014	Updated by the IG Team
V 1.2	Nov 2015	Amendments to reflect change in IG Team Structure
V 1.3	November 2016	Amendments to reflect change in IG Lead
V 1.4	March 2017	New NHS Manchester CCG Logo

Contents

- Title Page 1
- Document Control Sheet 2
- Contents Page 3

1.0 Introduction 4
2.0 Purpose 5
3.0 Roles and Responsibilities 5
4.0 Definitions of IG Components 13
5.0 Contacts 15

1. Introduction

1.1	The Information Governance Framework document aims to capture the Clinical Commissioning Groups' approach to Information Governance (IG). Robust IG requires clear and effective management, accountability structures, governance processes, documented policies and procedures, staff training and adequate use of resources. The way that an organisation chooses to deliver against these requirements is referred to within the IG Toolkit as the organisation's IG Management Framework. This framework will be approved by the Corporate Governance Committee and reviewed annually.
1.2	This Framework must be read in conjunction with the CCGs' IG Policy and IG Work Plan. A summary of the IG Work Plan can be found in Section 4. There are many different standards and legislation that apply to IG and information handling, including: • Data Protection Act 1998 • Access to Health Records Act 1990 • Freedom of Information Act 2000 • Caldicott Guidance • Public Records Act 1958 • Records Management NHS Code of Practice • Mental Capacity Act 2005 • Common Law Duty of Confidentiality • Confidentiality NHS Code of Practice • International information security standard: ISO/IEC 27002: 2005 • Information Security NHS Code of Practice • Current performance standards (NHS IG Toolkit) • Computer Misuse Act 1990 • Copyright, Designs and Patent Act 1988.
1.3	IG is required to be adequately resourced with effective organisational and managerial structures and processes underpinned by documented policies and procedures, and regular and updated staff training.
1.4	The Department of Health has developed standards of IG requirements and compliance is measured by the IG Toolkit (IGT). The CCG will complete this annual self-assessment tool. The requirements of the IGT cover all aspects of IG including: • IG management • Confidentiality and data protection assurance • Information security assurance • Clinical information assurance • Secondary use assurance • Corporate information assurance • Risk management.
2.	**Purpose**
2.1	The aim of this Framework is to set out how the CCGs will effectively manage IG. Compliance will be achieved through: • Establishing, implementing and maintaining local policies for the effective management of IG. • Establishing robust IG processes that conform to Department of Health standards and comply with all relevant legislation. • Ensuring information is provided accordingly to service users, stakeholders and shareholders about how information is recorded, handled, stored and

shared and managed.
- Providing clear advice, guidance and training to all staff to ensure that they understand and apply the principles of IG to their working practice.
- Sustaining an IG culture through increasing awareness and promoting IG, thus minimising the risk of breaches of personal data.
- Assessing performance using the IG Toolkit and internal audits and developing and implementing action plans to ensure continued improvement.

3. Roles and Responsibilities

3.1 Accountable Officer

The CCGs' Accountable Officers have overall responsibility for IG. As Accountable Officers they are responsible for the management of IG and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

3.2 Joint Governance Committee

The CCG's Joint Governance Committee provide regular IG updates to the Board and any security breaches are escalated to them.

The CCG's Joint Governance Committee, which reports to the Board, controls the implementation and compliance of IG principles. The responsibilities of the group include, but are not limited to:

- Recommending for approval and adoption all related policies, protocols, strategies and procedures within the IG arena, having due regard to legal and NHS requirements.
- Recommending for approval the annual submission of compliance with the requirements in the NHS IG Toolkit and related action plans.
- Co-ordinating and monitoring the IG Policy across the organisation.
- Making recommendations on the necessary resourcing to support requirements.
- Addressing all issues surrounding information management and information security issues that may affect the CCGs.
- Identifying and approving all necessary staff information and training as outlined in the NHS IG Toolkit.
- Ensuring that risks are included on the corporate risk register.

3.3 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) role should be held by a member of the CCG executive. The SIROs are responsible for identifying and managing the information risks to the CCG. This includes oversight of the CCG information security, incident reporting and response arrangements and the Registration Authority business process.

3.4 Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of the patient and service user information and enabling appropriate information sharing.

3.5 Head of IG and IT

	The Head of IT & IG is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. He is also responsible for identifying and managing the information security risks to the CCG. This includes oversight of the technical aspects of service provision and contractual management of Service Level Agreement (SLA) and in addition managing the IT Strategy.
3.6	**CCG IG Team** Currently compromising of The Head of IT & IG and 2 Senior Information Governance Officers. The Head of IG & IT working across the 3 CCGs has been appointed to act as the overall IG lead for the CCGs. They will manage and support delivery of the CCG's IG requirements. IG support will also be provided by the Senior IG Officer(s). Key tasks for the IG Team include: • Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, e.g. the production of an overarching high level framework document supported by relevant policies and procedures. • Ensuring that there is top level awareness and support for IG resourcing and implementation of improvements with the CCG executives. • Establishing working groups, if necessary, to coordinate the activities of staff with IG responsibilities and progress initiatives. • Ensuring annual assessments and audits of IG and other related policies are carried out documented and reported. • Ensuring that the approach to information handling is communicated to all staff and made available to the public. • Ensuring that appropriate training is made available to staff and completed as necessary to support their duties. Liaising with other committees, working groups and programme boards in order to promote and integrate IG standards. • Monitoring information handling activities to ensure compliance with law and guidance. • Providing a focal point for the resolution and/or discussion of IG issues.
3.7	**All Staff** All staff, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of IG.

4. Definitions of IG Components

IG Component	Description
IG Policy	Sets out the Information Governance approach in the three Manchester Clinical Commissioning Groups for ensuring that personal information is dealt with: • Confidentiality – Protecting the personal information from unauthorised access, disclosure or processing; • Integrity – Safeguarding the accuracy and completeness of information and systems; • Availability – Ensuring information is available to users when required; • Quality – Ensuring information is fit for purpose.
Data Protection & Confidentiality	The CCGs are committed to the delivery of a first class confidential service. This means ensuring that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can: • Understand the reasons for processing personal information; • Give their consent for the disclosure and use of their personal information where necessary; • Gain trust in the way the CCG handles information; • Understand their rights to access information held about them.
Information Security	The information held and managed by the CCG is an asset that all staff have a duty and responsibility to protect. The availability of complete and accurate information is essential to the CCG functioning in an efficient manner. The CCG will implement technical and operational standards, policies and processes that align with prevailing standards such as ISO27001 (Information Security Management).
Records Management	The Records Management policy establishes a framework for: 'the creation and management of authentic, reliable and useable records, capable of supporting business functions and activities for as long as they are required'. Records management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound. At the same time record management serves the operational needs of the CCGs and preserves an appropriate historical record. The key components of records management are: • Record creation • Record keeping • Record maintenance (including tracking of record movements) • Access and disclosure • Closure and Transfer • Appraisal • Archiving and disposal

Information Risks	Information risk is a factor that exists in all areas where information of a personal or confidential nature is used and managed. Information risk management is a part of Information Governance (IG) and it is acknowledged that IG, including the management of information risks should be part of the culture of the organisation, ensuring that staff are aware of, and work to, good IG (and therefore information risk) practices.
IG Incident Procedure	An Information Governance or Information Security related incident relates to breaches of security and/or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street. It could also be any event that has resulted or could result in: • The integrity of information system or data being put a risk. • The availability of information system or information being put at risk. An adverse impact, for example, embarrassment to the NHS, threat to personal safety or privacy, legal obligation or penalty, financial loss and/or disruption of activities.

5. Contacts

IG Team – Names and Roles

Mark Wright
Head of Information Governance and IT

Aliyah Ashraf
Senior Information Governance Officer
Covering North Manchester CCG and Central Manchester CCG

Shavarnah Purves
Senior Information Governance Officer
Covering South Manchester CCG and Citywide and Shared Services

Clinical Commissioning Group Leads – Names, Roles and Responsibilities

	Chief Officer	SIRO	Caldicott Guardian
CENTRAL	**Ian Williamson** Chief Officer	**Ed Dyson** Chief Officer	**Dr Manisha Kumar** General Practitioner
NORTH	**Jo Purcell** Chief Clinical Officer	**Martin Whiting** Chief Clinical Officer	**Dr Mobeen Shahbaz** General Practitioner
SOUTH	**Caroline Kurzeja** Chief Officer	**Claudette Elliot** Deputy Chief Officer	**Dr David Adams-Strump** General Practitioner