Policy Document

Reference: IG07

University Hospitals of North Midlands NHS Trust

Information Governance Management Framework

Version:	**8**
Date Ratified:	**January 2020 by Trust Executive Committee**
Date of Next Review:	**January 2023**
Policy Author:	**Information Governance Manager**
Executive Lead:	**Caldicott Guardian / Medical Director**

Version Control Schedule

Version	Issue Date	Comments
1	January 2005	Policy developed and approved.
2	April 2009	
3	January 2013	Approved by IGSG as part of Information Governance process, List of Policies on p6 corrected, approved using Chairs Action Updated and 4.1 for Compliance reasons, and References. Approved by IGSG.
4	December 2013	Ratified by Quality and Safety Forum. Minor changes: Pg. 7 – removed SHA and CfH. Added in HSCIC. Pg. 8 and 9 – added SIRO and Caldicott Guardian IG training to be competed annually. Pg. 11 – role of clinical audit and support manager added. Pg. 11 – incident reporting added.
5	October 2014	Page 11 – changed clinical audit and compliance support manager job title to information governance facilitator. Page 11 – added contact email address for IG department.
6	January 2015	Policy re-developed in line with IG toolkit requirement 101 which outlines what needs to be in the Framework, and to provide one policy across the Royal Stoke and County Hospital sites.
7	December 2018	Updated to reflect latest legislation, including GDPR and the Data Protection Act. Updated to reflect updates to the Data Security & Protection Toolkit
8	January 2020	Updated for Data Security & Protection Toolkit. Training Needs Analysis (Appendix 1) added. Definitions (Appendix 2) added. Monitoring Table added (Pg. 8) added.

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

CONTENTS **Page**

1. INTRODUCTION

Information plays a key part in the Clinical and Corporate Governance of the Trust. The quality in the provision of services, planning, performance management, assurance and financial management relies upon accurate and available information.

Information Governance (IG) is a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards. It is of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and management accountability are in place to provide a robust framework for the management of information. The Trust's approach to the management of IG and information handling, including the accountability, reporting and assurance arrangements are contained within this document.

The Information Governance Assurance Framework is a national framework of standards which incorporates all statutory, mandatory and best practice requirements. The standards are set out in the Data Security and Protection Toolkit as a road map enabling organisations to plan and implement standards of practice and to measure and report compliance on an annual basis.

The Data Quality Policy (C27) forms a part of the UHNM Data Quality Assurance Framework which sits with the wider Information Governance Assurance Framework. Data Quality Assurance seeks to raise the awareness within the Trust of the importance of high quality information used for patient services, reporting and decision making purposes. The Data Quality Team also acts to improve the quality of information where practicable.

The Trust's performance against these standards is mandated by and reported to the Department of Health and forms part of the assurance processes associated with the Care Quality Commission, Audit Commission, and NHS Digital. The Trust must submit evidence on an annual basis using the Data Security and Protection Toolkit.

The Trust Policies that cover these areas are:

- IG08 Freedom of Information Act Policy
- IG10 Data Protection, Security and Confidentiality Policy
- IG12 Pseudonymisation and Electronic use of PID
- RM01 Risk Management Policy and Strategy
- RM07 Trust Policy for Reporting and Management of Incidents including SIRI and STEIS Reportable Incidents
- RE01 Multidisciplinary Health Records Policy
- RE02 Clinical Photographic and Video Policy
- G11 Corporate Records Management Policy
- IG04 Safe Haven Policy
- IG14 Registration Authority Policy
- IT01 Corporate Policy for Information Security
- IT02 Trust policy for personal information security and acceptable use
- IT09 policy for disposal of Trust hardware
- C27 Data Quality Policy

It is a requirement for all NHS Chief Executive Officers to sign an Annual Governance Statement (AGS) as part of the statutory accounts and annual report. The AGS is evidence that the Chief Executive as the Accounting Officer has maintained a sound system of internal control, sufficient to support the organisation in achieving its aims and objectives. The Trust is committed to the provision of high quality services in environments that are safe for patients, staff and visitors alike.

The purpose of this document is to provide a statement on the use and management of the information in the Trust and to describe arrangements for providing assurance to the Trust Board that IG standards are defined and met and IG incidents are managed appropriately.

An “Equality Impact Assessment” has been completed and no actual or potential discriminatory impact has been identified relating to this document.

2. SCOPE

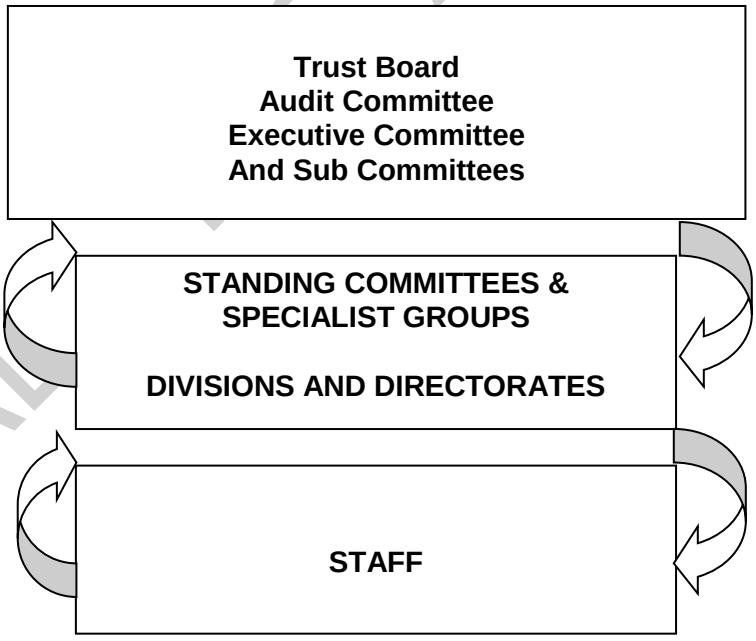
The Trust is committed to compliance with the Data Security and Protection assertions.

The Trust recognises, in the management of and use of all information, the need to facilitate, manage, and achieve an appropriate balance between confidentiality and openness. The Trust fully supports the standards of information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, any personal information relating to both patients and staff and to commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Trust believes that accurate, timely, and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes. The aim of this policy is to ensure that an appropriate IG structure exists, which adequately supports the Trust in managing IG related issues.

The Trust also aims to empower all staff to assume responsibility for contributing to effective risk management by setting out a framework that meets the needs of day to day risk management practice and encourages a ‘freedom to act hierarchy’

Freedom to Act Hierarchy



This “Freedom to Act Hierarchy’ ensures that risk assessment takes place throughout the hierarchy; for example individual staff can undertake risk assessment within a Ward or Department; Ward or Departmental heads may undertake assessment for their department. The results of any assessments feed into local action plans or risk reduction programmes, or Directorate/Divisional Risk and Assurance Registers in circumstances where the outcome suggests the need for involvement outside the immediate team.

Information Governance is formed by those elements of law and policy from which applicable IG standards are derived. It encompasses legal requirements, central guidance and best practice in information handling including:

- The common law Duty of Confidentiality
- Data Protection Act 2018/ General Data Protection Regulation (2018)
- Information Security
- Data Quality
- Records Management
- Freedom of Information Act 2000
- National Data Guardian Standards/ Data Security and Protection Toolkit
- The Privacy and Electronic Communications (EC Directive) Regulations 2003

This document provides a high level description of the arrangements in the Trust for developing, implementing and monitoring IG policy and procedure.

This policy applies to all staff regardless of job role. All staff must comply with specific information governance related legal and ethical obligations and therefore must be aware of the related standards which impact within their area.

3. DEFINITIONS

Please see Appendix 2 for definitions.

4. ROLES AND RESPONSIBILITIES

The Trust Board is ultimately responsible for ensuring the Trust meets its legal responsibilities, and for the adoption of internal and external governance requirements. The Quality Assurance Committee will be updated on Information Governance issues via the quarterly Compliance and Effectiveness report.

Chief Executive
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for IG throughout the Trust and is required to provide assurance that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner (SIRO)
The Trust SIRO is responsible to the Chief Executive for IG and acts as an advocate for information risk on the Trust Board.

Caldicott Guardian
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of Personal Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring PID is shared in an appropriate and secure manner.

Data Protection Officer
The Data Protection Officer (DPO) will advise and monitor compliance with the GDPR. They are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the Information Governance agenda. They will also be the first point of contact with the Supervisory Authority – the Information Commissioner's Office.

Head of Data Quality & Clinical Coding
Will work closely with the Information Governance team to provide information quality assurances across all areas of Trust activity. Within this context, the Data Quality Steering Group provides and receives regular reports to and from the Information Governance Steering Group.

Information Asset Owners (IAO)

Designated Information Asset Owners (IAOs) are responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility, are identified and recorded and that controls are in place to mitigate those risks.

Information Asset Administrators (IAA)
Information Asset Owners can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities. IAA ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date. Where an IAA is not in place, this function is carried out wholly by the IAO.

Information Governance Manager
The Trust's Information Governance Manager is responsible for supporting the Data Protection Officer in the implementation of the Trust's IG agenda.

Information Governance Facilitator
The Trust's Information Governance Facilitator is responsible for supporting the Information Governance Manager in the delivery of the IG agenda

Information Governance Steering Group (IGSG)
The Caldicott Guardian and SIRO are the chairs of the Trust's Information Governance Steering Group (IGSG). This group is responsible for overseeing the day to day management of the individual components of the Trust's Information Governance Framework.

Information Security Manager (RA and Privacy)
Provides advice to the Trust, ensuring compliance, and conformance, with local and national requirements, and, generally, on information risk analysis/management incorporating the Privacy Officer role which focuses on ensuring privacy related alerts from electronic systems (e.g. Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary.

All Staff
All staff, via job roles and contracts of employment/professional registrations must comply with specific IG related legal and ethical obligations and therefore must be aware of the related standards which impact within their area of responsibility. Individual staff must ensure that any personal and corporate information, is managed legally, securely, and efficiently in order to assist in the delivery of the best possible care/practice. Staff can email the IG team on infogovUHNM@uhnm.nhs.uk with any IG related queries.

Quality and Safety Forum
The Quality and Safety Forum has responsibility for receiving issues raised and actions taken, to ensure continuous improvements in the quality and safety of the care provided to our patients.

5. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

Information Governance Training is an annual mandatory requirement for all staff employed within the Trust. The Data Security and Protection Toolkit requires a minimum of 95% of staff to be trained in Information Governance. See Appendix 1 for the Trust's Training Needs Analysis.

Fundamental to the success of delivering the framework is developing a positive IG culture within the Trust. All staff utilise information in their day to day work. Awareness and training needs to be provided to everyone to promote this culture.

All staff, whether permanent, temporary or contracted, needs to be aware of their own individual responsibilities of the maintenance of information confidentiality, data protection, security and quality. To support this objective, all staff will receive training on commencement of employment and appropriately for their role on an annual basis.

In addition staff will be notified of changes by email, intranet display and any other mass coverage methods available.

6. INFORMATION GOVERNANCE INCIDENT REPORTING AND MANAGEMENT

A failure in one or more aspects of Information Governance may cause or contribute to an adverse event related to information handling. IG incidents involving loss or unintentional disclosure of sensitive personal data can have a significant impact on the data subjects, attract media interest and damage the reputation of the Trust.

Examples of the types of incidents that should be classified as Information Governance incidents are:

Disclosure or loss/ theft of information
Inappropriate access and/ or modification
Cyber-attacks on IT equipment/ data
Obtaining information by deception
Human error
Inappropriate processes

Staff must report incidents via the Datix system and/or immediately escalate to the IG team where the incident is deemed serious, in line with Trust policy. (Policy No [RM07]) Trust Policy for Reporting and Management of Incidents including SIRI and STEIS Reportable Incidents.

Incidents will be reviewed and investigated as necessary in line with Trust policy (Policy No (RM07) Trust Policy for Reporting and Management of Incidents including SIRI and STEIS Reportable Incidents.

7. MONITORING AND REVIEW ARRANGEMENTS

7.1 Monitoring Arrangements

The Information Governance Steering Group will monitor the implementation of this, and any subsequent revisions.

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Responsible for Receiving
IG Work programme Progress	Bi-Monthly/Quarterly	DS&P Toolkit	Minutes	IG Manager	Information Governance Steering Group
Incident Analysis	Bi-Monthly/Quarterly	Datix	Minutes	DPO/IG Manager	Information Governance Steering Group
DS&P Toolkit Status	Bi-Monthly	DS&P Toolkit	Report	IG Manager	Information Governance Steering Group
DS&P Toolkit Annual Assessment	Annually	DS&P Toolkit	Annually	DPO/SIRO	Information Governance Steering Group
Data Security Awareness Training	Monthly	DS&P Toolkit Stat. & Mand. Monitoring	Compliance Report	IG Manager	Information Governance Steering Group

This policy will be subject to on-going discussions with all relevant managers and departments with a formal annual review being undertaken by the IGSG.

It is recognised that as related legislation or NHS standards are introduced the policy may need to be updated to reflect these minimum requirements.

7.2 Review

This Policy is subject to review when any of the following conditions are met:

- The adoption of the Policy highlights errors or omissions in its content;
- Where other policies/strategies/guidance issued by the Trust conflict with the information contained herein;
- Where the procedural or guidance framework of the NHS evolves/changes such that revision would bring about improvement;
- The review date has elapsed;

8. REFERENCES

Data Protection Act 2018 and General Data Protection Regulation (2018)
The Data Protection Act (DPA) and General data Protection Regulation (GDPR) provide a framework which governs the processing of information that identifies living individuals. It protects the rights and freedoms of living individuals particularly in relation to the processing of personal data processing includes holding, obtaining, recording, using and disclosing of information. This applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, e.g. it also covers staff personnel records.

Human Rights Act 2000
Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, the Article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000
This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000
This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998
This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

Computer Misuse Act 1990
This Act makes it a criminal offence to access any part of a computer system, programme and/or data that a user is not entitled to access. Each organisation will issue each user an individual user id and password which will only be known by the individual they relate to and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of them inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly and may be liable to criminal prosecution under the provisions of the Act.

Access to Health Records Act 1990
This Act gives patient's representatives right of access to deceased patients' manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 2018.

Access to Medical Reports Act 1988
This Act allows those who have had a medical report produced for the purposes of employment and/or insurance to obtain a copy of the content of the report prior to it being disclosed to any potential employer and/or prospective insurance company.

Health & Social Care Act 2001: Section 60
Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. This is intended primarily as a temporary measure until anonymisation measures or appropriate recording of consent can be put in place. Where the powers provided by this legislation are used to support the processing of confidential patient information there will be additional safeguards and restrictions on the use and disclosure of the information. These may differ from case to case and change over time where the process of annual review, required by the legislation, results in more stringent safeguards being applied.

The Privacy and Electronic Communications (EC Directive) Regulations 2003
These Regulations outline privacy rights of individuals in relation to electronic communications. This may be in the form of marketing (calls, emails), or cookies, as an example. These Regulations sit alongside the Data Protection Act (2018) and the General Data Protection Regulation (2018).

APPENDIX 1: TRAINING NEEDS ANALYSIS FOR SPECIALIST IG TRAINING

All Information Governance training is to be completed on an annual basis in line with the Data Security & Protection Toolkit. Completion of specialist training is required for job-specific roles within the Trust and is required to be repeated every 3 years.

The required training is detailed below:

Job Role	Mandatory Training (Annual Requirement)	Specialist Training (Every 3 years)	Access to Records Management (Every 3 years)	Additional Training Compliance (Every 3 years)
SIRO	✓	✓		
Caldicott Guardian	✓	✓		
Data Protection Officer	✓	✓	✓	
Information Asset Owners	✓	✓		✓
Information Asset Assistants	✓	✓		
Information Governance Manager	✓	✓	✓	✓
Information Governance Team	✓	✓	✓	✓
Subject Access Co-ordinators	✓	✓	✓	
All Staff	✓			

APPENDIX 2: DEFINITIONS

Abbreviation	Term	Definition
BCP	Business Continuity Plan	A procedure that is used in the event of an incident to enable the organisation to continue to deliver its critical activities.
DS&P Toolkit	Data Security and Protection Toolkit	This replaced the previous Information Governance Toolkit.
CG	Caldicott Guardian	Holds the responsibility for reflecting staff and patients interests regarding the use of identifiable information and is responsible for ensuring such information is stored, used and shared in an appropriate and secure manner.
ICO	Information Commissioners Office	An independent regulatory body which upholds information rights in the interest of the public.
SIRO	Senior Information Risk Owner	The designated lead who sits on the board with responsibility for the Trust's information risks and provides a focus for the management of information risk at the highest level.
DPA	Data Protection Act	UK comprehensive framework which governs the processing of personal information about living individuals, in accordance with GDPR.
DPO	Data Protection Officer	Advisor for the Trust about its obligations in order to be complaint with GDPR and then monitors this compliance.
DPIA	Data Protection Impact Assessment	A method of identifying and addressing privacy risks in compliance with GDPR.
GDPR	General Data Protection Regulation	A European Union law which on data protection and privacy for all living citizens of the EU and European Economic Area.
IAO	Information Asset Owner	An IAO supports the SIRO and is assigned to each asset; they have the responsibility to complete the risk form, BCDR form and the SLSP form.
PID	Personal Identifiable Data	Items of data concerning an individual, that if used singly or in conjunction with other data items, could lead to the identification of the individual. Data items include (but are not limited to) name, address, photograph/clinical images, telephone and emails contact details
SCD	Special Category Data	Personal data of a more sensitive nature that requires a higher level of protection. This includes (but is not limited to) health, genetic data, biometric data, racial or ethnic origin and religion.
SLSP	System Level Security Policy	This document is a considered and specific view of the range of security policy and management issues relevant to a system and encompass a range of technical, operational and procedural security topics. When completed this gives a robust risk assessment of the Trusts information assets.