North Middlesex University Hospital NHS Trust

Information Governance Management Framework Policy

Policy Number	PO-000290
New or Revised Policy	Revised Policy
Version:	2.1
Published:	02/02/2022
Review Date:	01/11/2024
Expiry Date:	**01/02/2025**
Policy Executive Owner:	Chief Finance Officer (SIRO)
Policy Owner	Chief Information Officer (Deputy SIRO)
Policy Author/s	Head of Information Governance/Data Protection Officer
Ratification Committee	Policy Ratification Group
Date ratified:	01/02/2022
Approval Committee:	Information Governance & Data Protection Steering Group
Date approved:	09/12/2021
Target Audience:	All staff
Linked Policies:	Data Protection Policy Health Records Management Policy Information Security Policy
Key Words:	Information Governance, Data Security, Data Protection, IG, IG Framework
Name of other committees & meetings consulted	IG Working Group
Designation of Individual Staff Members or staff groups consulted	CFO, CIO, CCIO, CNIO, Head of IT, IG Lead, Data Protection Officer

This is a Controlled Document. Staff must refer to the Intranet version of this document to confirm the most up to date version of this policy. If older versions are in circulation, they must be either returned to the author above or destroyed.

Contents

VERSION CONTROL SHEET

Version	Date	Author	Status	Comment
1.2	09/05/2018	Head of IG/Data Protection Officer	Reviewed Draft	For approval by IGSG
2	20/09/2021	Information Governance Service Lead	Reviewed Draft	For Approval by IGDSSG
2.1	09-Dec-2021	IG Team	Ratified	Approved at IG & DP Steering Group

CHANGES & ALTERATIONS TO CURRENT POLICY (For revised policies only)

New Section 1 added;
Sections 7, 8 and 9 added

1. Summary

1.1. Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources throughout North Middlesex University NHS Trust. It plays a key part in clinical governance, service planning and performance management. Information assets must be considered with equal attention as financial and people (workforce) assets.

1.2. It is essential that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management to assure and demonstrate the proactive use of information as determined by legislative acts, statutes, regulatory requirements and best practice.

1.3. Information Governance is a "framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service". It brings together within a singular cohesive framework, the interdependent requirements and standards of practice.

1.4. Information Governance (IG) combines Information Security, Corporate Governance, Records Management and Business Continuity, and the increasing legislative and regulatory requirements relating to all of these, into a single unified management framework.

1.5. Information Governance is not simply a matter of good corporate record housekeeping. Accuracy (integrity) and availability of information is essential for the provision of healthcare (from individuals' clinical safety to Trust-wide operations) and the operation of the whole health and social care system. Good Information Governance can also lead to efficiency gains and make for more effective management of resources.

1.6. The Trust is required to have effective arrangements in place to govern the uses of information and information systems, as set out in NHS Digital's Data Security and Protection Toolkit.

2. Introduction

2.1. Information is a vital for direct clinical care (patient safety) and for the efficient management of services, resources and performance. It is therefore important that an appropriately robust policy framework is in place.

2.2. Information Governance is a "framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service". It brings together within a singular cohesive framework, the interdependent requirements and standards of practice.

2.3. Information Governance (IG) combines Information Security, Corporate Governance, Records Management and Business Continuity, and the increasing legislative and regulatory requirements relating to all of these, into a single unified management framework.

2.4. Information Governance is not simply a matter of good corporate record housekeeping. Accuracy integrity and availability of information is essential for the provision of healthcare (from individuals' clinical safety to Trust-wide operations) and the operation of the whole health and social care system. Good information governance can also lead to efficiency gains and make for more effective management of resources.

2.5. North Middlesex University Hospital (NMUH) is required to have effective arrangements in place to govern the uses of information and information systems, as set out in NHS Digital's Data Security and Protection Toolkit (DSPT).

3. Purpose of the Policy

3.1. The purpose of this document is to provide an overview of the NMUH's approach to information governance; a guide to the procedures in use and details of the information governance structures within the organisation. It relies strongly on a risk-based approach to the identification of Information Assets (IA) and ownership of such IAs by accountable Information Asset Owners (IAO) through a robust IA Management (IAM) programme.

3.2. To ensure this is undertaken effectively for all its patients and staff, the Trust has this policy, based on Department of Health (DH) guidelines and data protection related law. The UK General Data Protection Regulation – GDPR (now known as UK GDPR) has been implemented into UK law, with some adaptations, in the Data Protection Act 2018 (DPA18).

3.3. The overarching NHS framework is outlined in the Data Security and Protection Toolkit (DSPT). DSPT is an online tool that enables Health & Social Care and other organisations to measure their performance against data security and information governance requirements which reflect legal rules and Department of Health policy. The Toolkit has been developed in response to The NDG Review (Review of Data Security, Consent and Opt-Outs) published in July 2016 and the government response published in July 2017.

3.4. The Care Quality Commission's remit also includes significant elements of information governance, particularly in the areas of patient confidentiality and consent for use of information, transparency, working with other care providers and records management. From 2018 CQC works in partnership with NHS Digital to review the DSPT.

3.5. All policies are available to staff on the Trust Policy Hub and all staff are responsible for ensuring that they are familiar with policy content (to know where to obtain information where needed) and ensuring that individuals in their management responsibility (line management, contract management etc.) are also aware of the policies.

3.6. In its management of PCD (Personal Confidential Data), the Trust complies with UK GDPR and Caldicott Principles. PCD must be processed in line with six data protection principles:

1. Fairly, lawfully and transparently.
2. For specified purposes.
3. Using the minimum amount necessary.
4. Accurately.
5. For only as long as it is needed.
6. Securely.[1]
7. Accountability

[1] General Data Protection Regulation, Article 5(2) (a-f).

A seventh principle applies to Trusts and all individuals who are acting or working on behalf of a Trust.

Note: individuals acting in a personal capacity are not required to comply with data protection law, specifically, although other privacy law may apply in some circumstances.

Individuals (known as 'data subjects') have rights under the new legislation to:

a. Information about how their information is being processed. The Trust addresses this by ensuring a layered approach to informing data subjects how their information is used, including website notice(s), posters, pamphlets and service-level leaflets.

b. Access to their information.

c. Rectification when information is factually incorrect. Any request for rectification will be assessed on a case-by-case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

d. Erasure of information ("Right to be forgotten") - when it is appropriate. In healthcare information needs to be retained for care and medico-legal purposes, rendering this right largely exempt. Any request to be forgotten will be assessed on a case-by-case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

e. Restrict processing. Data Subjects may request that the Trust hold only sufficient Personal Data about them, but not process it any further. Any request for restriction of processing will be assessed on a case-by-case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

f. Data portability. This allows Data Subjects to obtain and reuse their information across different services. In healthcare there are not expected to be many requests, as much information is available as a SAR (Subject Access Request). Any request for portability of data will be assessed on a case-by-case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

g. Object to processing. This allows the Data Subject to object if they do not believe the use of their information is legitimate. Any request to object will be assessed on a case-by-case basis using the precedent of the Trust's developing experience of the new legislation, along with relevant case law.

h. Appropriate decision-making. The Trust is required to demonstrate that it has a lawful basis to carry out profiling and / or automated decision-making. This is undertaken by an annual Trust-wide assessment, led by the IG Team with essential support from IAOs.

All requests from Data Subjects to exercise their rights must be considered: other legislative requirements may mean that they cannot be met. Requests must normally be responded to within 30 days, unless there are extenuating circumstances, in which case there are some rights to extension under the legislation.

In the NHS, the Caldicott Principles are equally as important; when using PCD:

1. Justify the purpose(s).
2. Use confidential information only when it is necessary.
3. Use the minimum necessary.
4. Access should be on a strict need to know basis.
5. Everyone with access to information be aware of their responsibilities.
6. Comply with the law.

7. The duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is used.

Information Governance encompasses the following:

- Data Protection & Confidentiality
- Information Security
- Data Quality
- Records Management

4. Scope

This policy applies to and must be adhered to by all individuals working in North Middlesex University Hospital NHS Trust (NMUH) regardless of grade or profession, including all directly employed staff, bank, agency, contractors and locum employees, non-medical employees and internal appointments, seconded staff, volunteers and any other iteration of personnel that could legitimately be considered staff. Its application is to any individual whose personal data is in the Trust's records systems (patients and former patients, staff and former staff, staff at partner Trusts, general public, etc.).

All Trusts that have access to NHS patient data must provide assurances that they are practising good information governance and use the Data Protection and Security Toolkit (DSPT) to evidence this. Where services are commissioned for NHS patients, the commissioner is required to obtain this assurance from the provider Trust and this requirement is set out in the commissioner-provider contract. The DSPT may be reviewed by the CQC.

The Trust is not a competent authority for the purposes of the Network & Information Security Regulations 2018: these apply primarily to government departments and national bodies.

5. Duties within the organisation

5.1. **The Trust Board**

The Board is ultimately responsible for ensuring that IG is effectively managed and that the IG and Data Protection Officer functions are resourced.

The Finance and Performance Committee receives an annual report on information governance and considers reports from the internal audit on the assurances relied upon to manage information risk.

5.2. **The Chief Executive** is the Accountable Officer has overall responsibility for information governance and provides appropriate assurance through the governance statement in the annual report that information risks are effectively managed and mitigated.

5.3. The **Senior Information Risk Owner**

The SIRO is a director-level member of staff or member of the Senior Management Board with overall responsibility for the organisation's Information Risk Management. The SIRO also leads and implements the IG risk assessment and advises the Board on the effectiveness of IRM across the organisation. The Trust's SIRO is the Chief Finance Officer.

5.4. **The Caldicott Guardian**

The Caldicott Guardian is the person within the organisation with advisory responsibility for safeguarding the confidentiality of patient information and ensuring it is shared ethically, appropriately and securely. The Caldicott Guardian is supported by the IG Team. The Trust's Caldicott Guardian is the Departmental Lead for Quality Improvement in Care of the Elderly.

5.5. **The Chief Information Officer** oversees and is accountable for the operation of the information technology, information governance and informatics departments.

5.6. **The Information Governance Lead (Head of Information Governance)** has the leadership function information governance is responsible for day-to-day management of information governance and coordinates Trust's overall information risk approach and produces an annual information governance report. This includes ensuring that the organisation is fully compliant with all IG related legislation and that the Trust meets statutory and mandatory obligations for IG through development of strategy and implementation of IG policies.

The Information Governance Lead together with members of the IG Team provide advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle PCD.

The Information Governance Lead is also **the Data Protection Officer** and provides professional advice on the application of the UK General Data Protection Regulations and Data Protection Act 2018 and the Freedom of Information Act 2000.

5.7. **The Data Protection Officer**
The Data Protection Officer (DPO) is responsible for providing standards for data protection compliance and associated activities. The DPO function is independent and currently provided by an external managed service.

5.8. **Information Asset Owners**
Information Asset Owners (IAO) are responsible for the management of information held in their team including who has access to sensitive information. They understand and address risk to the information assets they own and escalate issues as required to the Information Governance Lead and the SIRO. They provide assurance to the SIRO on their security and use, including the creation of System Level Security Policies. The IG Team support the IAOs in fulfilling their role

5.9. **The Operational Lead for Health Records** is responsible for ensuring a planned approach to records management across the Trust and co-ordinates the work to the health records team and the media conversion project.

5.10. **The Health Records Manager** is responsible for day-to-day management of the case note library responsible for the operational delivery of the Health Records service and managing the case note library.

5.11. **The information Security Lead** is a role that provides advice on all aspects of Information Security (InfoSec). Their assessment of InfoSec risks, threats and advice on controls **contributes** significantly to the effectiveness of the Trust's InfoSec. The role holder is required to hold a formal InfoSec qualification.

5.12. **Information Governance and Data Security Steering Group (IGDSSG)**
The IGDSSG has representatives from across the Trust and is responsible for overseeing the implementation of the Information Governance Policy and Management Framework and the annual Data security and Protection Toolkit (DSPT). The group also reviews IG-related documentation. The Group reports to the Finance and Performance Committee.

5.13. **Directors, Managers and Supervisors**
All managers have a responsibility to promote this policy and enable good IG practice within their areas. They must promote that national and local IG standard are upheld within their department and advising all staff of their InfoSec, confidentiality and data quality responsibilities and supporting planned evaluation / audit of IG tasks, and implementing

necessary actions. They also have a responsibility to liaise with the IG Team where necessary regarding issue and/or incidents of concern.

5.14. **All Staff**

All users are expected to be familiar with this policy, and must adhere to it as they undertake their work duties.

Managers are responsible for ensuring their staff are familiar with the policy and adhere to it and that any data breaches are reported. Managers must use the standards defined within this code to ensure that clinical and business operations within their areas are undertaken in accordance with good practice.

It is a mandatory requirement to complete the Information Governance Induction Training for new starters and the Information Governance Refresher training on an annual basis. This training ensures staff understand their responsibilities in relation to this policy. Additional role-based training may be required for individuals in some roles (e.g. IAOs, project managers).

Non-adherence

A failure to comply, accidentally or deliberately, with this policy may lead to disciplinary action in accordance with the HR disciplinary policy. Activity on Trust IT systems and health records systems is monitored to ensure compliance with this policy.

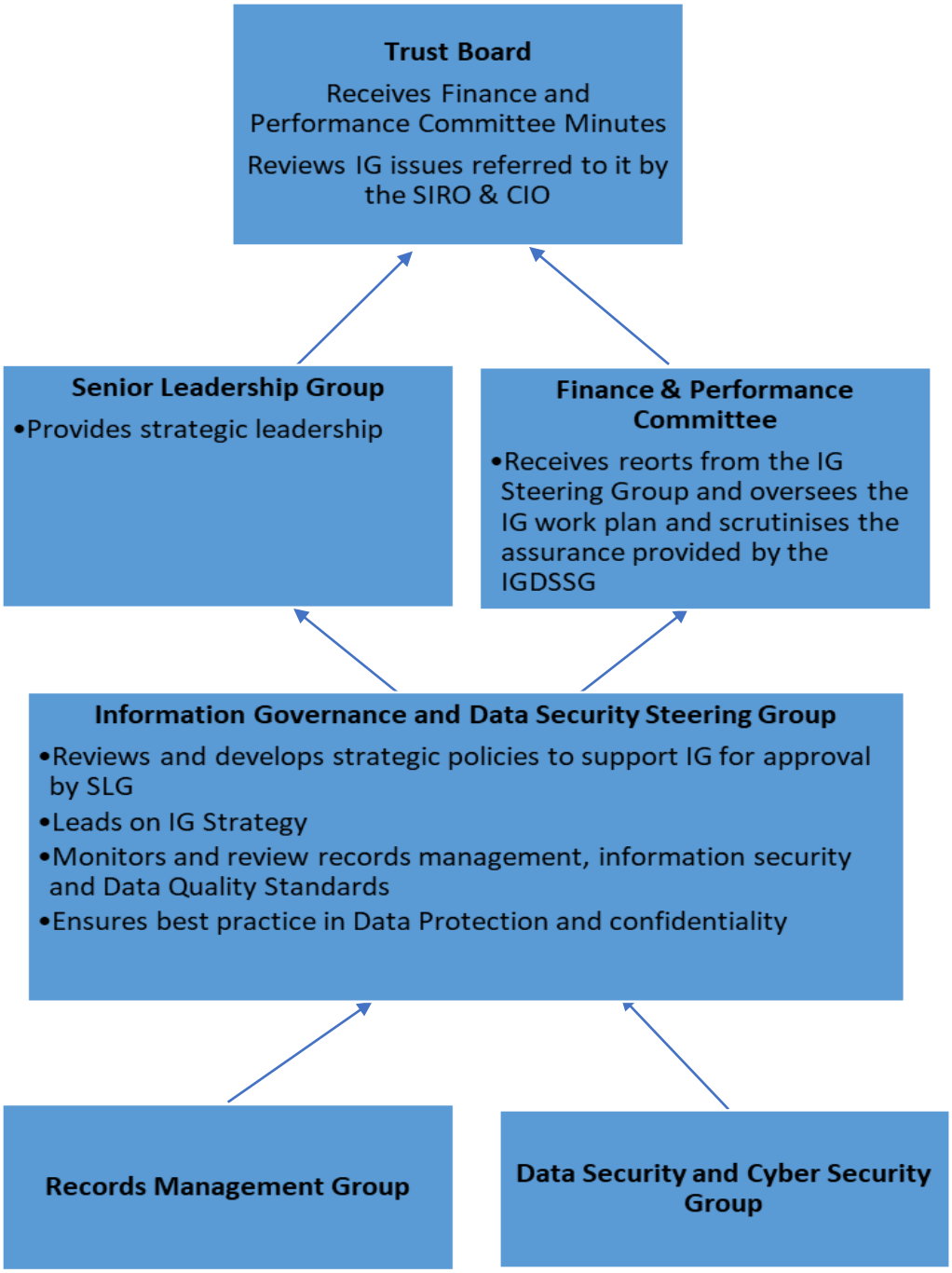
All 3rd party users of Trust systems are expected to adhere to the terms in this policy. Failure to comply may be taken as a breach in contract and as such may be subject to a contract review and/or termination of the contract.

It is understood that some of the standards set out in this policy (and related policies, standards and procedures) might conflict with existing working practices. Where such conflicts exist, these must be reported to the Information Governance Team, in order that an acceptable working practice is agreed and documented in order to manage any associated risk.
With your help and co-operation, we can all contribute to making the Trust a safe and secure working environment. If you have any questions, please ask your line manager in the first instance, or please get in touch via northmid@infogov.nhs.net

Remember:

Everyone is responsible for the security of information assets and the confidentiality of patient and sensitive staff information.

The structure for information governance management at the NMUH is as follows:



6. Definitions

BC	-	Business Continuity
CQC	-	Care Quality Commission
Data Breach	-	A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorised fashion
DFM	-	Data Flow Mapping
DH	-	Department of Health
DPA18	-	Data Protection Act 2018
DPIA	-	Data Protection Impact Assessment
DSPT	-	Data Security and Protection Toolkit
EEA	-	European Economic Area
FOI	-	Freedom of Information Act 2000
UK GDPR	-	UK General Data Protection Regulation
IAM	-	Information Asset Management
IAO	-	Information Asset Owner
IAR	-	Information Asset Register
ICO	-	Information Commissioner's Office
IG	-	Information Governance
InfoSec	-	Information Security
IRM	-	Information Risk Management
DSA	-	Data Sharing Agreement
NHSD	-	NHS Digital
PCD	-	Personal Confidential Data
SIRO	-	Senior Information Risk Owner
Personal Data:	-	Under DP legislation Personal Data is defined as: 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 (formerly 'sensitive' data)	-	Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Direct Care or Individual Care	-	A clinical, social or public health activity concerned with the prevention, investigation. and treatment of illness and the alleviation of suffering of individuals

Secondary Uses or Indirect Care (or other purposes):	"Purposes beyond individual care" refers to all other uses of data outside an individual's care and treatment.

Full information about confidentiality and data protection is in the Trust's Confidentiality & Data Protection Policy, available on the Policy Hub

7. NMUH's approach to Information Governance

The Trust undertakes to implement information governance effectively and will ensure the following:

7.1. Annual Information Governance Audit

The Trust's information governance and data security compliance is measured via a self-assessment against National Data Guardian's standards set out in the DSPT.

The National Data Guardian's 10 standards are:

- Only sharing data for 'lawful and appropriate' reasons.
- Making sure your staff get regular training in data security.
- Only letting people have access to personal information if they need it for their job
- Having a plan for what to do if there's a threat to data security.
- Not using older software that's unsupported – this means it no longer gets technical support from the manufacturer.
- Having a strategy for protecting your IT systems – you must base this on a proven framework like cyber essentials.
- Having contracts with IT suppliers that hold them to account for the way they handle your information and making sure they meet the national data guardian's standards.

7.2. Care Quality Commission (CQC) Oversight

CQC, as outlined in Safe Data, Safe Care (2016) have powers to inspect the Trust's IG as part of its inspection round. To this end the Trust must ensure that robust IG practices are in place. CQC specifically requires that Medical Records are accurate, fit for purpose, held securely and confidentially, and available when required.

7.3. Mandatory Training and Awareness

Fundamental to the success of delivering a robust information governance strategy across the Trust is the development of an information governance awareness culture. Training is provided to all staff to promote this ethos. An annual data security awareness level 1 training is made available to all staff on the eLearning platform - Phoenix and 95% is required. All new staff receive information governance training as part of the corporate induction programme. Trust volunteers are also required to undertake data security awareness level 1 training which is currently offered via e-Learning for Healthcare (e-LfH).

Some roles, such as SIRO, Caldicott Guardian, and IAOs are required to undertake regular training to remain current in their role. All decisions on the need for training will be documented in a Training Needs Analysis, which must be ratified by IGDSSG.

7.4. Confidentiality Code of Conduct

All staff must be aware of their individual responsibilities for the maintenance of confidentiality, DP, InfoSec management and data quality. Staff are given the tools for this through attending annual mandatory information governance training, and all staff receiving a Confidentiality Code of Conduct. Failure to maintain confidentiality may lead to disciplinary action, including dismissal.

7.5. Communicating Confidentiality and Data Protection

Patients and the public are adequately informed about confidentiality and the way their information is used and shared, their rights as data subjects, in particular how they may access their personal data and how they may exercise those rights. Staff have similar rights to be informed and to access their records through internal processes.

The key documents used to provide this information are the privacy notices for patients/public and a separate one for staff, both available from the Trust's external website and intranet.

7.6. Processing Data, the Use of Consent and Information Sharing

It is vital for partner agencies to share care information about patients / service users to ensure provision of co-ordinated and seamless provision of care and services. The Trust recognises the need for this sharing and robust InfoSec to support the implementation of joint working arrangements. The uses and sharing of clinical data can be divided into direct care and secondary care purposes.

7.7. Information Asset Management and Business Continuity

A core information governance objective is that Information Assets (IAs) that use information (personal confidential data) in them are identified and that the business importance of those assets is established.

IAs are those that are central to the efficient running of the Trust and specific departments, e.g. patient, finance, stock control etc. They also include, but are not limited to the following examples:

- Information: System documentation and procedures, archive media and data, including paper and electronic records systems.
- Software: Databases (which may include Excel spread sheets), application programs, systems, development tools and utilities.
- Physical: Infrastructure, equipment, furniture and accommodation used for data processing.
- Services – computing and communications, heating, lighting, power, air conditioning used for data processing.
- People: Qualifications, skills and experience in the use of information systems.
- Intangible: The Trust's reputation.

Essentially, an information asset is information in any format that is of value to an organisation and would be problematic if it were not accessible. Assets may be managed as groups/categories where appropriate.

The Trust has clear lines of accountability for IAM that lead directly to the Board through the SIRO. IAOs are usually senior members of staff who are the nominated owner for one or more of the Organisation's identified IAs, and report for this function to the SIRO.

Within their area of responsibility, it is the IAOs role to log the IAs held, and to ensure this is documented in an IA Register (IAR) and undertake a Data Flow Mapping (DFM) exercise. Collectively these IAM activities are owned by the IAOs, who are accountable for its effective completion.

Whereas it is ideal that all assets are clearly identified on the IAR, the Trust has a risk-based approach that gives priority to IAs that comprise or contain PCD and / or would have the greatest impact on patients, staff, a department and/or the Organisation if they were not available or if personal information within them is breached.

The SIRO has the final decision on approving identified risk mitigation plans. Serious risks must be entered onto the Corporate Risk Register for Board consideration.

IAOs are mandated by the SIRO to receive training, created by the IG Team, to ensure they remain effective in their role.

Data in the IAR includes necessary information to assist in a business Continuity (BC) event. IAOs must ensure that IAM risk assessments are performed at least annually, and that any significant risks to their asset, whether identified in the annual risk assessment or on an ad hoc basis, are reported immediately to the SIRO.

All information and assets associated with information processing facilities must be owned by a designated part of the organisation, for example an Organisation Directorate. The IAO is responsible for ensuring that information and assets associated with information processing facilities are appropriately identified and classified; defining and reviewing access restrictions, classifications, and BC arrangements considering applicable access control policies.

In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as 'services'. In this case the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

The IAO role is especially important where IAs are shared by multiple parts of the Trust.

Each IA and its IAO must have in place regular documented local data quality audits and regular documented data quality spot checks.

All changes to IA, such as system upgrades, should follow an established change control procedure, such as a Data Protection Impact Assessment (DPIA)

IAOs are encouraged, as best practice, to appoint an IA Administrator (IAA) to support them in their role, particularly if they manage a large operational area, to ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, ensure that user records are kept up to date (notification of starters, staff moves and leavers to HR and IT) and ensure that registers, risk assessments, change records etc. are accurate and up-to-date.

Whilst the IG function can support IAOs and IAAs with training and advice, the operational day to day activities sit most appropriately with the service.

7.8. Information Risk Management

The Trust is committed to making the best use of the information it holds to provide efficient healthcare and services to its patients and the local health economy while ensuring that adequate safeguards are in place to keep information secure and to protect Data Subjects' right to privacy.

The Trust recognises that information handling represents a significant corporate risk in those failures to protect information properly or use it appropriately can have a damaging impact on its reputation. Furthermore, failure to protect information adequately can attract the attention of the Information Commissioner's Office (ICO), which regulates data protection and has access to a range of sanctions including significant fines.

IRM complements the Trust's risk management framework. As part of this, information risks are clearly recognised and the appropriate controls implemented through the risk management policy.

Information risk is intrinsic in all administrative and business activities and all staff must continuously manage it. The Trust recognises that the aim of IRM is not to eliminate risk, but to provide the structural means to manage it, by balancing its treatments with anticipated benefits that maybe derived.

The Trust acknowledges that IRM is an essential element of broader Information Governance and InfoSec arrangements and is an integral part of good management practice; it should not be seen as an additional requirement.

The risk management framework is dependent on allocating clear organisational responsibilities, identifying all the IAs, assessing the associated risks and managing any incidents arising from them. This will:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the impact is significant.
- Ensure that clinical and information risk are addressed proportionately (with the balance in favour of minimising clinical risk) and documenting all decisions where reduction in one risk may increase another, adding them to the service risk register for regular review.
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed.
- Encourage proactive rather than reactive risk management.
- Inform decision making throughout the Trust.
- Meet legal and statutory requirements.
- Assist in safeguarding the Trust's IAs.

Information Risk Assessments are performed for all information systems and critical IAs at the following times:

At least annually, as an integral part of the IAM process. Ahead of introducing new systems, applications, facilities, etc. that may impact the assurance of Trust information or systems, using a DPIA. Ahead of agreeing enhancements, upgrades, and conversions associated with critical systems or applications. Those containing or which involve personal information will also require a DPIA. When NHS policy, legislation *or associated guidance requires risk determination, or when that legislation and guidance is changed or updated. When required by the Trust, as directed by the SIRO, Caldicott Guardian or Information Governance Lead and/or the Data Protection Officer.*

Where Risk Assessment is not part of the IAM or DPIA processes, the Trust's standard ICT project delivery approach, may be used, although a DPIA would cover most needs. As in the Trust's overarching Risk Management Policy, any Risk Assessments scoring 12 or above must be entered onto the Corporate Risk Register. For those undertaken as part of the IAM process, every attempt is taken to Treat, Mitigate or Eliminate risks scored as anything other than Green on the Red/Amber/Yellow/Green scoring matrix. Any scoring Red will be considered by the SIRO for addition to the Corporate Risk Register. The DPIA process is intentionally designed to ensure all new / amended processes are introduced with the least possible risk apparent and that risks to information are appropriately considered alongside other organisational risks, with rationales for risk response clearly documented.

7.9. Information Incident Management

Information incident reporting is in line with the Trust's overall risk management incident reporting processes. Additional guidance is drawn from NHS Digital's (NHSD) Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation or subsequent guidance.

Indicators that IRM is being positively enacted include, but are not limited to successful completion of the DSPT and there having been no involvement from the ICO as a result of significant confidentiality or data protection breaches.

An annual review will be carried out by the IG Team on behalf of the SIRO and reported to IGDSSG or other suitable management route. Overall responsibility for action plans lies with the SIRO, to be completed by relevant IAO and monitored by the IG Team.

7.10. Caldicott Guardian

The Caldicott Guardian and the "conscience" of the Trust, providing the focus for patient confidentiality and information sharing issues and advising on the options for the lawful and ethical processing of information as required; ensuring that the Trust complies with the seven Caldicott principles.

7.11. Data Security

ISO27001:2013, the International Standard on Information Security defines the concept as the 'Preservation of confidentiality, integrity and availability of information', adding that other properties are involved, such as authenticity, accountability, non-repudiation and reliability.

The Trust's information security management system (ISMS) is as promoted in the Information Security Code of Practice, based on ISO 270001, providing a comprehensive and coherent approach to identify and manage IAs, whether electronic or manual. There is significant parity between DSPT and ISO27001.

The Trust will protect personal data held in its information systems through compliance with the Department of Health Information Security Code of Practice and the additional information security guidance subsequently provides: National Data Guardian reports, cyber essentials standards and the Data Security and Protection assertions.
The SIRO ensures that individuals have sufficient skills and access to knowledge to perform their roles, that there are procedures to ensure all access profiles are issued appropriately and that IT equipment meets current specifications, is adequately maintained, subject to BC and contingency planning needs, and are securely stored.

Information security management is managed by the IT Team, supported by the IG Team.

7.12. Transfers of Personal Information outside the European Economic Area (EEA)

All transfers of PCD to countries outside the EEA must be for a lawful and justified purpose and authorised following a risk assessment by the Caldicott Guardian, who must be satisfied that there are adequate safeguards in place. A log of such transfers shall be maintained.

7.13. Third Party Contracts

Third party organisations are frequently contracted to undertake tasks and services on behalf of the Trust. Contracts or sharing agreements must be in place for any activity where third parties have access to patients, their PCD, or staff PCD on behalf of the Trust.

Sharing agreements may also be in place with other health and social care Trusts to ensure continuity and quality of patient care. It is possible that as a result of access to Information Assets, third party staff may have significant access to patient or staff PCD. DPIAs must be undertaken before any contract or agreement is signed and/or any third-party access to systems granted. Note: sharing arrangements are already in place for local GP practices and NHS providers.

It is the joint responsibility of the Procurement team and contract manager to ensure that the information governance function is consulted to review contracts and agreements for IG and data protection compliance. This is an NHS national requirement through DSPT (Standard 10).

The most up to date Standard NHS Contract for Procurement of Goods & Services is also fully acceptable in ensuring the requirements are met. Any deviation from that contract must be reviewed for appropriateness by the IG Team. It is particularly important to ensure that the latest version of this contract is used for new contracts and renewals.

The SIRO and IAOs must take all reasonable steps to ensure that third party providers and partners to whom PCD is disclosed comply with their contractual obligations to keep PCD secure and confidential. To provide assurance, third parties may be asked to provide copies of their IG policies.

Directors, managers and supervisors at all levels, and IAOs must ensure that all existing contracts are monitored and reviewed annually to ensure that information governance controls are being adhered to and to resolve problems or unforeseen events.

An accurate register of all third-party contracts must be maintained by the Trust, and is managed by the Finance Team.

Contract managers should ensure that a risk assessment has been carried out prior to entering into agreements with contractors to evaluate the risks to personal information.

Existing contracts should be reviewed annually to ensure that IG controls have been adhered to.

The procurement department will maintain a register of third-party contracts, indicating which contractors have access to personal information and undertake a review to update the contractual clauses to comply with UK GDPR.

7.14. Data Protection Impact Assessments

Data Protection Impact Assessments (DPIA)
Data protection law requires that a DPIA must be undertaken for any project, procurement, business case, transfer of Personal Data or departmental / team initiative where there is a potential impact upon the privacy of individuals.

DPIAs are a Risk Assessment tool to analyse how a particular project or system will affect the privacy of the individuals involved. Projects are not formally defined by the Trust, but must be understood to be part of any business change, including service change plans, proposals, procurement, business case and / or departmental / team initiative that include changes to how personal data is processed as part of the change.

The DPIA process must be integral to conventional project management techniques, and screening must be undertaken from the very earliest stages of the project's initiation at business case and/or pre-feasibility stage.

Data protection and confidentiality law have an over-arching aim of enabling individuals to protect their own information, be informed, and, wherever possible, have choice over how it is used. The Trust's DPIA processes are therefore aligned to DP and Caldicott principles, with specific focus on minimising of harm arising from intrusion into privacy, as defined by those principles.

An effective DPIA allows the Trust to identify and resolve any such problems at an early stage, minimising costs and reputational damage which might otherwise occur.

8. Freedom of Information

The Trust ensures that it complies with the Freedom of Information Act 2000 and the associated Lord Chancellor's Code of Practice. This is set out in the Trust's Freedom of Information Policy.

9. Information Quality Assurance

The Trust promotes data quality through the use of policies and procedures and training. There are also statutory professional requirements to ensure that data quality is assured at the point of collection. Managers are expected to take ownership of and seek to improve the quality of data collected within their services. The Data Quality IG Group have action plans in place to ensure that data quality improvements are implemented.

Records Management

The Trust manages health records in accordance with the Records Management Code of Practice for Health and Social Care. Corporate records are managed by the relevant corporate team. Patient records are managed by the Health Records Team. The Trust aims to become a paper light organisation and is actively working towards this goal.

10. Dissemination and Implementation

This policy will be communicated to staff through the Trust's communication channels and highlighted at Information Governance training and awareness sessions.
Once approved, it will also be available to all staff on the Trust's internet.

11. Process for Monitoring Compliance and Effectiveness

Frequency	Measurable Policy Objective	Method	Who performs the monitoring	Reported to & Review by	Responsibility for action plans
Monthly	The Trust will achieve compliance with all assertions of the Data Security and Protection Toolkit	Information Governance & Data Security Steering Group Annual internal audit	Information Governance & Data Security Steering Group	Finance & Performance Committee	Information Governance Service Lead, CBU managers and corporate heads of departments.

The Trust's declaration with the Data Protection and Security Toolkit is audited annually by the Trust's internal auditors.

Data Quality and Health Records management are audited internally. All audit reports will be reviewed at the IGDSSG and the Finance and Performance Committee who also oversees the implementation of recommended actions.

12. References

Data Security and Protection Toolkit
UK General Data Protection Regulations

13. Associated documentation

Policies and procedures in use at the NMUH

- Data Protection Policy
- Information Risk Management Policy – includes the incident management procedure
- Information Sharing Policy
- Information Security Policy
- Health Records Management Policy
- Email usage and internet policy
- Mobile Device and Mobile device e-mail policy
- Pseudonymisation and Safe Haven Policy
- Encryption policy
- Introduction and upgrade of IT systems policy
- Electronic patients' records policy
- Remote access policy
- Registration authority policy
- Subject Access Requests Policy
- Freedom of Information Policy
- Data Quality Policy
- Freedom of Information Policy

Appendices

Appendix 1- Equality Analysis

Equality analysis is an evidence-based approach which enables the Trust to have **due regard** to the need to eliminate discrimination, advance equality of opportunity and foster good relations, as required by the Public Sector Equality Duty (Section 149 of the Equality Act 2010).

Equality analysis involves gathering and analysing evidence to determine the possible impact of proposed policies, procedures and practices on different groups protected from discrimination by the Equality Act 2010 and then using such evidence to inform action to maximize positive impact and remove or minimize negative impact.

Equality analysis is required when:

- Developing a new policy or procedure
- Amending or reviewing an existing policy or procedure
- Commissioning a new service
- Reviewing delivery of a service

Equality analysis should be a meaningful exercise not a tick box process. Evidence of how the trust has had due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations can be requested to be made public.

In advance of implementing a policy please complete this template:

Division/Department:	Information Governance
Name of person completing the equality analysis	
Date of Equality Analysis:	

What is the aim of this policy or procedure?	This document sets out the framework for implementation of Information Governance within NMUH
Who will be affected by this policy or procedure? e.g., staff, patients, carers etc	Primarily staff
Is the policy/procedure being developed or reviewed?	Reviewed

Could this policy or procedure affect people differently because of:	Yes/No	Is the difference likely to be positive or negative? Please explain why	What evidence sources have you used to make this assessment?* Say if you have not used any evidence sources**
Age	No		
Disability	No		
Gender Reassignment	No		
Marriage/Civil Partnership	No		
Pregnancy / Maternity	No		
Race	No		
Religion or belief	No		
Sex	No		
Sexual Orientation	No		

* E.g. patient/staff surveys; patient/staff demographics; research (Local/national); borough/STP data; consultation exercises, management reports etc

** a lack of evidence should not be taken as a reason for stating that there is no impact on equality

Where you have indicated there is a negative impact on any group, could this be potentially discriminatory? * **	**No** If yes, could any discriminatory impact be objectively justified ****?
Where negative impact has been identified please say what action you will take to remove or mitigate this? Consider who will do this, by when and what the review arrangements there will be	**N/A**

***** If you have identified a potential discriminatory impact of this policy/procedure please contact the Associate Director of Equality, Diversity & Inclusion or the Deputy Director Human Resources for advice.**

**** Is this a 'proportionate means of achieving a legitimate aim?' (cost alone is not sufficient justification)

Appendix 2 - Patient Safety Impact Assessment Tool

Division: Information Governance	
Policy/Strategy/Service redesign: Information Governance Framework Policy	
Lead: Keith James, Information Governance Service Lead	
Date of Assessment:	
Review Date: 08/05/2021	
Patient Safety Domains	**Impact of Policy, Strategy or Service Redesign on Patient Safety (Positive or Negative)**
Mortality	**N/A**
Patient Experience	**Positive as robust information governance will enhance availability and security of patient records**
Staffing Levels	**N/A**
Quality of Service	**Positive. Better patient service, better outcome for Trust objectives and reporting to regulators**
What has been done to promote patient safety in this piece of work? The promotion of good information management practices ensures that patient related information is up-to-date, accurate, available when required by clinicians.	
Signature:	
Date:	

Appendix 3 – Ratification Checklist (For new policies only)

	Title of document being reviewed:	Yes/No	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is it clear that the relevant people/groups have been involved in the development of the document?	Yes	
	Are people involved in the development?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
5.	**Evidence Base**		
	Are key references cited in full?	N/A	
	Are supporting documents referenced?	N/A	
6.	**Approval**		
	Does the document identify which committee/ group will approve it prior to ratification by Executive Management Board?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
8.	**Document Control**		
	Does the document identify where it will be held?	Yes	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
	Is there a plan to review or audit compliance	Yes	

	Title of document being reviewed:	Yes/No	Comments
	with the document?		
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for co-coordinating the dissemination, implementation and review of the document?	Yes	

Executive Sponsor Approval			
f you approve the document, please sign and date it and forward to the author. Policies will not be forwarded to Senior Leadership Group for ratification without Executive Sponsor Approval			
Name		Date	
Signature			
Executive Management Board Approval			
The Finance Director signature below confirms that this policy was ratified by Senior Leadership Group			
Name		Date	
Signature			