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

MANCHESTER CITY COUNCIL

NHS Manchester Clinical Commissioning Group

GovernIn

Framework Document

Information Governance Framework

Version: **1.6**

Date: **August 2020**

Document Control Sheet

Title of document:	Information Governance Framework		
Placement in Organisation:	Corporate Services Framework		
Consultation/Stakeholders	NHS Manchester CCG Information Governance Team		
Author(s) name:	Shavarnah Purves, Data Protection Officer		
Department/Team:	Information Governance Team		
Approved by:	Governance Committee		
Approval date:	August 2020	Review date:	August 2021
Implementation Date:			
Implementation Method:	CCG Website Staff Intranet		
This document is to be read in conjunction with the following documents: *Information Governance Policy* *Records Management Policy* *Acceptable Use Policy*			

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
V 1.5	January 2019	Amendments to reflect change in organisation structure and the new GDPR legislation
V1.6	August 2020	Minor changes

Contents

1.	**Introduction**
1.1	The Information Governance Framework document aims to capture Manchester 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 Data Security & Protection Toolkit as the organisation's IG Management Framework. This framework will be approved by the Governance Committee and reviewed annually.
1.2	This Framework must be read in conjunction with the CCGs' IG Policy. There are many different standards and legislation that apply to IG and information handling, including: • Data Protection Act 2018 • General Data Protection Regulations • 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 Data Security and Protection Toolkit) • Computer Misuse Act 1990 • Copyright, Designs and Patent Act 1988. • Cyber Security Essentials
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 and audited staff training.

1.4 NHS Digital has developed standards of IG requirements and compliance is measured by the revised Data Security and Protection Toolkit. The CCG will complete this annual self-assessment tool. The requirements cover all aspects of IG including:

1. **Personal Confidential Data**
   All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

2. **Staff Responsibilities**
   All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. **Training**
   All staff complete appropriate annual data security awareness training and pass a mandatory test.

4. **Managing Data Access**
   Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. **Process Reviews**
   Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

6. **Responding to Incidents**
   Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

7. Continuity Planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

8. Unsupported Systems

No unsupported operating systems, software or internet browsers are used within the IT estate.

9. IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually

10. Accountable Suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

2. Purpose

2.1 The aim of this Framework is to set out how the CCG 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 and NHS Digital 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 Data Security and Protection Toolkit and internal audits and developing and implementing action plans to ensure continued improvement.
2.2	**General Data Protection Regulations (GDPR)** Although in general the principles of the Data Protection Act 2018 remain similar, there is greater focus on evidence-based compliance with specified requirements for transparency, more extensive rights for data subjects and considerably harsher penalties for non-compliance. The GDPR introduced a principle of 'accountability'. This requires that organisations must be able to demonstrate compliance.
3.	**Roles and Responsibilities**
3.1	**Accountable Officer** The Accountable Officer has overall responsibility for IG. The Accountable Officer is responsible for the management of IG and for ensuring appropriate mechanisms are in place to support service delivery and continuity.
3.2	**Governance Committee** The Governance Committee provides regular IG updates to the Board and any security breaches are escalated to them. They all also control 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 Data Security and Protection 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 CCG. • Identifying and approving all necessary staff information and training as outlined in the NHS Data Security and Protection 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 Team. The SIRO is 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.
3.4	**Data Protection Officer (DPO)** The DPO is responsible for ensuring that MHCC complies with all aspects of IG and the GDPR and the Data Protection Act 2018. The DPO is in place to ensure that we can demonstrate compliance with all the requirements of the GDPR.
3.5	**Head of Business Intelligence (BI) & IG** The Head of BI & IG is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG.
3.6	**Head of IT** 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.
3.7	**IG Team** The Head of BI & IG has been appointed to act as the IG lead for the CCG. The IG Team comprises of a Data Protection Officer and 2 Senior IG Officers, this is currently under review. They will manage and support delivery of the CCG's IG requirements. 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 IG approach 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 CCG is 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 CCG 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

Graham Hayler
Head of Business Intelligence and Information Governance

Shavarnah Purves
Data Protection Officer

2 x Senior IG Officers - currently none in post

Manchester Clinical Commissioning Group Leads – Names, Roles and Responsibilities

Chief Officer	**SIRO**	**Caldicott Guardian**
Ian Williamson Chief Operating Officer	**Ed Dyson** Executive Director of Planning & Operations	**Dr Manisha Kumar** Clinical Director

6. Data Security & Protection Toolkit Standards

Ref.	Question
1.1.1	Name of Senior Information Risk Owner.
1.1.2	SIRO Responsibility for data security has been assigned.
1.1.3	Name of Caldicott Guardian.
1.1.4	Who are your staff with responsibility for data protection and/or security?
1.1.5	Staff awareness- Leadership (Q1) I feel data security and protection are important for my organisation.
1.1.6	Name of Appointed Data Protection Officer.
1.2.1	There is a data security and protection policy or policies that follow relevant guidance.
1.2.2	When were the data security and protection policy or policies last updated?
1.2.3	Policy has been approved by the person with overall responsibility for data security.
1.2.4	Data Security and Protection Policies available to the public.
1.2.5	Staff awareness - Policies (Q2). I know the rules about who I share data with and how.
1.2.6	Staff awareness – Policies (Q3). I know who to ask questions about data security in my organisation.
1.3.1	ICO Registration Number.
1.3.2	Transparency information is published and available to the public.
1.3.3	How have Individuals been informed about their rights and how to exercise them?
1.3.4	There is a staff procedure about how to provide information about processing and individuals' rights at the correct time.
1.3.5	There is an updated subject access process to meet shorter GDPR timescales.
1.3.6	Provide details of how access to information requests have been complied with during the last twelve months.
1.3.7	Total ICO Fines in last 12 months.
1.4.1	A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing.
1.4.2	Have information flows been approved by the person responsible for data security?
1.4.3	Date of when information flows were approved by the person with responsibility for data security.
1.4.4	Provide a list of all systems/information assets holding or sharing personal information.

1.4.5	List of systems which do not support individual login with the risks outlined and what compensating measures are in place.
1.5.1	There is approved staff guidance on confidentiality and data protection issues.
1.5.2	Data Protection Compliance monitoring /staff spot checks are regularly carried out to ensure guidance is being followed.
1.5.3	Results of staff spot checks and actions taken when data protection non-compliance is identified.
1.5.4	Staff awareness Question - Used legally and securely (Q4) …. I am happy data is used legally and securely in my organisation.
1.6.1	There is a procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.
1.6.2	Data Protection by design procedure has been agreed.
1.6.3	There are technical controls that prevent information from being inappropriately copied or downloaded.
1.6.4	There are physical controls that prevent unauthorised access to sites.
1.6.7	There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.
1.6.8	The Data Protection Impact Assessment Procedure has been agreed by the person in the organisation with overall responsibility for data security.
1.6.9	The Data Protection Officer is consulted as a matter of routine when a Data Protection Impact Assessments is being carried out.
1.6.10	Have any unmitigated risks been identified through the Data Protection Impact Assessment process?
1.6.11	All high risk data processing has a Data Protection Impact Assessment carried out before processing commences.
1.6.12	All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO.
1.6.13	Data Protection Impact Assessments are published and available as part of the organisation's transparency materials.
1.7.1	There is policy and staff guidance on data quality.
1.8.1	There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived.
1.8.2	A records retention schedule has been produced.
1.8.3	Provide details of when personal data disposal contracts were last

	reviewed/updated.
2.1.1	When was the last review of the list of all systems/information assets holding or sharing personal information?
2.1.2	The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security.
2.2.1	Staff awareness - Shared securely (Q5) …. I know how to use and transmit data securely.
2.2.2	Staff awareness - Used legally and securely (Q6) …. I feel that confidentiality is more important than sharing information for care.
2.2.3	Staff awareness - Processes (Q7) …. The tools and processes used by my organisation make it easy to use and transmit data securely.
2.2.4	Staff awareness - Raising concern (Q8) …. I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination.
2.3.1	There is a data protection and security induction in place for all new entrants to the organisation.
2.3.2	All employment contracts contain data security requirements.
2.3.3	Staff awareness - Laws and principles (Q9) …. I understand the important laws and principles on data sharing, and when I should and should not share data.
2.3.4	Staff awareness - Data sharing questions (Q10) …. If I have a question about sharing data lawfully and securely I know where to seek help.
2.3.5	Staff awareness - Personal responsibility (Q11)…. I take personal responsibility for handling data securely.
3.1.1	A data security and protection training needs analysis has been completed.
3.1.2	Date of last data security and protection training needs analysis.
3.1.3	Training Needs analysis has been approved by the person with overall responsibility for data security.
3.2.1	Staff awareness - Training (Q12) … The data security training offered by my organisation supports me in understanding how to use data lawfully and securely.
3.3.1	Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training.
3.3.2	Average mark of first attempt of Level 1 Training.
3.4.1	Number of staff assessed as needing role specialist training.
3.4.2	Number of staff completing advanced Data Security Training.

3.4.3	Details of any Other data security and protection specialist training undertaken .
3.5.1	SIRO and Caldicott Guardian have received appropriate Training.
4.1.1	The organisation maintains a current record of staff and their roles.
4.1.2	For each system holding personal and confidential data, the organisation understands who has access to the information.
4.2.1	Date last audit of user accounts held.
4.2.2	List of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.
4.2.3	Staff awareness - Access to information (Q13): The level of access I have to IT systems holding sensitive information, is appropriate.
4.3.1	All system administrators have signed an agreement which holds them accountable to the highest standards of use.
4.3.2	The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel.
4.3.3	Acceptable IT usage banner displayed to all staff when logging into system, including a personal accountability reminder.
4.3.4	List of all systems to which users and administrators have an account, plus the means of monitoring access.
4.3.5	Staff have provided explicit understanding that their activity of systems can be monitored.
5.1.1	Dates of process reviews held to identify and manage problem processes which cause security breaches.
5.1.2	List of actions arising from the process review, with names of actionees.
5.2.1	Scanned copy of the process review meeting registration sheet with attendee signatures and roles held.
5.3.1	Explain how the actions to address problem processes are being monitored and assurance given to the person with overall responsibility for data security.
6.1.1	A data security and protection breach reporting system is in place.
6.1.2	List routes available for staff to report data security and protection breaches and near misses.
6.1.3	List of all data security breach reports in the last twelve months with action plans.
6.1.4	The person with overall responsibility for data security is notified of the action plan for all data security breaches.
6.1.5	Individuals affected by a breach are appropriately informed.
6.2.1	Number of security and personal information breaches recorded.

6.2.2	Speed of data security and protection breach reporting.
6.2.3	Staff awareness - Reporting (Q14) - I know how to report a data security breach.
6.2.4	Number of breaches that have been reported to the Information Commissioner
6.3.1	Name of anti-virus product.
6.3.2	Number of alerts recorded by the AV tool in the last three months.
6.3.3	Name of spam email filtering product.
6.3.4	Number of spam emails blocked per month.
6.3.5	Number of phishing emails reported by staff per month.
6.4.1	Number and details of incidents caused by a known vulnerability being exploited.
6.4.2	Have you had any repeat data security incidents of the same issue within the organisation.
6.4.3	Staff awareness - Incidents (Q 15) - When there is a data security incident my organisation works quickly to address it.
6.4.4	Staff awareness - Learning Lessons (Q16) - When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again.
7.1.1	There is an incident management and business continuity plan in place for data security and protection.
7.1.2	The incident plan has been approved by the person with overall responsibility for data security.
7.1.3	Staff awareness - Contingency plan (Q17) - If a data security incident was to prevent technology from working in my organisation, I know how to continue doing the critical parts of my job.
7.2.1	Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held.
7.2.3	From the business continuity exercise which issues and actions were documented, with names of actionees listed against each item.
7.2.4	All emergency contacts are kept securely, in hardcopy and are up-to-date.
7.2.5	Location of hardcopy of emergency contacts.
7.2.6	Date emergency contact list updated.
7.2.7	Date emergency contact list printed/shared.
7.2.10	Document any re-defined processes to respond to common forms of cyber attack in the last twelve months.
8.1.1	What software do you use?
8.2.1	List of unsupported software prioritised according to business risk, with remediation

	plan against each item.
8.2.2	Where it is not possible to upgrade/update software, reasons are given.
8.2.3	The person with overall responsibility for data security confirms that the risks of using unsupported systems are being treated or tolerated.
8.3.1	Provide your strategy for security updates.
8.3.2	How regularly do you apply security updates to desktop infrastructure.
8.3.3	How often, in days, is automatic patching typically being pushed out to remote endpoints?
8.3.4	How many times, in the last twelve months has the person with overall responsibility for data security been notified where patches have not been applied for longer than two months, with reasons why?
8.3.5	List of where software updates have not been applied for longer than two months, with reasons why.
9.1.1	The person with overall responsibility for IT infrastructure confirms all networking components have had their default passwords changed.
9.1.2	A Penetration test has been conducted in the last 12 months, which confirmed that all networking components have had their default passwords changed
9.2.1	A penetration test has been conducted in the last 12 months, which confirmed web applications were not vulnerable to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities.
9.2.2	The person with overall responsibility for IT has reviewed the results of latest penetration testing, with action plan against outstanding OWASP findings.
9.3.1	The annual IT penetration testing is scoped in negotiation between the business and the testing team, and uploaded.
9.3.2	The SIRO confirms the scope of the annual IT penetration testing is adequate, and that actions from the previous penetration testing are complete or ongoing (with reasons for non completion).
9.4.1	The person with overall responsibility for data security confirms the organisation has a data security improvement plan.
9.4.2	What are your top three data security and protection risks?
9.4.3	Evidence that your management team has discussed your top three data security and protection risks and what is being done about them?
9.4.4	Date for full implementation of the data security improvement plan.
9.4.5	Data security improvement plan status.
10.1.1	The organisation has a list of its suppliers that handle personal information, the

	products and services they deliver, their contact details and the contract duration.
10.1.2	Contracts with all third parties that handle personal information are compliant with GDPR.
10.2.1	Basic due diligence has been undertaken against each supplier according to ICO guidance.
10.2.4	The person with overall responsibility for data security is assured that suppliers who are Data Processors are prepared for GDPR.
10.3.1	List of data security incidents – past or present – with current suppliers.