NHS
Manchester
Clinical Commissioning Group

Information Governance

IG2 - Information Governance Policy

Version: **4.0**

Document Control Sheet

Title of document:	IG2 – Information Governance Policy		
Supersedes:	IG1 Information Governance Policy, IG3 Confidentiality and Data Protection Policy IG6 Information Security Policy IG7 Email Policy IG18 Encryption Policy IG12 Information Security Spot Checks		
Placement in Organisation:	Information Governance		
Consultation/Stakeholders	Manchester CCG		
Author(s) name:	Shavarnah Purves – Senior Information Governance Officer Chris Upton – Head of IT & IG		
Approved by:	Governance Committee		
Approval date:	November 2018	Review date:	November 2021
Implementation Date:	November 2018		
Implementation Method:	Team briefings/meetings CCG Website		
This document is to be read in conjunction with the following documents: *Records Management Policy* *Acceptable Use Policy*			

Version Control

Version	Date	Brief description of change
V0.1	June 2013	*Amendments to reflect CSU management of CCG Information Governance*
V0.2	August 2013	*Amendments from the Corporate Governance Committee*
V1.0	October 2013	*Corporate Services Team – Information Governance Policies and Procedures Development and Implementation sign off*
V1.1	February 2014	*CSU IG Team reviewed all policies to look at merging some together. These amendments reflect this.*
V2.0	February 2016	*Changes to reflect new IG structure*
V2.1	November 2016	*Changes to reflect new IG Lead and changes in the national NHS IG Training Tool*
V2.2	March 2017	*New NHS Manchester CCG logo*
V3.0	August 2017	*Changes to reflect the new Data Security Awareness Training from NHS Digital*
V4.0	October 2018	*Updated to reflect the changes under GDPR*

PLEASE NOTE: the formally approved copy of this document is held on Manchester CCG's website. Printed copies or electronic saved copies must be checked to ensure they match the current online version.

Contents

Appendices

1.0 Introduction

1.1 This Policy sets out the Information Governance approach in Manchester Clinical Commissioning Group 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 the intended purpose.

2.2 Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service.

1.3 The aims of this document are to ensure that information is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically;
- shared and disclosed appropriately and lawfully.

2.0 Legal Compliance

Manchester CCG regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

The CCG will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including:

- Human Rights Act 1998
- Health and Social Care Act (Safety and Quality) Act 2015
- Common Law Duty of Confidentiality
- Privacy and Electronic Communications (EC Directive) Regulations.

The CCG, when acting as a Controller, will identify and record a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6(1)(e) 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller', the CCG will identify the official authority (legal basis) and record this on relevant records of processing.

3.0 Purpose

3.1 This policy applies to those members of staff directly employed by the CCG and for whom the CCG have a legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations' policies are also applicable whilst undertaking duties for or on behalf of the CCG. This policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

3.2	This policy applies to all forms of information, including but not limited to: • paper and electronic filing systems; • communications, including those sent by post, electronic mail and text messaging; • information that is stored in and/or processed by information systems including servers, personal computers (PCs), any other mobile device; • information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internally or externally to a third party.
4.0	**Responsibilities**
4.1	Overall accountability for procedural documents across the organisation lies with the Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.
4.2	Responsibilities will be given to: • **The Caldicott Guardian who will:** o ensure that the CCG satisfies the highest practical standards for handling patient identifiable information; o act as the conscience of the CCG; o facilitate and enable information sharing and advise on options for lawful and ethical processing of information; o represent and champion IG requirements and issues at Board level; o ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and o oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS. • **The Senior Information Risk owner (SIRO) will:** o be an Executive Board Member; o take overall ownership of the information aspects within the Risk Policy acting as champion for information risk on the Board and provide advice to the Accountable Officer on the content of the CCG's Statement of Internal Control in regard to information risk; o understand the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed; o work with the IG Team to manage the IG risk assessment and management processes within the CCG; o advise their Board on the effectiveness of information risk management across the CCG; o receive training as necessary to ensure they remain effective in their role as SIRO. • **The Data Protection Officer (DPO) will:** o be responsible for ensuring that MHCC complies with all aspects of IG and the GDPR/DPA 2018. At a high level, the DPO is in place to ensure that we can demonstrate compliance with all the requirements of the GDPR. Key components of this include: • monitoring compliance with GDPR/DPA 2018; • providing advice, assistance and recommendations to the SIRO in relation to data protection risks;

- advising on and monitoring Data Protection Impact Assessments (DPIAs);
- being the first contact point for the Information Commissioners Office (ICO) and patients in terms of data processing;
- informing and advising MHCC on its Data Protection obligations.

The DPO role is advisory and is not accountable.

- **Information Asset Owners (IAO) will:**
  - lead and foster a culture that values, protects and uses information for the success of the CCG and benefit of its customers;
  - know what is in the asset and what is linked to it. Have an understanding of how the data flows to and from the asset, know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy;
  - understand and address risks to the asset, providing assurance to the SIRO.

- **Information Governance & IT Lead will:**
  - manage the Senior Information Governance Officers to deliver Information Governance for the CCG;
  - ensure the CCG complies with all legislation and NHS Policy in relation to Data Protection, Freedom of Information, Records Management, Caldicott, Confidentiality and Information Security.
  - understand and address risks to the information assets, providing assurance to their SIRO;

- **The Senior Information Governance Officers will:**
  - supply advice and guidance to all staff on all elements of Information Governance;
  - maintain an awareness of Information Governance issues within the CCG;
  - review and update the Information Governance Policy in line with local and national requirements providing template documents to the CCG;
  - ensure line managers are aware of the requirements of the Information Governance Policy;
  - support the SIRO and Caldicott Guardian;
  - support and monitor the Information Governance training requirements for all CCG staff.

- Line managers will take responsibility for ensuring that the IG Policy is implemented within their group or directorate.

- It is the responsibility of each employee to adhere to the policy.

- Staff will receive instruction and direction regarding the policy from a number of sources:
  - policy/strategy and procedure manuals;
  - line manager;
  - specific training course;
  - other communication methods, for example, team meetings; and
  - staff Intranet.

5.0	**IG Framework**
5.1	The IG Framework will be supported by the Information Governance Policy and other related policies and procedures to cover all aspects of IG, which are aligned with the NHS Operating Framework and the Data Security and Protection Toolkit

requirements:

- Records Management Policy
- Secure Transfers of Information Procedure
- PIA Proforma Procedure
- IG Incident Report Procedure (Appendix of the Incident Reporting Policy)
- Subject Access Policy

In addition, the following policies will be part of the IG suite of policies which will be supported by those framework documents, above.

5.2 The Policy framework will encompass the following:

- Acceptable Use Policy
- Records Management Policy
- Secure Transfer of Information Procedure

6.0 Definitions

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents.

Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Special Categories of Personal Data	Special Categories of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share 2013.

	Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to Manchester CCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

7.0 Requirements

7.1 The CCG will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

Non-confidential information about the CCG and its services will be available to the public through a variety of media.

The CCG will maintain policies to ensure compliance with the Freedom of Information Act. Please refer to the Freedom of Information Policy.

The CCG will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to The CCG Subject Access Policy in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

7.2 **Personnel Information**

In keeping with good Human Resources practice, the CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process special categories of personal data as defined by the Data Protection Act 2018 (DPA)/GDPR for example, in relation to sickness and occupational health records, performance reviews, equal opportunities monitoring and for the prevention of fraud or other illegal activities.

The CCG may process such data and such data may be legitimately disclosed to appropriate employees and to CCG professional advisors, in accordance with the principles of the DPA.

The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/her may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the HR Lead.

8.0 Information Security

8.1 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 following information has been taken from the existing IT policies (Information Security, Email & Encryption) for more detailed information on anything below please refer to these policies which can be found on the staff intranet page.

8.2 **Information Security – Requirements**

The CCG will implement technical and operational standards, policies and processes that align with prevailing standards such as ISO:27001 (Information Security

	Management). The requirements of policy, processes and procedures will be incorporated into the CCG operational procedures and contractual agreements. Information stored and processed by the CCG will be appropriate to business requirements and no information will be stored or processed unnecessarily. The CCG will develop, implement, maintain and test where required, local business continuity plans. Such plans will be a contractual obligation of any relevant supplier. The CCG will ensure that appropriate controls are applied to all types of communication, internal and external, to ensure the communication is secure, appropriate and reaches the intended recipient. The CCG will undertake risk assessments to identify, quantify and prioritise information security risks in accordance with the Risk Assessment Policy. Controls will be selected and implemented to mitigate the risks identified. The CCG will adhere to the NHS Guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under GDPR, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the organisation becomes aware of the incident.
8.3	**Asset Management** All CCG information (electronic and hardcopy), software, computer and communication equipment, will be accounted for and have an owner. The CCG will implement controls that will ensure its assets are appropriately protected. Owners of such assets will be responsible for the maintenance and protection of assets they are assigned.
8.4	**Information Systems Acquisition, Development and Maintenance** The Senior Information Governance Officers should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the SIRO and the Information Asset Owner's (IAO's). All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA and where required, seek review from the IG Team prior to approval or further work.

8.5	**User Access Controls** Only authorised CCG staff or partner organisations, such as the MLCO, are permitted to access CCG computers and the information that is held on them. All staff must have their own unique computer account and only login to systems or applications that they have been granted access to. Access controls must take account of security requirements of the business application and permit access to be granted only on approval by the system administrator in consultation with the appropriate senior manager where there is any concern or doubt. Remote access to the CCG network is protected by strong authentication and passwords. Employees will normally be granted access only to such information that is required to perform their work duties. If they are erroneously granted any other access, then this fact must be reported to their line manager immediately as it may become construed as unauthorised access. Where information is copied between systems within the network, then employees should ensure that any confidential information remains secure and that the recipient system has the same or greater standard of security protection as the sender.
8.6	**Passwords** Only the person to whom a password is issued should use that password and it must not be divulged to anyone else. Any doubts or exceptional circumstances that require disclosure must be referred to the Information Governance Team immediately. If you suspect that your password is known by another user you must change it as soon as possible. If a Systems Administrator is required to do this then it is up to the staff concerned to contact them. Passwords used within the CCG's systems must be a minimum of 6 characters. All staff must change their password when prompted.
8.7	**Encryption** Encryption is the process of converting information using an algorithm to make the information unreadable to anyone except those who have the decryption key. The CCG will ensure all of its electronically held data is adequately protected from loss and inappropriate access. To reduce the risk of unauthorised access the CCG will ensure that the following devices are encrypted by default: • Laptops • Open access Desktops • Handheld devices (where windows OS is used) • Portable storage devices (Memory sticks etc) • Removable media e.g. DVDs and CDs.

	Staff must not bypass, cause to bypass or use tools or software to bypass the encryption software installed on devices. The CCG is also working with clinical system providers to ensure that all GP clinical systems backup tape media are encrypted to the required level. Guidance from the Department of Health and NHS Digital specifies standards for encryption and a national procurement has taken place to provide the products to achieve these standards. The CCG will ensure that all data stored on the above devices will be encrypted to a minimum of AES 256bit encryption. The software, processes and procedures to allow this are being implemented throughout the CCG via GM Shared Service IT Department.
8.8	**Anti-Virus** Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, Trojans and worms. Virus threats are a day to day threat, however the type, strain, and the number of incidents may well increase due to the increase in web activity. This can cause serious disruption to both the user and IT Services. • All computers must run anti-virus software which is constantly updated; • Staff must contact the GM Shared Service IT Service Desk if a virus incident is known or suspected.
9.0	**IG and Records Management**
9.1	The Governance Committee will monitor the implementation and on-going management of the IG Management Framework and Data Security and Protection Toolkit requirements. The Governance Committee will be responsible for ensuring that the Records Management Policy is implemented and that the records management system and processes are developed, co-ordinated and monitored. The Records Management Policy can be found on the staff intranet.
10.0	**IG Training**
10.1	All staff whether permanent, temporary or contracted are required to comply with the CCG IG Staff Handbook which stresses the importance of appropriate information handling and incorporates legislation, the common law and best practice requirements. Information Governance is the framework drawing these requirements together therefore it is important that staff receive the appropriate training. The CCG will ensure that all staff receives annual Information Governance training appropriate to their role through the online E-Learning module via Manchester Hospitals Foundation Trust (MFT) E-Learning system on an annual basis. Managers are responsible for monitoring staff compliance. New starters and any temporary, contract or agency staff must also complete the Information Governance Training when beginning their employment and annually thereafter. Where relevant further training and education will be required of staff. Staff will be informed by the Training Needs Analysis.

11.1	**Process for Approval & Ratification**
11.1	The process for approval and ratification detailed in the 'Corporate Document Template and Users Guidelines Policy' will be used.
11.2	The Governance Committee is the committee with delegated authority for the approval and ratification of this document. This will be reviewed every 2 years.
12.0	**Dissemination, Training & Advice**
12.1	Staff will receive instruction and direction regarding the policy from a number of sources: • policy/strategy and procedure manuals; • line manager; • specific training course; • other communication methods (e.g. team brief/team meetings); • staff intranet.
12.2	This policy and a set of procedural document manuals are available on the staff Intranet.
12.3	Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notifications via the staff intranet.
13.0	**Review, Monitoring and Compliance**
13.1	This policy will be monitored through staff awareness and supporting evidence within the Data Security and Protection Toolkit.
13.2	This policy will be reviewed regularly, and in accordance with the following on an as and when required basis: • legislative changes; • good practice guidance; • case law; • significant incidents reported; • new vulnerabilities; • changes to organisational infrastructure.
13.3	**Equality impact assessment** The CCGs aim to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCGs' Legal Equality Duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief. Where relevant further training and education will be required of staff. Staff will be informed of this need when the situation arises. The Equality Impact Assessment has been completed and has identified impact or potential impact as "no impact".

14.0	References
14.1	• Data Protection Act 2018 • The General Data Protection Regulations • The Common Law Duty of Confidentiality • Confidentiality: NHS Code of Practice (Department of Health) • Freedom of Information Act 2000 • Health and Social Care (Safety and Quality) Act 2015 • Caldicott 2 - Information: To share or not to share? 2016 • The Public Interest Disclosure Act 1998 • Human Rights Act 2000 • Regulation of Investigatory Powers Act 2000 • Computer Misuse Act 1990 • Public Records Act 1958

Appendix A – Section 251 Exemption

When CCGs were introduced they were not given the same legal powers to process PCD as Primary Care Trusts were. The Health and Social Care Act (HSCA) 2012 states that only the NHS Digital can receive and process PCD, for secondary use without patient consent.

The North West Data Service for Commissioners Regional Office (DSCRO) currently acts as a regional office for the NHS Digital and are able to process PCD legally.

Controlled Environment for Finance

In light of the information sharing difficulties encountered by CCGs as a result of the HSCA 2012 the Secretary of State introduced an exemption to the Act known as Section 251 to support commissioning activities.

- **Controlled Environment for Finance (CEfF)**

  CCGs can become a Controlled Environment for Finance (CEfF) which allows trained staff to process patient identifiable data for invoice validation purposes subject to certain conditions being met.

  In summary patient identifiable data must not be included on the invoice and should be sent separately to secure email addresses only accessible to the nominated and appropriately trained CEfF staff.

Appendix B - Key Contacts

IG Team – Names and Roles

Chris Upton
Head of Information Governance and IT
christopher.upton@nhs.net

Shavarnah Purves
Senior Information Governance Officer
shavarnah.purves@nhs.net

Aliyah Ashraf
Senior Information Governance Officer
aliyah.ashraf@nhs.net

SIRO
Ed Dyson

Caldicott Guardian
Dr Manisha Kumar

Data Protection Officer
Nick Gomm

Appendix D – Information Governance Training Needs Analysis

Information is an extremely valuable resource and is essential for the delivery of high quality services. Good Information Governance (IG) practices ensure necessary safeguards for the appropriate use of business and Personal Confidential Data (PCD) are in place and managed effectively. These safeguards can be found in the policies and procedures applicable to all staff but of equal importance is the knowledge and awareness each individual maintains of IG to recognise and work within these safeguards.

Therefore it is a mandatory requirement that all staff including permanent, temporary, contractors and agency staff will receive appropriate basic Information Governance Training and to have that training refreshed annually.

While there is a requirement within the new Data Security and Protection Toolkit to annually complete IG training. The importance of this training was also clearly recognised in with recent Caldicott Review 2 which states:

> 'All staff should receive annual basic Information Governance Training appropriate to their role'

The IG training requirement also requires that:

- Basic IG training is provided for all new starters as part of their induction; and
- Additional training is provided to staff in key roles

Basic Mandatory Training

Manchester CCG currently use Manchester University Hospitals Foundation Trust (MFT) E-Learning system.

The training can be accessed via the following link: https://learninghub.mft.nhs.uk/theme/dynamic/login.php.

Your username is your ESR assignment number e.g. 12345678 and you will be asked to change your password when you log on for the first time. From the log in screen you will be able to view all eight of the modules. Simply click on the module title to begin and follow the on-screen instructions.

Additional Training

There are key roles within the organisation for example, Senior Information Risk Officer (SIRO), Information Asset Owner (IAO) as well as specific areas that may handle PCD or other types of key information. These key roles or areas will be required to undertake additional IG training relevant to their role. This additional training is necessary to ensure relevant safeguards are full respected.

Principally, additional training will be delivered via NHS Digitals IG Training Tool as this site has 4 modules covering topics such as:

1. Introduction to security awareness
2. Information and the law
3. Data security - protecting information
4. Breaches and incidents.

The website can be found using the following link: https://nhsdigital.e-lfh.org.uk/Dashboard

To register to access this learning material please click on the link above and select the Register button and complete the requested details. If you already have an account on the e-Learning for Healthcare (e-LfH) site, you can use your existing login details to access the training.

Subject to discussion with the Information Governance Team, additional bespoke sessions can be arranged as required or may be arranged in response to demand.

Departmental Training

To complement the knowledge gained from the e-learning modules and IG range of policies, IG can deliver face to face sessions with each department on an annual basis to support a specific business requirement, including:

- Understanding and application of IG policies and procedures;
- Provision of specific departmental advice and guidance;
- Facilitation of an informal Q&A session.

Work Experience staff

You are still required to complete an IG assessment. Speak to the Senior IG Officer on how best to complete this. The appropriate modules should be completed within the first four weeks of commencing your placement.

Monitoring and Compliance

Organisations are expected to achieve 95% compliance with Information Governance Training (mandatory module). Compliance against the IG training plan will be monitored throughout the year with regular reports provided to managers for staff management and governance purposes. All compliance reports published also form the evidence base for external audits.