NHS
Midlands and Lancashire
Commissioning Support Unit

Information Governance & Data Security and Protection Policies

October 2021

Consultation and Ratification Schedule	
Document Name:	Information Governance & Data Security and Protection Policies
Policy Number/Version:	6.0
Name of originator/author:	Midlands & Lancashire CSU Information Governance Team
Ratified by:	Integrated Governance Committee
Name of responsible committee:	Information Governance Steering Group
Date issued:	19th October 2021
Review date:	19th October 2023
Date of first issue:	20th November 2014
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of Midlands & Lancashire CSU.
Purpose:	To set out the policy for Information Governance. To detail all staff responsibilities for Information Governance and the possible consequences of not following the guidance.
Action required:	All staff are required to read and sign the declaration at the back of the Staff Code of Conduct. Signing the declaration does not confirm that you are aware of everything but confirms that you have read it and know where to refer back to in the future if required.
Cross Reference:	Information Governance Handbook/Information Governance Staff Code of Conduct
Contact Details (for further information)	Midlands and Lancashire CSU Information Governance Team mlcsu.ig@nhs.net / 01782 872648

DOCUMENT STATUS

This is a controlled document. Whilst this document may be printed, the electronic version posted on the Midlands & Lancashire CSU internet site is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

Version Control

Policy Name: Information Governance & Data Security and Protection Policies			
Version	Valid From	Valid To	Document Path/Name
1.0	20/11/2014	20/11/2015	
2.0	29/07/2015	01/11/2016	
3.0	07/11/2016	07/11/2017	
4.0	26/07/2017	26/07/2018	
5.0	11/09/2018	10/09/2021	
6.0	19/10/2021	19/10/2023	

Document Status			
This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet / internet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet / internet.			
Version	**Date**	**Author**	**Changes**
6.0	19/10/2021	IG Team	Update contents to reflect move from GDPR to UK GDPR following exit from the EU. Update references to NHS Records Management Code of Practice from the 2016 guidance to the 2021 guidance.

Glossary of Terms

Term	Acronym	Definition
Anonymisation		The process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describes remain anonymous.
Business Continuity Plans	BCP	Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver its critical activities at an acceptable defined level.
Caldicott Guardian	CG	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
CareCERT		NHS Digital has developed a Care Computer Emergency Response Team (**CareCERT**). CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.
Clinical Commissioning Group	CCG	They are responsible for commissioning healthcare services in both community and hospital settings.
Commissioning Support Unit	CSU	A Commissioning Support Unit (CSU) is an Organisation. Commissioning Support Units provide Clinical Commissioning Groups with external support, specialist skills and knowledge to support them in their role as commissioners, for example by providing Business intelligence services.
Code of Conduct	CoC	A set of rules to guide behaviour and decisions in a specified situation.
Continuing Healthcare	CHC	CHC is health care provided over an extended period of time for people with long-term needs or disability / people's care needs after hospital treatment has finished.
Common Law		The law derived from decisions of the courts, rather than Acts of Parliament or other legislation.
Care Quality Commission	CQC	This is an organisation funded by the Government to check all hospitals in England to

Term	Acronym	Definition
		make sure they are meeting government standards and to share their findings with the public.
Data Controller	DC	The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	DP	A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Data Protection Act 2018	DPA 2018	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information.
Data Processor Agreement	DPA	The Data Controller has a legal responsibility to ensure that anyone they ask to process personal information on their behalf understands what their role is and what processing they can do. The controller is responsible for assessing that its processor is competent to process personal data in line with the UK GDPR's requirements. This assessment should consider the nature of the processing and the risks to the data subjects. This is because Article 28(1) says a controller must only use a processor that can provide "sufficient guarantees" (in particular in terms of its expert knowledge, resources and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the UK GDPR and protects the rights of individuals.
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with UK GDPR requirements.
Data Protection Officer	DPO	A role with responsibility for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation.
Data Security and Protection Toolkit	DSP Toolkit	The DSP Toolkit is the standard for cyber and data security for healthcare organisations. Organisations measure performance against the National Data Guardian's 10 data security

Term	Acronym	Definition
		standards.
Data Sharing Agreement	DSA	An agreement outlining the information that parties agree to share and the terms under which the sharing will take place.
Data Subject		An identified or identifiable natural person who can be identified by their personal information.
Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities.
United Kingdom General Data Protection Regulation	UK GDPR	"GDPR" means UK GDPR. UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
Information Asset Administrator	IAA	Information Asset Administrators ensure that policies and procedures are followed within their area, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information assets registers are accurate and up to date.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.
Information Assets		Includes operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications.
Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Individual Funding Requests	IFR	An application to fund treatment or service not routinely offered by the NHS.
Key Performance Indicators	KPI's	Targets that performance can be tracked against.

Term	Acronym	Definition
Pseudonymisation		The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Record Lifecycle		Records lifecycle in records management refers to the stages of a records "life span", from its creation to its preservation (in an archive) or disposal.
Senior Information Risk Owner	SIRO	Board member with overall responsibility for: • The Information Governance policy • Providing independent senior board-level accountability and assurance that information risks are addressed • Ensuring that information risks are treated as a priority for business outcomes • Playing a vital role in getting the institution to recognise the value of its information, enabling its optimal effective use.
Subject Access Request	SAR	A subject access request (SAR) is simply a written or verbal request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act.

Table of Contents

Information Governance Policy

Purpose of Policy

This overarching Data Security and Protection or Information Governance policy provides an overview of the organisation's approach to information governance and includes data protection and other related information governance policies, and details about the roles and management responsible for data security and protection in the organisation.

Introduction

Information is the most important asset available to an organisation and therefore all organisations must have robust arrangements for Information Governance (IG) which are reviewed annually and described in the new Data Security and Protection Toolkit (DS&PT).

It is of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

The policies will provide assurance to the MLCSU and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

Through the action of approving the policy and its associated supporting documents, the Board provides an organisational commitment to its staff and the public that information will be handled within the identified framework.

The role of the CSU is to support its client CCGs who commission healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CSU will support CCGs in meeting the objectives prescribed in the NHS Act 2006 and the Health & Social Care Act 2012 and to uphold the NHS Constitution. The policy's objective is to ensure that people who work for the MLCSU understand how to look after the information they need to do their jobs, and to protect this information on behalf of data subjects including patients.

UK General Data Protection Regulation/Data Protection Act 2018

The EU General Data Protection Regulation (GDPR) was approved in 2016 and has become directly applicable as law in the UK since 25th May 2018 and the Data Protection Act 2018 (DPA18) fills in the gaps of the UK GDPR, addressing areas in which flexibility and exemptions are permitted.

The UK GDPR/DPA18 is underpinned by a number of data protection principles which drive compliance.

Principles of the General Data Protection Regulation/Data Protection Act 2018 (UK GDPR/DPA18)

- Lawful, fair and transparent processing – this principle emphasises transparency for all UK data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organisation or what data the organisation has about them, that information needs to be available.

- Purpose limitation – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place. Consider organisations that require forms with 20 data fields, when all they really need is a name, email, address and maybe a phone number. Simply put, this principle says that organisations shouldn't collect any piece of data that doesn't have a specific purpose, and those who do may not be compliant.

- Data minimisation – this principle instructs organisations to ensure the data they capture is adequate, relevant and not excessive. Businesses collect and compile every piece of data possible for various reasons, such as understanding customer buying behaviors and patterns or remarketing based on intelligent analytics. Based on this principle, organisations must be sure that they are only storing the minimum amount of data required for their purpose.

- Accurate and up to date – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing. It may seem like a lot of work, but a conscious effort to maintain accurate customer and employee databases will help prove compliance and hopefully also prove useful to the business.

- Kept for no longer than necessary – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organisations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, organisations should prevent users from saving a copy of a customer list on a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations is a compliance nightmare.

- Appropriate security measures – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organisation that is collecting, and processing data is now solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects. Negligence is no longer an excuse under UK GDPR/DPA18, so organisations must spend an adequate amount of resource to protect the data from those who are negligent or malicious. To achieve compliance, organisations should evaluate how well they are enforcing security policies, utilising dynamic access controls, verifying the identity of those accessing the data and protecting against malware/ransomware.

- Accountability and liability – this principle ensures that organisations can demonstrate compliance. Organisations must be able to demonstrate to the governing bodies that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, organisations must be sure that every step within the UK GDPR strategy is auditable and can be compiled as evidence quickly and efficiently. For example, UK GDPR requires organisations to respond to requests from data subjects regarding what data is available about them. The organisation must be able to promptly remove that data, if desired. Organisations not only need to have a process in place to manage the request, but also need to have a full audit trail to prove that they took the proper actions.

Caldicott Principles

The Caldicott Principles, first introduced in 1997, amended in 2013, and then further amended with an additional Principle in 2020, are guidelines applied widely across the field of health and social care information governance to ensure that people's data is kept safe and used appropriately. Caldicott Guardians support the upholding of these principles at an organisational level.

- Principle 1: Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

- Principle 2: Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

- Principle 3: Use the minimum necessary personal confidential data

Where use of personal confidential data is essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

- Principle 4: Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

- Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

- Principle 6: Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

- Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

- Principle 8: Inform the expectations of patients and service users about how their confidential data is to be used

Patients and service users should not be surprised about how their data is used. Where appropriate they should also be given an accessible way to opt-out of processing.

Appointment of Data Protection Officer

Under UK GDPR/DPA18, Data Protection Officers (DPO's) will be at the heart of this new legal framework for all Health and Social care organisations facilitating compliance with the provisions of the UK GDPR.

it is **mandatory** for data controllers and processors to designate a DPO. It is especially important for organisations to nominate a DPO where it is processing personal and sensitive information on a large scale.

It would also be important to ensure that the DPO contact details are available in accordance with the requirements such as in fair processing notices.

For public authorities, DPO's are also required to have knowledge of administrative rules and procedures of the organisation.

The UK GDPR/DPA18 requires that organisations involve the DPO, "in all issues which relate to the protection of personal data". It is therefore crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection.

In relation to Data Protection Impact Assessments (DPIA), the UK GDPR/DPA18 explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.

Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the DPA18, promote a privacy by design approach and should therefore be standard procedure within an organisation's governance and procurement procedures.

In addition, it is important that the DPO be seen as a discussion partner within the organisation and that they are part of the relevant working groups dealing with data processing activities within the organisation.

Due to the large volume of high-risk sensitive data being processed within the NHS the concept of the Data Protection Officer role is well embedded due to the mandated requirement to comply with the existing Data Protection Act through the Data Security and Protection Toolkit. This means that the roles, tasks and responsibilities are already undertaken within the CSU due to the maturity of Information Governance compliance in the CSU and the wider National Health Service.

Within MLCSU the DPO role has been delegated to the Head of information Governance, which includes compliance responsibility for UK GDPR/DPA18, FOIA and Data Security.

Organisations should continue to ensure that the Head of Information Governance or the designated representative:

- Is invited to participate regularly in meetings of senior and middle management where data processing activities are discussed, for example the IG Steering Committee.
- Are consulted where decisions with data protection implications are taken. All relevant information must be passed on to the IG team in a timely manner to allow them to provide adequate advice.
- The opinion of the IG team should always be given due weight. In case of disagreement, the UK GDPR/DPA18 recommends, as good practice, to document the reasons for not following the DPO or IG team's advice.
- The DPO/IG team must be promptly consulted once a data breach or another incident has occurred, for example when incidents occur.

Resources

The UK GDPR/DPA18 requires that the organisation support the DPO function by providing resources necessary to carry out tasks and access to personal data and processing operations to maintain their expert knowledge, this could be through:

- Active support for the DPO function by senior management at Board Level
- Sufficient time to fulfil their duties
- Adequate support in terms of financial resources, infrastructure and premises
- Official communication of the role and support
- Continuous training to stay up to date within the field of Data Protection

It may also be necessary to set up a DPO team.

Scope

This suite of policies applies to all staff employed or who undertake work/volunteer, for MLCSU.

Responsibilities:

Organisation (Accountable Officer)

Overall accountability for procedural documents across the organisation lies with the MLCSU Managing Director as the CSU Accountable Officer. The Accountable Officer has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

SIRO

MLCSU has appointed the Digital Innovation Director as Senior Information Risk Owner (SIRO), who will:

- Take overall ownership of the organisation's Information Risk Policy.
- Act as champion for information risk on the Board and provide written advice to the Accountable Officer on the content of the organisation's annual governance statement in regard to information risk.
- Understand how the strategic business goals of the CSU and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed.
- Implement and lead the NHS Information Governance Risk Assessment and Management processes within the CSU.
- Advise the Board on the effectiveness of information risk management across the CSU and
- Receive training as necessary to ensure they remain effective in their role as SIRO.

Caldicott Guardian

MLCSU has appointed the Director of Nursing and Urgent Care as Caldicott Guardian, who will:

- Ensure that the CSU satisfies the highest practical standards for handling patient identifiable information.
- Facilitate and enable appropriate information sharing and make decisions on behalf of the CSU following advice on options for lawful and ethical processing of information, in particular in relation to disclosures.
- Represent and champion Information Governance requirements and issues at Board level.

- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff, and
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS

Data Protection Officer

MLCSU has also appointed the Head of Information Governance as the Data Protection Officer (see section above about this role).

Information Asset Owners

Information Asset Owners are accountable for the application of this policy to the information assets that they 'own':

- Lead and foster a culture that values, protects and uses information for the benefit of patients.
- Know what information comprises or is associated with the asset and understands the nature and justification of information flows to and from the asset.
- Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.
- Understand and address risks to the asset and providing assurance to the SIRO.
- Ensure there is a legal basis for processing and for any disclosures, and
- Refer queries about any of the above to the Head of Information Governance.

Information Asset Administrators

The role of Information Asset Administrators is to ensure that policies and procedures are followed within their area, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information assets registers are accurate and up to date.

Head of Information Governance

The Head of Information Governance will:

- Maintain an awareness of information governance issues within the MLCSU.
- Review and update the information governance policy in line with local and national requirements.
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis, and
- Ensure that line managers are aware of the requirements of this policy.

Chief Information Officer

The Chief Information Officer is responsible for:

- The formulation and implementation of IT related policies and the creation of supporting procedures, and ensuring these are embedded within the service developing, implementing and managing robust IT security arrangements in line with best industry practice.
- Effective management and security of the MLCSU IT resources, for example, infrastructure and equipment.
- Developing and implementing a robust IT Disaster Recovery Plan.
- Ensuring that IT security levels required by NHS Statement of Compliance are met.
- Ensuring the maintenance of all firewalls and secure access servers are in place at all times, and.

- Acting as the Information Asset Owner for the IT infrastructure with specific accountability for computer and telephone equipment and services that are operated by corporate and clinical work force, e.g., personal computers, laptops, personal digital assistants and related computing devices, held as an NHS asset.

Line Managers

Line managers will take responsibility for ensuring that these policies are implemented within their department or area of responsibility.

User

It is the responsibility of each employee to adhere to the policies.

All staff must make sure that they use the organisation's IT systems appropriately and in accordance with the IG Handbook/Code of Conduct.

Information Governance Steering Group

MLCSU has established an Information Governance Steering Group to monitor and co-ordinate implementation of the policies, the Data Security and Protection Toolkit requirements and other information related legal obligations.

Information Governance Team

The MLCSU Information Governance Team will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Providing advice and guidance on Information Governance issues to all staff.
- Developing information governance policies and procedures.
- Developing information governance awareness and training programmes for staff.
- Ensuring compliance with UK GDPR/DPA18, Information Security and other information related legislation.
- Providing support to the team who handle freedom of information and subject access requests.
- Providing support to Caldicott Guardian and Senior Information Risk Officer for information governance issues

Information Governance Training

All staff are mandated to undertake Information Governance training on a rolling annual basis. Staff will undertake the MLCSU Information Governance training on-line via ESR.

Data Security and Protection Toolkit

The Data Security and Protection Toolkit (DSP Toolkit) forms part of a framework for assuring that organisations are implementing the ten data security standards and meeting their statutory obligations on data protection and data security recommended in the government's response to the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs and the Care Quality Commission's Review 'Safe Data, Safe Care'.

The ten data security standards apply to all health and care organisations. When considering data security as part of the well-led element of their inspections, the Care Quality Commission (CQC) will look at how organisations are assuring themselves that the steps set out in this document are being taken.

MLCSU, works in partnership with NHS England and consequently, must comply with the requirements. As a professional support provider MLCSU works closely with its CCG clients providing all necessary advice, guidance and support to ensure CCGs comply with these requirements.

Data Security and Protection Requirements – NHS Organisations

Leadership Obligation 1	
People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles	
Data Security Standard 1	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is shared for only lawful and appropriate purposes.
Data Security Standard 2	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
Data Security Standard 3	All staff complete appropriate annual data security training and pass a mandatory test, provided through the DSP Toolkit (or provide similar via in-house training programmes).

Leadership Obligation 2	
Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses	
Data Security Standard 4	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
Data Security Standard 5	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
Data Security Standard 6	Cyber-attacks against services are identified and resisted and security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
Data Security Standard 7	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3	
Technology: Ensure technology is secure and up to date.	
Data Security Standard 8	No unsupported operating systems, software or internet browsers are used within the IT estate.
Data Security Standard 9	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
Data Security Standard 10	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Supporting policies and procedures to meet their information governance, data security and protection obligations and enable the CSU and our client CCGs to fulfil their information governance responsibilities. These policies provide a framework to bring together all the requirements, standards and best practice that apply to the handling of confidential, business sensitive and personal information and include:

- Data Protection
- Data Quality
- Records Management
- Access to Information
- Freedom of Information
- IT/Network Security (Links to IT provider policies)

Policy Review

These policies will be reviewed in 2 years or earlier if required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance.

Data Protection Policy

Introduction

MLCSU needs to collect personal confidential information about people with whom it deals to carry out its business and provide its services for healthcare. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, data of birth, private and confidential information, and sensitive information.

In addition, the CSU may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g., on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with UK GDPR/DPA18.

The lawful and proper treatment of personal information by the CSU is extremely important to the success of our business and to maintain the confidence of our service users and employees. We ensure that personal information is held lawfully and correctly and in line with this policy.

Keeping data subjects informed

We are required to let patients and other data subjects know what Information we collect about them, how we will use it and who we may share it with.

There are a number of methods for achieving this, for example information is posted on our public facing website.

Data quality and reuse

We will seek to maintain standards of information quality and avoid duplication, inaccuracy and inconsistencies across personal information. We will maintain comprehensive records management policies to help avoid excessive retention or premature destruction of personal information.

We will only use personal information where strictly necessary. Wherever it is possible to use anonymised data this will be preferred.

Data subjects' rights

We have a records management policy which ensures that individuals can exercise rights over their own personal data in line with UK GDPR/DPA18. Access to the records of the deceased is also covered under the remit of this policy, though these fall outside of the UK GDPR/DPA18 and are dealt with in line with the Access to Health Records Act 1990 and the Freedom of Information Act 2000.

Record of Processing Activities

As part of its compliance with UK GDPR/DPA18 and to provide assurance to its regulatory bodies we must maintains an internal record of processing activities which includes the following: -

- Purposes of the processing.
- Description of the data processed
- Details of who we send personal data to

- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Description of technical and organisational security measures.

Security

Personal data should be kept secure at all times. We ensure that there are adequate policies and procedures in place to protect against unauthorised access and against loss, destruction and damage.

Data Quality Policy

Introduction

MLCSU is committed to ensuring the quality of its data, to promote effective decision making and patient safety.

High quality information means better patient care and patient safety, and there could be potentially serious consequences if information is not correct and up to date, both for patients and for the CSU and client CCGs.

Management information produced from patient data is essential for the efficient running of the CSU and to maximise utilisation of resources for the benefit of patients and staff. It supports making effective decisions about the deployment of resources, and in demonstrating the value of the services provided by the CSU.

MLCSU requires accurate, timely and relevant data including personal data to support:

- Commissioners to improve patient care
- Effective and efficient continuing health care provision
- Bespoke services on individual funding request management
- Assist commissioners in achieving substantial savings
- Help commissioners deliver more effective, safe patient care
- The delivery of core business objectives including HR management
- The monitoring of activity and performance for internal and external management purposes
- Clinical governance and clinical audit
- Service agreements and contracts
- Healthcare planning
- Accountability
- Compliance with UK Data Protection Act 2018
- Medicines management efficiencies
- To be able to evidence compliance with regulatory requirements
- Support effective decision making with regards to the deployment of resources

The key obligations upon staff to maintain accurate records relate to:

- Department of Health, Information Governance requirements
- Legal – UK GDPR/DPA18
- Care Records Guarantee
- Freedom of Information Act (2000)
- Environmental Information Regulations (2000)
- Access to Health Records Act (1990)
- Contractual (contracts of employment)
- Ethical (Professional codes of practice)
- Policy (Records Management Policy, Information Governance Policy)
- NHS Constitution

MLCSU is committed to ensuring and improving where possible the quality of data it uses for all purposes.

Purpose

The purpose of this policy is to set out what is required by all staff to ensure the quality of data used across the CSU.

Responsibility for data quality rests with the Chief Information Officer.

It is the responsibility of all staff to ensure the information they generate is legible, complete, accurate, relevant, accessible and recorded in a timely manner. The quality of information produced can have a significant impact on the quality of services that we provide.

Data Quality is essential for:

- Efficient delivery of patient care e.g., by ensuring that patients are given appointments and admission dates based on clinical priority and length of waiting time.
- Clinical governance and minimising clinical risk e.g., wrong patient, wrong treatment.
- Management information to enable decisions to be made on the basis of sound information, operational and strategic, local and national.
- Performance measurement against national trends and trends over time, so that we can continually plan improvements for our patients.
- As a foundation on which future investment and strategic decisions will be based.
- To support clinical audit and research and development, with a view to improving patient care in the future

All staff need to be able to rely on the accuracy of the information available to them, to provide timely and effective services regardless of whether they are patient facing or central support functions.

To achieve this, all staff need to understand their responsibilities regarding accurate recording of patient data, whether on a computer system or on paper, e.g., case notes.

Data Quality Standards

The CSU data quality standards are:

Accurate and up to date:

All data must be correct and accurately reflect what happened. Therefore, all reference tables including GPs and postcodes must be updated regularly usually within a month of publication. Every opportunity must be taken to check a patient's demographic details with the patient themselves at every in-patient, out-patient and any associated service in accordance with service area specific Standard Operating Procedures (SOPs) as inaccurate demographics may result in important letters being mislaid, or the incorrect identification of patients. However, it is important to note that the accuracy and timeliness of data does not just relate to patients.

Valid:

Data should be within an agreed format which conforms to recognised national or local standards. Codes must map to national values and wherever possible, computer systems should be programmed to only accept valid entries.

Complete:

Data should be captured in full. All mandatory data items within a data set should be completed and default codes will only be used where appropriate, not as a substitute for real data. The use of mandatory data items on the computer systems is to be encouraged but only where this would not cause undue delay. For key data items which are not mandatory on the computer system, it is vital that a list of records with missing items can be produced, to be actioned later.

Timely:

Data should be collected at the earliest opportunity; recording of timely data is beneficial to the treatment of the patient. All data will be recorded to a deadline which will ensure that it meets national reporting and extract deadlines

Defined and consistent:

The data being collected should be understood by the staff collecting it and data items should be internally consistent. Data definitions should be reflected in procedure documents.

Coverage:

Data will reflect the work of the CSU and not go unrecorded. Spot checks and comparison of data between months can highlight potential areas of data loss. Staff should be cognisant that if something is not recorded there is no auditable proof that something occurred, and as such could be challenged.

Free from duplication and fragmentation:

Patients should not have duplicated or confused patient records, and where possible data should be recorded once, and staff should know exactly where to access the data. Where a duplicate record is created, for example in the event that a record is misplaced, records should be merged once the original is found.

Security and confidentiality:

Data must be stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.

How Data Quality can be improved

MLCSU acknowledges that good quality data can be achieved by careful monitoring and error correction, but it is more effective and efficient for data to be entered correctly first time. To achieve this, good procedures must exist so that staff can be trained and supported in their work.

Information Asset Owners are responsible for ensuring that there are specific policies or procedures in place in relation to all information assets under their control, which set out as a minimum, when the information asset should be used, how it should be used and by whom and how the quality of data recorded will be monitored.

Where appropriate Information Asset Owners must ensure that training is available for staff to use the asset, and that information risks associated with each asset are actively identified, and being mitigated, ensuring that they provide assurance to the SIRO.

Procedures need to be reviewed at least every two years or in response to changes in legislation, best practice etc., to

take account of any changes in national standards and definitions.

Tight version control is essential so that staff in all parts of the CSU are using the same procedures which reflect current data definitions.

Records Management Policy

Introduction

This policy sets out the principles of records management for the CSU and provides a framework for the consistent and effective management of records that is standards based and fully integrated with other information governance initiatives within the CSU.

Records management is necessary to support the business of the CSU and to meet its obligations in terms of legislation and national guidelines.

The policy is based on guidance from the NHSx Records Management Code of Practice 2021 and NHS England's Corporate Records Retention and Disposal Schedule 2019. Which provide guidelines and good practice in managing all types of NHSE records and highlights the responsibilities of all staff for the records they create or use.

MLCSU has a statutory obligation to maintain accurate records of their activities and to make arrangements for their safe keeping and secure disposal. All records created in the course of the business of the MLCSU are public records under the terms of the Public Records Act 1958.

Effective records management is an essential requirement of the obligations of the CSU. It also recognises the importance of good records management practices to ensure:

- The right information is available at the right time.
- Authentic and reliable evidence of business transactions.
- Support for decision making and planning processes.
- Better use of physical and server space.
- Better use of staff time.
- Compliance with legislation and standards.
- Reduced costs.

Purpose and Scope

This policy applies to employees, agents and contractors working for, or supplying services to the CSU.

MLCSU records are part of the organisation's corporate memory, providing the evidence of actions and decisions and representing a vital asset to support daily functions and operations and to:

- provide guidance to staff to carry out their corporate and personal record management responsibilities to support high quality patient care.
- support the organisation and staff in meeting their obligations in terms of legislation and national good practice guidance.
- provide effective governance arrangements for record management, also known as 'information lifecycle management'.

Definitions

Records: Recorded information in any form or medium, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs.

Health Records: records which consists of information relating to the physical or mental health of an individual and has been made by or on behalf of a health professional in connection with that care.

Corporate Records: records which relate to the corporate business of the CSU such as accounts, minutes and meeting papers and legal and other administrative documents. They may contain personal identifiable information, for example personnel files and should be treated with the same degree of care and security as patient/service user records.

Records Management: is a discipline which utilises administrative systems to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CSU and preserving an appropriate historical record.

Records Lifecycle: a period a record exists from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as semi-active or closed records which may be referred to occasionally) and finally either confidential destruction or archival preservation.

Records Management

Records Creation

All records created in the CSU must be created in a manner that ensures that they are clearly identifiable, accessible, and can be retrieved when required.

All records created in the CSU must be authentic, credible, authoritative and adequate for the purposes for which they are kept. They must correctly reflect what was communicated, decided or undertaken.

Adequate records must be created where there is a need to be accountable for decisions, actions, outcomes or processes. For example, the minutes of a meeting, a clinician's examination of a patient, the payment of an account or the appraisal of a member of staff.

Records Use and Maintenance

All staff have a duty for the maintenance and protection of records they use. Only authorised staff should have access to records.

The identification and safeguarding of vital records necessary for business continuity should be included in all business continuity /disaster recovery plans.

Any incidents relating to records, including the unavailability and loss, must be reported as an incident using the CSU incident reporting system.

Accuracy of statements i.e., record keeping standards, should pay particular to stating facts not opinions.

Records Tracking

Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain

is to be located quickly and efficiently. One of the main reasons records are misplaced or lost is that the next destination is not formally recorded.

All services/departments should ensure they have appropriate tracking systems and audit trails in place to monitor the use and movement of records.

Records Transportation

When records are being transported, whether they are electronic or paper, care should be taken to ensure the safe transition to the new location, whether this be temporary or permanent.

Records Storage

Records storage areas must provide storage, which is safe from unauthorised access, but which allows maximum accessibility to the records commensurate to its frequency of use.

The following factors must be taken into account:

- Compliance with Health and Safety and fire prevention regulations.
- Degree of security required.
- User needs.
- Type of records stored.
- Size & quantity of records.
- Usage and frequency of retrievals.
- Ergonomics, space, efficiency and price.

Inactive records sent for storage off-site (Iron Mountain) must be boxed and include a retention date. The Information Asset Owner is responsible for keeping an accurate and up-to-date inventory of all records sent off-site.

Retention

The minimum length of time that a record is retained by the CSU depends on the type of record. The CSU has adopted the minimum retention schedules published in the Records Management Code of Practice for Health and Social Care 2021.

Records, in whatever format they are held, may be retained for longer than the minimum retention periods, but should not normally be kept for more than 30 years.

Requests for extended preservation are subject to approval by the Information Governance Steering Group. This may only happen on grounds of historical archival value, relevance to research or other preserved records.

Information Asset Owners are responsible for determining if a record for which they are accountable should be retained for longer than the minimum retention period. This should be listed in a local retention schedule and communicated to all Information Asset Administrators. Local retention schedules must be approved by the Information Governance Steering Group before implementation.

Disposal and destruction of records

For records that have reached their minimum retention period and there is no justification for continuing to hold them, they should be disposed of appropriately.

Paper records of a confidential nature should either be shredded using a cross shredder to DIN standard 4 or put in confidential waste that is appropriately destroyed by a company contracted to the organisation. Electronic records must be deleted from the device and not simply moved into the Trash folder, known as double deleting.

Access to Information Policy (Subject Access Requests - SAR)

Introduction

All living individuals have the right under the Data Protection legislation (UK GDPR/DPA18), subject to certain exemptions, to have access to their personal records that are held by the CSU. This is known as a 'subject access request' (SAR).

The UK GDPR/DPA18 applies only to living persons but there are limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990

Requests may be received from members of staff, service users or any other individual who the CSU has had dealings with and holds data about that individual.

This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

Anyone making such a requested is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, where the information was gathered from.

Under UK GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or raise and objection to the processing altogether.

UK GDPR/DPA18 changes to SAR

Under UK GDPR/DPA18 the right to make a SAR will be very similar, with the key changes including:

- Abolition of the £10 administration fee (although "reasonable" fees can be charged for an excessive request or for further copies).
- Information must be provided without delay and at the latest within one calendar month of receipt.
- Higher fines for failing to comply. The maximum fine that can be issued by the Information Commissioner (ICO) is 4% of the total annual global turnover or £17.5 million, whichever is higher, and individuals also retain the right to pursue a claim in court.

Scope and Purpose

This policy applies to those members of staff that are directly employed by MLCSU and for whom the CSU has legal responsibility. The policy also applies to all third parties and others authorised to undertake work on behalf of the CSU.

The purpose of this policy is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests.

What is a SAR

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- told whether any personal data is being processed.
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- given a copy of the personal data; and
- given details of the source of the data (where this is available)

Personal data is information that relates to an individual who can be identified either directly or indirectly and includes any expression of opinion about the individual and any indication of the intentions of the information holder or any other person in respect of the individual.

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR, other conditions to consider:

- All clinical data should be reviewed by a clinician and consideration should be given to redacting any information likely to cause serious harm to the mental or physical health of any individual
- Information supplied by third parties e.g., family members should usually be redacted
- Data and information held from other agencies may be disclosable but should be discussed with the originating body first
- Any information subject to Legal Professional Privilege should not be disclosed
- Information should not be disclosed where there is a statutory or court restriction on disclosure e.g., adoption records
- References written for current or former employees are exempt (but not those received from third parties)
- In the case of deceased records, information should not be disclosed where the entry in the records makes it clear that the deceased expected the information to remain confidential
- A personal record may also contain reference to third parties and redaction should be considered by balancing the UK GDPR/DPA18 rights of all parties

Recognising a SAR

A SAR must be made in writing or verbally; however, the requestor does not need to mention UK Data Protection/GDPR or state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 2000, but their request should still be treated according to this policy.

The following are examples of formal subject access requests:

- Please send me a copy of my HR file, or medical records
- I am a solicitor acting on behalf of my client and request a copy of their medical record (an appropriate authority is enclosed)
- The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior police officer

Requests should be dealt with within a maximum of one calendar month under UK GDPR subject to the necessity to seek clarification. It is possible to extend this timescale by a further two calendar months where requests are complex however if this is the case the CSU must inform the individual within one calendar month of the request and explain why the extension is necessary.

NHS best practice recommends disclosure within 21 days where a record has been added to in the last 40 days.

The Common Law Duty of Confidentiality extends beyond death. Certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:

- The patient's personal representative (Executor or Administrator of the deceased's estate)
- Any person who may have a claim arising out of the patient's death

A Next of Kin has no automatic right of access, but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from the Caldicott Guardian in relation to requests for deceased records.

A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Fax
- Post
- Social media
- MLCSU website
- Verbally

Where an individual is unable to make a written request, it is the Department of Health view that in serving the interest of patients it can be made verbally, with the details recorded on the individual's file.

Requests made about or on behalf of other individuals

A third party, e.g., solicitor, may also make a valid SAR on behalf of an individual.

Where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals consent or evidence of a legal right to act on behalf of that individual e.g., power of attorney must be provided by the third party.

Requests on behalf of a child

Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian.

So, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child can be considered competent under Gillick/Fraser guidelines, has the capacity to understand their rights and any implications of the disclosure of information, then child's permission should be sought to action the request.

Further clarification guidance is still awaited in relation to the rights of children under UK GDPR/DPA18.

The Information Commissioner (ICO) has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

The Caldicott Guardian should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that, just because a child has capacity to make a SAR, that they also have the

capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so.

Requests for personal information – Police/HMRC

Requests for personal information may be made by the above authorities for the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders; and
- The assessment or collection of tax or duty.

A formal documented request signed a senior office from the relevant authority is required before proceeding with the request.

The request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

These types of requests must be considered by a senior manager or the SAR team before any decision or action is taken to release information.

Court Orders

All Court Orders requesting personal information about an individual must be complied with.

Subject Access Request Process

Requests for information held about an individual must be directed to the Access to Information team:

To exercise Subject Access rights for the CSU please contact one of the following:

- By telephone – 01782 872648
- By email – mlcsusars@nhs.net
- Postal address – Access to Information Team, NHS Midlands & Lancashire Commissioning Support Unit, Heron House, 120 Grove Road, Fenton, Stoke on Trent, ST4 4LX

The Access to Information team will acknowledge the request and log it and notify the requestor of the next steps. The requestor may be asked to complete an application form to better enable the CSU to locate the relevant information.

It is important that a SAR is identified and sent to the Access to Information team quickly in order for the request to be responded to within one month or receipt.

Responding to requests

A detailed Standing Operating Procedure has been produced which gives full details as to how the CSU responds to an individual SAR. Access to the standard operating procedure is available through the Access to Information team.

It is essential though that a log of all requests received is maintained and includes (as a minimum):

Date received

Date response due (within one calendar month)

Data Subjects details

Applicants' details

Proof of Identification

Information requested

Exemptions applied, if applicable

Details of decisions to disclose information without the data subject's consent (if applicable)

Details of information to be disclosed and the format in which they were supplied

When and how supplied (for example, hard copy and by post)

Performance monitoring

The CSU will ensure that monitoring and evaluation of SAR's takes place on a regular basis. The Access to Information team will provide progress reports to the Information Governance Steering Group and will include following:

- Number of requests
- Incidents/Breaches in response times (detailed exception reports)
- Complaints

Freedom of Information (FOI) Policy

Introduction

The Freedom of Information Act (2000) came into effect for all public authorities in January 2005. Since then, all requests for information have had to be answered in accordance with the Freedom of Information (FOI) Act 2000 or the Environmental Information Regulations 2004 (EIR).

The Freedom of Information Act gives a general right of access to all types of recorded information held by public authorities. Disclosures are subject to the application of relevant exemptions contained within the Act.

Under the Act, MLCSU must consider all requests for recorded information it receives and must:

- Inform the applicant whether the information is held; and
- supply the requested information subject to the application of relevant exemptions contained within the Act

We remain committed to promote a culture of openness and accountability to enable you to have a greater understanding of how we carry out our duties, how we make decisions and how we spend public money.

The FOIA is fully retrospective and covers all information held in a recorded format. The deadline for a public authority to respond to requests made under the Act is 20 working days, although there are some circumstances where this may be extended under the terms of the legislation.

A request for information under the general rights of access must be:

- received in writing (FOI)
- received verbally or in writing (EIR)
- state the name of the applicant and an address for correspondence
- clearly describe the information requested

A request can also be made electronically via email.

Exemptions

The rights within the Act may be limited by applying certain exemptions. Several sections of the Act confer an absolute exemption on information. There are 23 exemptions from the rights of access under the Act. These exemptions mark out the limits of the right of access to information under the Act. Further details about applying exemptions can be obtained from the Access to Information team.

Other sections of the FOI Act direct the CSU to weigh up whether the public interest in maintaining the bar on confirmation/denial or in maintaining the exemption is greater than the public interest in disclosing whether the public authority holds the information, or in disclosing the information at all. In some cases, if an exemption applies the CSU may be obliged to disclose the information if the public interest test outweighs the exemption.

Refusal of requests

MLCSU is obliged to disclose information requested under the Act unless an exemption applies. If the CSU refuses a request, the applicant should be informed, at the same time as notification of the exemption, of the procedure to follow if the requester is not satisfied. This procedure includes an internal review by the CSU, if the requester is not happy with the findings of the internal review, then they should be directed to make a complaint to the ICO. Further details of dealing with FOI refusals should be sought from the Access to Information Team.

If a request is made for information that is subject to a current piece of work and premature disclosure is not deemed in the public interest, then the CSU can withhold the information temporarily. If withheld, then an indication of when the information will be available should be given.

Release of employee names and details

As a public authority, there is a recognised justification for the disclosure of some employee names and contact details. Board members and other staff members whose names are already published on the CSU's website will be released without seeking additional consent.

Those staff with public facing roles will have work contact details routinely released, however, for other staff, consent will normally be sought if release is deemed appropriate. Personal contact details (home address, home telephone number or personal email address) will **never** be released in response to a request under the Act.

Time limits for compliance with requests

The CSU has a statutory obligation to comply with the Freedom of Information Act and has established systems and procedures to ensure that the organisation complies with the Act and to provide the information requested within 20 working days of a request.

Compliance with the 20-day time limit arising from FOI requests is also monitored.

If the CSU chooses to apply an exemption to any information, or it exceeds the appropriate limit for costs of compliance, a notice shall be issued within twenty working days informing the applicant of this decision.

What to do if you receive a request for information

If a member of staff receives a request, it must be passed to the Access to Information Team immediately. Failure to do this may result in a delay in processing the request and complying with the Law.

All requests should be sent to mlcsu.foi@nhs.net

Monitoring and Evaluation

The CSU will ensure that monitoring and evaluation of the implementation of FOI takes place on a regular basis. The Access to Information team will provide progress reports to the Information Governance Steering Group and will include following:

- Number of requests
- Breaches in response times (detailed exception reports)
- Justification of exemptions
- Complaints
- Any requests escalated to the ICO

Network and IT Security Policies

All Network and IT Policies are available on the CSU Staff Portal at: https://csucloudservices.sharepoint.com/SitePages/IT-Policies.aspx

Registration Authority Policy and Procedure

The policy applies to MLCSU, and all organisations supported by MLCSU, who are involved in the use of smartcards when accessing health and social care systems. All users of these systems must be registered to ensure adequate and appropriate safeguards are in place to maintain the confidentiality of patient data. NHS Digital support the delivery of IT infrastructure and facilitate organisations that need access to patient information within National Systems and the NHS Care Records Service (CRS). The only method by which users can access a Spine compliant Application is via a Smartcard and passcode.

The role of the Registration Authority within MLCSU is to ensure that authorised individuals have timely access to health and social care applications and information where they have a legitimate relationship, or justifiable need based upon their role-based access control requirements. It is essential that the NHS Confidentiality Code of Practice is upheld by the Registration Authority providing a robust role-based access control management infrastructure.

An essential part of the role is to verify the identities of the MLCSU and associated organization staff for whom a Registration Authority service is provided. Identities are verified to the NHS Employers' identity check standards. The Care Identity Services are used for verifying and individual's identity and authorizing access rights for NHS Registration Authority systems. Access controls need to be provided to individual user accounts so that staff only have access to the patient information they require to perform their role.

MLCSU provides a service to "child organisations", who must ensure that compliance is maintained with Registration Authority policies by its users. These policies must be embedded in the "child organisations", IG Framework.

MLCSU, as part of its service delivery, will report any non-conformance.

The CSU Information Governance Steering Group will ensure that:

1. The MLCSU Managing Director approves and appoints Registration Authority managers.
2. Periodic reports are provided from the Registration Authority as necessary.
3. It reviews and approves, where necessary, inter organizational agreements.
4. It requires Registration Authority Managers and sponsors to work to the National Registration Authority Policy and within the IG Framework, bound by the Data Security & Protection Toolkit, UK GDPR, Data Protection Act 2018, and the NHS Confidentiality Code of Practice.
5. Registration Authority functions are embedded in the Information Governance Framework to ensure the best interests of patients are reflected in the registration process; and
6. MLCSU nominates a senior manager at MLCSU senior management level for Registration Authority activities.

Child organisations will ensure that:

- Staff will adhere to Registration Authority policies and requirements as set out in the Data Security & Protection Toolkit;

- They nominate a Caldicott Guardian, Privacy officer and sponsors to represent their organization; and
- Registration Authority functions are embedded in the IG Framework to ensure that the best interests of patients are reflected in Registration Authority processes.

Issue of smartcards

Smartcards are considered to be a controlled asset, and these are ordered by the CSU Registration Authority Manager. The smartcards are issued in accordance with the obligations of the NHS Care Record Guarantee published by the Department of Health.

New employees

New employees will only receive a Smartcard if they have been authorised by a recognised Sponsor and their identities meet the requirements laid down in the NHS Employers' identity check standards. The control and issuance of the smartcard assets will fully comply with the requirements of the National Registration Authority Policy and procedures and will be managed by the Registration Authority Team.

Appropriate documentation concerning identity must be provided by the member of staff to the Registration Authority Team before they are issued with a Smartcard.

Existing staff and temporary, agency, contract workers

The requirement for existing staff to be issued with Smartcards will be confirmed by organisational sponsors. All temporary staff will be sponsored, and smartcards issued in the same manner as for new employees.

Management of smartcards

As soon as the Smartcard is no longer required, it shall be the responsibility of the Sponsor to either notify the CSU Registration Authority team or revoke the user's access to the organisation according to the individual organisation process

Record management

All information relating to the verification of identity is to be treated as strictly confidential and used only for the purposes of the Registration Authority.

All records for identity management will be held in accordance with CSU policies and shall be retained for a minimum period of six years after the staff member has left prior to review and thereafter maintaining a summary until the person's 70th Birthday, as in accordance with the NHS Code of Practice on Records Management for Health & Social Care.

Registration Authority documentation must be stored securely at all times and if in paper format kept in a locked and secure area. Access to Registration Authority documentation is on a strict need to know basis and will generally be limited to the Registration Authority Team.