NHS
Leicestershire Partnership
NHS Trust

Information Lifecycle and Records Management Policy

This policy describes mandatory guidance for the policies, processes, practices, services and tools used by the organisation to manage its information through every phase of its existence, from creation through to destruction.

Key Words:	Information, Records, Management, Lifecycle, electronic record, retention, disposal, transit
Version:	6.1
Adopted by:	Trust Policy Committee
Date this version was adopted:	24 August 2022
Name of Author:	Head of Data Privacy/ Data Protection Officer
Name of responsible Committee:	Data Privacy Committee
Please state if there is a reason for not publishing on website:	n/a
Date issued for publication:	August 2022
Review date:	January 2025
Expiry date:	31 October 2025
Target audience:	All LPT Staff

Type of Policy	Clinical √		Non Clinical √
Which Relevant CQC Fundamental Standards?	Regulation 17: Good Governance		

Contents

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
3.0 Draft version	February 2012	Harmonisation of policies as a result of the TCS process
3.1 Final	April 2012	Final Harmonised policy following consultation changes
3.2 Final	February 2013	Amendments incorporated to NHSLA Monitoring section (Appendix 5)
3.3 Final	March 2013	Further amendments incorporated to NHSLA Monitoring Section (Criteria 5.2 added to Appendix 5)
3.4 Draft	November 2013	Review as a result of implementation and NHSLA requirements
3.5 Draft	May 2014	Final amendments following extensive consultation. Issued for approval to Records and Information Governance Group
4	October 2017	Final Draft following review against revised Records Management Code of Practice for Health and Social Care issued 2016
5 Draft	September 2020	Review in line with policy management
6	March 2022	Review following the publication of the Records Management Code of Practice by NHSX December 2021
6.1	July 2025	Ext until Oct 2025 to allow review agreed by KD

For further information contact:
Head of Data Privacy

Email: lpt.dataprivacy@nhs.net

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Due Regard

LPT will ensure that Due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- **Strategies, policies and services are free from discrimination;**
- **LPT complies with current equality legislation;**
- **Due regard is given to equality in decision making and subsequent processes;**
- **Opportunities for promoting equality are identified.**

Please refer to due regard assessment (Appendix 4) of this policy.

Definitions that apply to this Policy

Access	The availability of or permission to consult records
Archiving	The storing of files, records, and other data for reference and alternative backup
Authentic record	A record that can be proven: • To be what it purports to be • To have been created, or sent by the person purported to have created or sent it • To have been created or sent at the time purported
Breach of Confidentiality	The unauthorised disclosure of personal confidential information
Caldicott Guardian	The person within an NHS organisation who is responsible for the systems that protect patient data
Confidential Information	Anything that relates to patients, staff or any other information (such as contracts, tenders etc) held in any form (such as paper or other forms like electronic, audio) howsoever stored (such as patient records, paper diaries, portable devices) or even passed word of mouth. Personal identifiable information is anything that contains the means to identify an individual.
Corporate Records	Records (other than health records) that are of, or relating to, an organisation's business activities covering all functions, processes, activities and transactions of the organisation and of its employees
Current Records	Records necessary for conducting the current and on going business of an organisation
Destruction	The process of eliminating or deleting records beyond any possible reconstruction
Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and the transfer of custody of records (including the transfer of selected records to an archive institution). They may also include the movement of records from one system to another (for example paper to electronic)
Electronic Records	Records where the information is recorded in a form that is suitable for retrieval, processing and communication by a digital computer

File	An organised unit of documents grouped together either for current use by the creator or in the process of archival arrangement, because they relate to the same subject, activity or transaction.
Paper Records	In the form of files, volumes, folders, bundles, maps, plans etc (this list is not exhaustive)
Patient Identifiable Information	Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
Protective marking	The process of determining security restrictions on records. Previously called 'classification'
Public Record	Records defined in the Public Records Act 1958 or subsequently determined as public records by The National Archives.
Record	Anything which contains information (in any media), which has been created or gathered as a result of any aspect of the work of NHS employees.
Records Management	Filed of management responsible for the efficient and systematic control of creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.
Retention	The duration of time for which information should be maintained or 'retained', irrespective of format
Scanning	The process of transferring one document, or a series of documents, into a form that is suitable for retrieval, processing and communication by digital computer.
Transit	The movement of items from one place to another
Due Regard	Having due regard for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. • Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

1.0. Purpose of the Policy

This Policy reflects the requirements of the Records Management Code of Practice 2021 which sets out a framework for consistent and effective records management based on established standards.

This policy is an important component in guiding employees on security of personal identifiable information and the use of information in accordance with relevant legislation, such as Data Protection and Freedom of Information Laws.

This policy relates to all clinical and non-clinical operational records held in any format by the organisation. These include:

- All administrative records (e.g. Personnel, estates, financial and accounting records; notes associated with complaint-handling); and Human resource files
- All patient health records (for all specialties and including private patients, x-ray and imaging reports, registers, etc)

2.0. Summary and Key Points

This document sets out Leicestershire Partnership NHS Trust's mandatory standards for the information and records used by the organisation to manage its information, held in whatever format, through every phase of its existence from creation to destruction.

The Records Management Policies and procedures form part of the organisations information lifecycle management, together with other processes, such as records inventory, secure storage, records audit etc.

Supplementary documents relating to specific areas of records management within the Trust but aligned to this policy include the following:

Electronic Health Records Policy (including management)
Clinical Document Scanning Policy
Data Protection and Information Sharing
Information Security and Risk
Data Protection Impact Assessment Policy and Procedure
Individual Information Rights

Aligns to:
- The Public Records Act 1958;
- Data Protection Legislation (currently UK GDPR/DPA 2018);
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;

- ➢ The NHS Confidentiality Code of Practice
- ➢ Records Management Code of Practice, 2021
- ➢ Care Quality Commission Outcomes Framework
- ➢ Caldicott2 Review, 2013
- ➢ National Data Guardian Standards
- ➢ NHS LA Risk Management Standards
- ➢ Information Security Management: NHS Code of Practice
- ➢ All professional bodies: HCPC,GMC, NMC

Describes processes and responsibilities for
- ➢ Record Creation, keeping and maintenance;
- ➢ Record Quality;
- ➢ Record disclosure and transfer;
- ➢ Record retention and disposal;
- ➢ Record storage, archiving and scanning

Is designed to support all staff, ensuring that records of all types are properly controlled, tracked, accessed and made available for use and eventually archived or otherwise disposed of appropriately.

3.0. Introduction

An Information Lifecycle and Records Management Policy is a high level document which sets out the Organisations policy towards the management of its information.

3.1 Records Management is the process by which an organisation manages all aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal

3.2 Code of Practice

The Records Management Code of Practice 2021 was published by the NHSX for the Department of Health (DH) as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisation and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver safe and effective services in consistent and equitable ways.

Information (records) management, through proper control of the content, storage and volume of records, reduces vulnerability to legal challenge or financial loss and promotes best value in terms of human and space resources through greater coordination of information and storage systems.

The Trust has adopted this information lifecycle and records management policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from doing so. These include:

- More efficient use of physical and electronic storage space;
- More efficient use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards; and
- Reduced costs

The Trust also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated yet integrated corporate function.

3.3 Information Security Management

The guidance contained within the Information Security Management: NHS Code of Practice and its related materials applies to NHS information assets of all types (including the records of NHS patients treated on behalf of the NHS in the private healthcare sector)
These information assets may consist of:

- digital or hard copy patient health records
- digital or hard copy administrative information
- digital or printed X-rays, photographs, slides and imaging reports, outputs and images

- digital media (including data tapes, CD-ROMS, DVDs, USB disc drives, removable memory sticks

- computerised records, including those that are processed in networked, mobile or standalone systems

- email, text and other message types.

3.4 Framework
This document sets out a framework within which the staff responsible for managing the organisation's records can develop specific guidance and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

4.0. Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. The organisation will take actions as necessary to comply with the legal and professional obligations set out in the Records Management Code of Practice, in particular:

- The Public Records Act 1958;

- The Data Protection Act 2018;
- The Retained General Data Protection Regulation (EU) 2016/679 – UK GDPR
- Access to Health Records Act 1990
- The Freedom of Information Act 2000;
- Health and Social Care Act 2008
- Environmental Information Regulations 2004
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice 2003
- National Patient Safety Agency (NPSA) – Use of the NHS Number 2008
- Records Management Code of Practice 2021

And any new legislation affecting records management as it arises.

Staff who are registered to a Professional body, such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC) or Health and Care Professionals Council (HCPC) will be required to record keeping standards defined by their registrant body. This is designed to guard against professional misconduct and to provide high quality care in line with the requirements of professional bodies.

5.0. Duties within the Organisation

5.1 The organisation as a Corporate Body
The organisation recognises that it has a specific corporate responsibility for records management. All contracts of employment must contain record keeping standards as laid out in this policy and in guidelines produced by regulatory bodies.

The organisation must have robust systems and processes that ensure that records are fit for purpose, are stored securely, are readily available when needed and are destroyed in compliance with the retention and destruction schedule at the end of the cycle of the particular record.

The Trust Board has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

5.2 Chief Executive
The Chief Executive has overall responsibility for records management in the organisation. As accountable officer, the Chief Executive is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

5.3 Senior Information Risk Owner
The Senior Information Risk Owner (SIRO) is an Executive Director of the organisations Board. As SIRO they are expected to understand how the strategic business goals of the organisation may be impacted by information risks and act as an advocate for information risk on the Board. They have an essential role in ensuring that identified information security risks are followed up and incidents managed. The role is supported by the organisations Head of Data Privacy (the individual responsible for records management), Information Asset Owners and the Caldicott Guardian.

5.4 Caldicott Guardian

The organisation's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

5.5 Head of Data Privacy

The Head of Data Privacy is responsible for the overall development and maintenance of records management practices throughout the organisation, in particular for drawing up guidance for good records management practice

5.6 Information Asset Owners

Information Asset Owners (IAOs) are accountable to the SIRO and provide assurance that information risk is being managed effectively for those information assets that they have been assigned ownership. They will be assisted in their role by staff acting as Information Asset Administrators (IAAs). These roles are generally fulfilled by Service Directors

5.7 Data Privacy Committee

This Committee is responsible for ensuring that the records management strategy and policy are implemented. It advises on clinical records management issues maintaining standards by:

- Identifying areas where improvements could be made
- Reporting performance standards
- Monitor compliance with the standards, legislation, policies and procedures relating to the management of records
- Approving locally devised methods of recording information e.g. the development of a standard format/design for clinical records

Its remit also includes:

- Ensuring record collection activities are rationalised by encouraging users to share records and the information they contain (subject to Data Protection and agreed confidentiality guidelines)
- Publicise and promote the local guidelines by supporting the implementation of a formal training programme to launch and support the guidelines and the inclusion of records management in induction training and staff handbooks.

5.8 Service Directors and Heads of Service

are responsible for local records management .Heads of Departments/ Professional leads within the organisation have overall responsibility for the management of records generated by their activities, i.e. ensuring that records controlled within their unit are managed in a way which meets the aims of the organisation's Records Management policies.

5.9 All Staff

All staff within the organisation, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the organisation

and manage those records in keeping with this policy and with any guidance subsequently produced.

All staff are provided with information on Information Governance standards during induction and are expected to familiarise themselves with organisational policy in relation to these issues. New starters are required to complete Data Security Awareness Level 1 training within 6 weeks of their commencement with the Trust.

All staff must have an understanding of the key requirements of laws and guidelines concerning records, in particular those relating to confidentiality, data protection and access to information including under the Freedom of Information Act 2000. All staff and those carrying out functions on behalf of the organisation have a duty of confidence to patients and a duty to support professional ethical standards of confidentiality. The duty of confidence continues even after the death of the patient or after an employee or contractor has left the NHS. Unauthorised disclosure of information may lead to a complaint against the organisation or a disciplinary action against a member of staff for a breach of confidentiality.

5.10   Contractors and support organisations
Service Level Agreements and contracts must include responsibilities for information governance and records management as appropriate.

6.0   What is a record?

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management 8, defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

Section 205 of the Data Protection Act 2018 defines a health record as a record which:

- Consists of data concerning health;
- Has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.

6.1   Aims of our Records Management System

The design and implementation of record keeping systems (DIRKS) is a manual which led to the creation of ISO 15489-1:2016 Information and documentation – Records Management. This standard focuses on the business principles behind records management and how organisations can establish a framework to enable a comprehensive records management programme.

The aims of our Records Management System are to ensure that:

- **Records are available when needed** – from which the organisation is able to form a construction of activities or events that have taken place

- **Records can be accessed** – records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist
- **Records can be interpreted** – the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records
- **Records can be trusted** – the record reliably represents the information that was actually used in, or created by, and its integrity and authenticity can be demonstrated
- **Records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format
- **Records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as the records are required
- **Records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value
- **Staff are trained** – so that all staff are made aware of their responsibilities for record –keeping and records management.

7.0   The 5 Phases of the Information Lifecycle

The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest. This can be seen diagrammatically in Figure 1.

This policy covers the details for each of these phases and the obligations of the Trust's employees' under this policy. This policy covers the obligations of all organisations employed by the Trust, all organisations contracted to the Trust and any organisation, or third party that shares Person Confidential Data (PCD) with the Trust.

7.1   Declaring a Record - Creation

Within a record keeping system, there must be a method of deciding:
- What is a record
- What needs to be kept

This process is known as 'declaring a record'. This is normally done at the point that it is created but it can also happen at a later date.

The process of declaring a record must be clear to staff. A declared record is then managed in a way that will fix it in an accessible format until it is appraised for further value or disposed of, according to the retention policy adopted.

Some activities will be pre-defined as creating a record that needs to be kept, such as a health record or the minutes and papers of board meetings. Other records will need

to fulfil criteria as being worth keeping, such as unique instances of a business document or email.

Figure 1 – The Records/Information Lifecycle
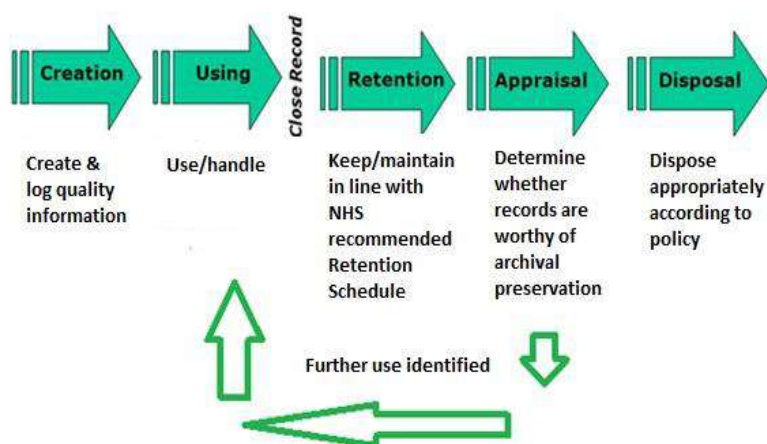
Characteristics of authoritative records

ISO 15489-1:2016 Information and documentation - Records management,30 published by the International Organization for Standardization (ISO), describes the characteristics that will enable records to be authentic, reliable, integral and usable throughout their lifecycle.

Record characteristic	How to evidence
Authentic	☐ It is what it purports (claims) to be ☐ To have been created or sent by the person purported to have created or sent it and ☐ To have been created or sent at the time purported.
Reliable	☐ Full and accurate record of the transaction/activity or fact ☐ Created close to the time of transaction/activity ☐ Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity.
Integrity	☐ Complete and unaltered ☐ Protected against unauthorised alteration ☐ Alterations after creation can be identified as can the persons making the changes.

Useable	☐ Located, retrieved, presented and interpreted
	☐ The context can be established through links to other records in the transaction/activity.

In addition to the above, employees should consider the following when creating information:

- What they are recording and how it should be recorded;
- Why they are recording it;
- How to validate information (with the staff, patient or carers or against other records) to ensure they are recording the correct data;
- How to identify and correct errors and how to report errors if they find them;
- The use of information; staff should understand what the records are used for and therefore why timeliness, accuracy and completeness of recording is so important; and
- How to update information and how to add in information from other sources
- Tracking & Retrieval System for paper based records

7.2 Using and handling records

All information must be used consistently, only for the intentions for which it was intended and never for individual employee's personal gain or purpose. If in doubt employees should seek guidance from the SIRO or, for health records, the Caldicott Guardian.

7.2.1 Organising records

The organisation must have a means of physically or digitally organising records. This is often referred to as a file plan or business classification scheme. In its most basic form, a business classification scheme is a list of activities (for example, finance or HR) arranged by business functions but most often linked to the organisations hierarchical structure.

At the simplest level, the business classification scheme can be anything from an arrangement of files and folders on a network to an Electronic Document Records Management System (EDRMS). The important element is the naming convention which is logical and can be followed by staff.

Classification schemes should try to classify by function first. Once the functional classification has been selected, the scheme can be further refined to produce a classification tree based on function, activity and transaction, for example:

Function: Corporate Governance
Activity: Board minutes and associated papers
Transaction: April 2020 – March 2021

7.2.2 Applying security classification

The NHS has developed a protective marking scheme for records it creates. It is based on the Cabinet Office 'Government Security Classifications' defined protective marking scheme which is used by both central and local government. Under the NHS Protective Marking Scheme 2014, patient information is classed as 'NHS Confidential'.

Unauthorised disclosure or misuse of information contained in records constitutes a serious breach of conduct that may lead to disciplinary action, and is also a criminal offence under Section 170 of the Data Protection Act 2018. Staff must guard against breaches of confidentiality by protecting information from improper disclosure and use at all times.

The Data Protection Act 2018, Professional Codes of Conduct, Human Rights Act 1998, administrative law and common law duty of confidentiality all place responsibility on everyone to maintain confidentiality of personal information. ('Confidentiality: NHS Code of Practice' provides further guidance and applies to all NHS employees)

Basic principles that should be adhered to are as follows:

• Records should never be left in a position where unauthorised persons can obtain access to them (including computer screens left on but unattended)
• Only staff who are authorised to access patient/service users records as part of their duties in or associated to the provision of care and treatment, or in carrying out audit and governance duties, are permitted to do so. The content of records should not be communicated with persons not authorised to receive them. They may be discussed on a need to know basis only to provide care and treatment to the patient/service user.
• Correspondence between the organisation and staff/patient/service users about staff/patient/service users should be clearly marked 'NHS Confidential' to ensure confidentiality.

7.2.3 Information Sharing

National policy developments, the White Paper *Our Health, Our Care, Our Say',* highlights the need for health and social care to work together to provide seamless services to patients wherever the need arises. This has important implications for sharing information between health and social care. This was confirmed within the Health & Social Care Act 2012, the Caldicott 2 Review (To Share or Not to Share) and the National Data Guardian update to the Caldicott Principles (See *Data Protection and Information Sharing Policy* for more details).

As an NHS organisation, we increasingly need to seek assurances that our social care partners apply the equivalent information security standards to their own information assets and vice versa. Where cross-boundary NHS information sharing arrangements are required, the implementation of relevant and consistent standards for information security management provides the basis that underpins trust and confidence in these partnership arrangements.

Person confidential data will be shared in line with legislation, national guidance and documented information sharing agreements which have been agreed through the Trusts Information Governance processes.

7.2.4   Tracking & Retrieval System
When paper records are retrieved or removed for any reason from the file storage system, their removal and subsequent return should be recorded using a robust tracking system. As a minimum it should include:

- The unique identifier (NHS Number in the case of clinical records)
- A description of the item
- The name of the individual requesting and the reason for the request
- The person or department to whom it is being sent
- The date of transfer
- The date of return
- The signature and printed name of the person returning the file

In order to provide an effective retrieval service, it is essential that the movement of all patient records are recorded either on an electronic system; on a suitable database for manual tracking systems.

Electronic tracking of records through a PAS or Secure Tracking through the off-site storage supplier should be used to record and monitor movement of records, where staff have access to it. Where these systems are not used, the transfer of information slips/tracking record slips should be used, particularly where there are site to site transfers using the portering service.

7.2.5   Transporting of Records

Paper records

The mechanism for transferring information from one organisation to another should also be tailored to the sensitivity of the material contained within the records and the media on which they are held.

Health records or other confidential information for transportation between LPT sites/departments or to other health organisations within the Local Health Community must be enclosed in sealed bags /envelopes/designated secure boxes and labelled appropriately i.e. Confidential, and sending location included in order to aid return. For specific situations of extreme sensitivity e.g. child protection, a further statement should be added stating '*to be opened by addressee only'*.

Records must be carried between sites/departments by authorised staff only. Authorised staff may include:

- Appropriate member of staff
- Internal transport systems – Portering Service
- Authorised courier service
- Off-site records storage supplier
- Special Delivery by Royal Mail

Where external courier services are used to transfer staff/patient/service user records between health organisations, a formal contract needs to be put in place including ensuring that the documents are transported in sealed envelopes. The contract should include confidentiality issues. A schedule of documents should be presented to the courier for signature which should be cross-checked by the organisation receiving the records.

Employees must not send health records by first class mail. Appendix 6 sets out a risk assessment process to assist in making the decision about the appropriate transport mechanism and media.

Records should not be left unattended in transit at any time. When carried in a car they must be locked in the boot.

Only in exceptional circumstances may records be taken home by a member of staff to work on. Where this is necessary, a risk assessment should be undertaken and arrangements put in place to ensure that they are kept secure. Evidence of this risk assessment should be held locally by the service, with authorisation from the lead for the service. Staff who do will be responsible for the security and confidentiality of the records (See Information Security and Risk Policy and Appendix 7 – Guidance for Staff carrying records off site).

Transporting records from LPT premises requires vigilance and the principles of confidentiality must be maintained.

Electronic Records

In line with the level of security around the transfer and transport of paper records, electronic records require the same level of sensitive handling.

Where there are requests for records to be sent to other organisations, individuals or agencies (including solicitors and the Police), these request should be handled by the Data Privacy Team under a Request for Information. The Subject Access Request Standard operating Procedure outlines the detail of what needs to be done.

In the rare occasion where a staff member is requested to send clinical documentation or electronic records, they are requested, in the first instance, to contact the Data Privacy Team (lpt.dataprivacy@nhs.net) for advice and support.

7.3 Record Closure

Information held in records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use, other than for reference purposes. An indication that a file of paper records or folder of electronic records has been closed should be shown on the record itself as well as noted in the index or database of files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the information is created.

The storage of closed, or non-current records awaiting disposal should follow accepted standards relating to environment, security and physical organisation of files.

For digital records, a system may already be set up whereby records no longer required for current business are stored (such as a dedicated network drive or space on a drive). Records should be moved there keeping operational space free for current cases or work. This will also restrict unnecessary access to non-current personal and sensitive data.

7.4   Retention

It is a fundamental requirement that the organisation's records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the organisation's business functions.

The organisation has adopted the retention periods set out in the Records Management Code of Practice 2021. A separate guidance document setting out these retention periods is available.

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in format. The use of standardised filenames and version control methods should be applied consistently throughout the life of the information.

7.4.1   Storage of Records

All manual and electronic records in the organisation must be appropriately stored and retained in accordance with recommended retention periods

Paper: Wherever possible the Trusts direction of travel is to move to digital records. The original paper guarantees the authenticity of the record. However, it can be hard to audit access to the record, depending on where it is stored, because paper records do not have automatic audit logs.

Digital: digital records offer many advantages over paper records. They can be accessed simultaneously by multiple users, take up less physical storage space and enable activities to be carried out more effectively.

Digital information must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format in addition to providing information about those who have accessed the record.

The movement and location of records should be controlled to ensure that a record could be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

Records must always be kept securely with appropriate security measures in place to prevent loss, unauthorised access and modification, but a balance needs to be

achieved between security and accessibility. Storage accommodation for current records should be clean and tidy, and it should prevent damage to the records.

Equipment used for active records should provide storage which is safe from unauthorised access and for paper records storage, this also includes meeting fire regulations, but which allows maximum accessibility to the information commensurate with its frequency of use. The following factors must be taken into account:

- Compliance with health and safety regulations
- Degree of security required
- Users needs
- Type of records to be stored
- Size and quantity of record
- Usage and frequency of retrievals
- Ergonomics, space, efficiency and price.

Electronic records/documents in shared folders

Where electronic records/documents are stored on a network shared folder, it is important that the naming of the folders are clear in order that their contents are easily identifiable/retrievable (as outlined in 7.2.1); the access to the folders should be restricted to those who require access and not left with open access (contact with LHIS service desk for support with this).

Clinical documents/records should not be stored outside of the clinical record unless they are too large to be uploaded or attached but where this is the case the secure cloud storage or LPT Clinical Drive should be used as a preference. Alternatively a separate clearly marked and restricted access folder created and referenced in the clinical record.

7.4.2 Records in Patient/Service Users' Homes

In some circumstances records may be stored at the patient/service user's home, e.g. nursing care plans. They must be returned to the base when no longer in use. Stored records should be made safe whenever they are left unattended. Ideally they should be protected by additional security such as being locked up and keys made available to authorised staff only. However, confidentiality of records left in the patient/service user's home is the responsibility of the patient/service user and they must be informed of this.

7.5 Appraisal

The process of deciding what to do with records when their business use has ceased and the minimum retention period has been reached. No record or series can be automatically destroyed or deleted.

Appraisal will be defined in a separate Standard Operating Procedure and any decisions documented and linked to a mandate to act. Any changes to the status of records must also be reflected in the Trusts' Record of Processing Activity (ROPA).

When appraising records that have come to the end of their minimum retention period, the following should be considered:

- **Ongoing use**: The may be a reason to keep the record for longer than the minimum retention period for care, legal or audit reasons. In these cases extensions can be set provided it is justified and approved.

- **Classification of diseases (based on ICD-10 code):** Some health conditions lend themselves towards longer, or extended retention periods.

- **Operational Delivery**: The way a service was delivered may have been transformative at the time, which may justify an extended retention or long-term archival preservation.

- **The way care is delivered**: The records may be reflective of health or care policy at the time.

- **Series Growth**: If records are part of a series that will be added to (type of record as opposed to additional content) there may need to be a consideration of space. For example, continued expansion of a series of records that has a very low recall rate, continued retention would be harder to justify.

- **Recall rates**: If a series of records is routinely accessed to retrieve records, then there must be justification for extending the retention period due to ongoing use. Whereas for a series with very low recall rate would be harder to justify.

- **Historical value**: If the record has potential historical or social value (for example, innovative new service or treatment or care delivery method) then consideration may be considered for retaining longer. In these circumstances it is worth engaging with the Trusts Records Exploitation Manager to have early contact with the local Place of Deposit (PoD). They normally do not accept records before 20 years retention has passed, unless there are exceptional circumstances for early transfer.

- **Previous Deposits**: The records held may be a continuous series that has historically been accessioned by a local PoD. It is important to find out what has historically been accessioned so that a series of records remains complete. It is likely that records that add to an already accessioned series will continue to be taken by the PoD.

Digital records can be appraised if they are:

- Arranged in an organised filing system

- Differentiated by the year of creation

- Organised by the year of closure

- Clear about the subject of the record

If digital record have been organised in an effective classification scheme or electronic record system, this process is made easier. Decisions can then be applied to an entire class of records rather than reviewing each record in turn.

There will be one of three outcomes from appraisal:

☐ Destroy / delete

☐ To keep for a longer period

☐ To transfer to a place of deposit appointed under the Public Records Act 1958.

All appraisal decision need to be justified, follow documented Trust guidance and be documented and approved by the Data Privacy Committee or delegated sub-group.

7.6 Disposal

It is particularly important under freedom of information legislation that the disposal of records, is undertaken in accordance with clearly established policies which have been formally adopted by the Trust and which are enforced by properly trained and authorised staff. No information can be destroyed if it is the subject of a request under the Data Protection Act 2018 and/or the Freedom of Information Act 2000.

7.6.1 Permanent Destruction / Deletion

It is important to keep accurate records of destruction and appraisal decisions. Destruction implies a permanent action. For electronic records 'deletion' may be reversed and may not meet the standard as the information can/may be able to be recovered or reversed.

Paper records: Records may contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and secures their complete illegibility and inability to be reconstructed. Any records that have been identified for destruction must be destroyed as soon as possible after they are eligible in accordance with approved Trust procedures and using Contractors and methods authorised by the Trust.

The Destruction provider must provide a certification of destruction for the bulk destruction of records. This certification must be linked to a list of records, so that the Trust has clear evidence that particular records have been destroyed.

Records that do not contain personal information or confidential material can be destroyed in a less secure manner (such as confidential waste bins that do not provide certificates of destruction). If there is any doubt, material should be treated as confidential and evidentially destroyed.

Do not use the domestic waste or put records in rubbish bins that will go to the tip because the confidential material remains accessible to anyone that finds it.

Digital records/media: Destruction implies a permanent action. For digital records 'deletion' may not meet ISO 27001 standard as the information can or may be able to be recovered or reversed. Destruction of digital information is therefore more challenging.

One element of records management is concerned with accounting for information, so any destruction of hard assets, like computers, hard drives and backup tapes, must be auditable in respect of the information they hold. An electronic records management system will retain a metadata stub which will show what has been destroyed.

The Information Commissioner's Office (ICO) guidance '*Deleting Personal Data*'[1] sets out that information is deleted from a live environment and cannot be readily accessed then this will suffice to remove information for the purposes of Data Protection Law.

Electronic systems vary in their functionality. They may have the ability to permanently delete records from the system or not. Where a record has reached its retention period and has been approved for destruction, then the record should be deleted if the system allows. A separate record should be kept of what record has been deleted.

If a system does not allow permanent deletion, then all reasonable efforts must be made to remove the record from normal daily use. It should be marked in such a way that anyone accessing the record can recognise that it is dormant or archived.

7.6.2 <u>Digital Records, Digital Continuity, Digital Preservation and Forensic Readiness</u>

Digital information presents a unique set of issues which must be considered and overcome to ensure that records remain authentic and reliable, retaining their integrity and usability. Digital continuity refers to the process of maintaining digital information in such a way that the information will continue to be available, as needed, despite advances in digital technology. Digital preservation ensures that digital information of continuing value remains accessible and usable. Refer to The Digital Preservation Coalition handbook when considering issues associated with retaining digital records for long periods of time and well as the Trusts' Information Security and Risk Policy section on IG Forensic Readiness

---

[1] https://ico.org.uk/media/for-%20organisations/documents/1475/deleting_personal_data.pdf

.

8.0   Incidents and Lost records

This section predominantly relates to paper records/documents.

Any incident or near miss relating to a breach in the security regarding use, storage, transportation or handling of records must be reported using the organisation's Incident recording system.

A serious breach of security e.g. major theft or fire must be managed in accordance with the same Policy in relation to it being a Serious Untoward Incident.

A lost record is defined as any record that cannot be located within 10 working days of first attempt to access the record or any record that has been stolen from a known place, for example, the boot of a car. Any suspected thefts must be reported to the Police.

The organisation's Caldicott Guardians must be informed immediately of any loss or misplacement of any document that is used to record patient information, including diaries, or organisational business. When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of all actions including:
- When and where the record was last seen, with date known
- If stolen, from where and Police Incident Number
- Actions taken to locate file

It is the responsibility of the line manager, liaising with and taking advice as necessary from the Data Privacy Team, to investigate such incidents and identify any learning points that must be implemented in order to prevent a recurrence.

9.0   Information Risk

Threats to NHS data shall be appropriately identified and based upon robust risk assessments and risk management arrangements in line with the organisations risk management strategy and policy, and shall be managed and reviewed regularly to ensure:

- protection against unauthorised access or disclosure
- that the integrity and value of information is maintained
- that information is only available to authorised personnel as when it is required.

The organisation will ensure adequate audit provision, based upon robust risk management arrangements, ensuring the continuing effectiveness of NHS information security management arrangements.

In particular, the organisation will set out its commitment to create, maintain and manage the security of its key information assets (including its records) and other external information resources that it depends upon, and documents its principle activities in this respect.

Also see the Information Security and Risk Policy for more detailed guidance.

10.0 Research Governance

Any research, as opposed to audit, undertaken using patient records must first have had Research Ethics Approval as part of the Research Governance Framework. For advice on your proposed project and requests for information from other organisations, please contact the organisations Research lead.

11.0 Training needs

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory training.

At least 95% of all staff, including new starters, locums, temporary, students and staff contracted to work in the organisation must have completed their annual Data Security Awareness Level One training in the period 1 April to 31 March. A record of the training will be recorded on uLearn.

The information button 🛈 against the title of the module 'NHS Data Security Awareness Level 1' on uLearn identifies who the training applies to, the update frequency and learning outcomes.

There is also a recommendation for additional non-mandatory subject specific training where roles involve the management of requests to access health records.

The governance group responsible for monitoring the training is Trust's Data Privacy Committee.

12.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	All new starters complete Data Security Awareness Level 1 training within 6 weeks of commencement	Section 5.9	Monthly Mandatory training Report	Data Privacy Committee	Quarterly
	Unauthorised use of disclosure constitutes and offence	Section 7.2.2	Incident Reporting – Caldicott Report	Data Privacy Committee	Quarterly

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	There should be a tracking mechanism in place for movement and transfer of paper records	Section 7.2.4	Incident Reporting – Caldicott Report	Data Privacy Committee	Quarterly
	Incidents of lost records are reported	Section 8.0	Incident Reporting – Caldicott Report	Data Privacy Committee	Quarterly

13.0 Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
Data Protection and Security Toolkit	All records are appropriately stored or archived

14.0 References and Bibliography

This policy was drafted with reference to the following:

National and Legal requirements

NHSX Records Management Code of Practice 2021

National Data Guardian Standards

Data Protection and Security Toolkit

Data Protection/Privacy Law

Freedom of Information Act 2000

Trust Policy

Data Security and Protection Strategic Framework

Data Protection and Information Sharing Policy

Freedom of Information Policy

Electronic Health Records Policy (including management)

Individual Information Rights Policy

Information Security and Risk Policy

Data Protection Impact Assessment Policy and Procedure

Appendix 1

Training Needs Analysis

Training Required	YES ✓	NO
Training topic:	Data Security Awareness Level 1	
Type of training: (see study leave policy)	✓ Mandatory (must be on mandatory training register) ☐ Role specific ☐ Personal development	
Division(s) to which the training is applicable:	✓ Adult Mental Health & Learning Disability Services ✓ Community Health Services ✓ Enabling Services ✓ Families Young People Children ✓ Hosted Services	
Staff groups who require the training:	All Staff including temporary, contract and students	
Regularity of Update requirement:	Annually	
Who is responsible for delivery of this training?	eLearning through ULearn	
Have resources been identified?	Yes	
Has a training plan been agreed?	Yes	
Where will completion of this training be recorded?	✓ ULearn ☐ Other (please specify)	
How is this training going to be monitored?	Monthly manager reports with overarching oversight by Data Privacy Committee	

Appendix 2

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	✓
Respond to different needs of different sectors of the population	✓
Work continuously to improve quality services and to minimise errors	✓
Support and value its staff	☐
Work together with others to ensure a seamless service for patients	✓
Help keep people healthy and work to reduce health inequalities	✓
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	✓

Appendix 3

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation

Circulated to the following individuals for comment

Name	Designation
Members of Data Privacy Committee	
Dr Avinash Hiremath	Medical Director/Caldicott Guardian
Sharon Murphy	Executive Director of Finance & Performance/SIRO

Appendix 4

<p align="center">**Due Regard Screening Template**</p>

Section 1	
Name of activity/proposal	Information Lifecycle and Records Management Policy
Date Screening commenced	
Directorate / Service carrying out the assessment	Enabling/Data Privacy
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland, Head of Data Privacy
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The purpose of the document is to promote good practice and consistency of information being collected, managed and used within Leicestershire Partnership NHS Trust (LPT). The principles of records management practices are embedded in national guidance and Law	
OBJECTIVES: To provide staff with a framework within which they can operate, taking into account the safety, security and integrity of the information and records that they hold for all service users	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Disability	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Gender reassignment	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Marriage & Civil Partnership	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Pregnancy & Maternity	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Race	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Religion and Belief	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Sex	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust

Sexual Orientation	Positive – the policy covers the expectations for the management and handling of **all** information held by the Trust
Other equality groups?	

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please <u>tick</u> appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click <u>here</u> to proceed to Part B		Low risk: Go to Section 4.	✓

Section 4			
If this proposal is low risk please give evidence or justification for how you reached this decision:			
The Policy is written in line with national guidance and the legal framework for the management and handling of information, which does not discriminate			
Signed by reviewer/assessor	Sam Kirkland	**Date**	08/03/22
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed		**Date**	

Appendix 5

DATA PRIVACY IMPACT ASSESSMENT SCREENING

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy. The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.		
Name of Document:	**Information Lifecycle and Records Management Policy**	
Completed by:	**Sam Kirkland**	
Job title	**Head of Data Privacy**	**Date: 08/03/22**
Screening Questions	**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	No	
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	No	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	No	
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**No**	
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	No	
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	No	
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	No	
8. Will the process require you to contact individuals in ways which they may find intrusive?	**No**	
If the answer to any of these questions is 'Yes' please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk In this case, adoption of a procedural document will not take place until review by the Head of Data Privacy.		
Data Privacy approval name:	**Sam Kirkland, Head of Data Privacy**	
Date of approval	**08/03/22**	

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust

Appendix 6

Risk Assessment for Transferring/Transporting/Sending Confidential Personal Data

All NHS organisations work to a Code of Conduct for handling patient-identifiable information. Working to the same Code of Conduct helps ensure a more unified approach across NHS organisations to the way NHS staff handle, store, transfer and work with patient information. This also helps ensure compliance with the Data Protection Legislation.

The NHS holds large amounts of confidential information about you, members of your family, friends, and colleagues; but the vast majority of this information will be about strangers, most of whom you are unlikely to meet. This information is classed as Patient Confidential Data (PCD). The information belongs to the patients. Their information should be treated with as much respect and integrity as you would like others to treat your own information. It is your responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that patient-identifiable information is not made available to unauthorised persons.

Breaches of confidentiality are a serious matter. Non-compliance with this code may result in disciplinary action being taken. No employee shall knowingly misuse any information or allow others to do so.

What is meant by the transfer of patient confidential data?

The transfer of patient confidential data, by whatever means, can be as simple as:
- taking a document and giving it to a colleague;
- making a telephone call;
- sending a email;
- passing on information held on computer, for example confidential clinical information held on patient records.

In all cases, however simple or complicated, the Caldicott Principles (Figure 1) must be adhered to in order to ensure that patient-identifiable information is not disclosed inappropriately.

Figure 1 Caldicott Principles

> 1. **Justify the purpose.**
> 2. **Don't use patient-identifiable information unless it is absolutely necessary.**
> 3. **Use the minimum necessary patient-identifiable information.**
> 4. **Access to patient-identifiable information should be on a strict need to know basis.**
> 5. **Everyone should be aware of their responsibilities.**
> 6. **Understand and comply with the law.**
> 7. **The duty to share information can be as important as the duty to protect patient confidentiality**
> 8. **Inform service users and patients about how their information is used**

ENSURING CONFIDENTIALITY

Information transfer principles

It is imperative that the utmost care is exercised when transferring PCD. To this end written documents as well as email should be used with care. When internal courier post or public mail is used, it is essential to confirm that the addressee details are correct. The basic rule is that in all circumstances where PCD is shared, by whatever method, the items transferred should be restricted to a minimum. Only essential items of information should be included. Other items should be omitted or blocked out before transmission.

When transferring paper documents, including records, which contain PCD, make sure "NHS CONFIDENTIAL" is marked in a prominent place on the front of the envelope. Ensure that the address of the recipient is correct and clearly stated, using the following format and using window envelopes:

- Name;
- designation (job title);
- department;
- organisational address.

Write a return address on the back of the envelope (if using a plain envelope).

If PCD is to be sent in carrier (internal) envelopes, the envelope must be sealed and marked "NHS CONFIDENTIAL". Internal mail should still be properly named and addressed, e.g. not just to "Mary from Medical Records".

Do not pass documents containing PCD to other colleagues by leaving them on a secretary's desk or in an "IN" tray. Always ensure that the information is in a sealed envelope addressed to the recipient and clearly marked "NHS CONFIDENTIAL".

Transfer between hospital sites, clinics, community bases etc.

You should always ensure that a secure system for transferring care records (or other personal information that identifies individuals) between sites is used, referring to this guidance.

Only authorised personnel may assist in the transfer of patient records where an office, department or practice is moving premises from one site to another. This must be done under the guidance of an authorised employee/employees of the relevant organisation.

Transfer between departments on site

Where there is an internal system for transferring confidential information (e.g. routine portering transfer) in place, this may be used to transport records between departments. Alternatively, appropriate special arrangements may need to be made for information required urgently (e.g. non-routine portering transfer). In either situation, the information must be correctly packaged and labelled as detailed earlier. Depending upon circumstances, it may be more appropriate and expedient to transport the information personally. If this is the preferred option, do not leave any information visible inside the car; ensure that it is locked away securely in the boot.

It is not appropriate for unpackaged information to be handed to another person for delivery simply because she/he is going to the destination department.

If you have any specific questions regarding transferring patient records, contact the assigned Data Privacy Team or line manager for further guidance.

Risk associated with sending patient identifiable information out of the organisation

Risks related to transporting/transferring patient information	Some Suggested Controls
Sending appointment letters out to patients with no clinical details	Confirm numbers Use of Royal Mail Provide return address (PO Box for mental health services)

Sending referrals to external agency with clinical information included	Use of agreed format outlining proportionate amount of detail What is the preferred method of sending to the agency/organisation? Can you keep a copy of the information sent? How do you obtain receipt to referral? Consider use of secure online form/sending via secure email
Sending detailed report including medical conditions and outcomes of treatment	Do you know who the report should go to i.e. named individual? Can the information be password protected? Does the receiving organisation/individual have a secure email address? Is the receiving organisation/individual local? Do you need to be able to track the journey of the report? Consider using secure email/Arrange to hand deliver/ Recorded Delivery mail where no tracking required/Special Delivery

Appendix 7

GUIDANCE FOR STAFF CARRYING PATIENT RECORDS OR OTHER CONFIDENTIAL / SENSITIVE INFORMATION OFF-SITE

Who is this guidance for?

Any staff of the organisation including temporary, agency or
bank staff and staff under contract, who are transporting confidential, sensitive or personally identifiable information themselves.

It does not apply to transportation by porters, internal or external mail, or transport of records between hospitals by ambulances or couriers.

What is covered?

This includes, *but is not limited to,* any patient records, sensitive financial, estates or personnel records, contracts, and confidential information relating to GP and other independent contractor practices. This information is hereafter called 'records' in the remainder of the guidance. If in any doubt talk to your line manager

Are formats other than paper covered?

➢ Any hard copy format is covered. For guidance on electronic records you are strongly advised to read the Secure Email Guidance for Sending PCD. You can also refer to the Information Security and Risk Policy.

➢ At local induction managers need to make clear to the individual what records they can take off-site and what, if anything, should never be removed without prior permission. This should ensure clarity of understanding and also that the individual does not need to get approval for individual records.

➢ No records should be removed from base unless they are needed for work.

➢ It is recognised that healthcare professionals may find it necessary to remove patient's health records or other related clinical documentation from their base, to facilitate their daily practice of seeing patients in community setting. To reduce the risk of loss of such records and to reduce the risk of breaches of confidentiality there are various considerations to be made, based on best practice. Only those records required for the patients being seen in the community should be removed. Ideally, records should not be removed for general administration purposes, e.g. writing reports. There should be a trace or booking out reference kept at the base from which records have been removed.

➢ It is important that other staff know where the records have gone. Use the tracking system in place. If one does not exist then discuss creating one with your line manager. This does not have to be complex.

- Records/clinical documentation should be transported from the office in suitable covers or containers so that they are protected and not in danger of being dropped or damaged. They should be handled carefully when being loaded or unloaded. Vehicles must be fully covered so that records are protected from exposure to weather, wind, excessive light and other risks such as theft.

- Records/clinical documentation should not usually be left unattended in cars. However, it is acceptable to do so if there is a definite risk that they will be viewed by unauthorised personnel, damaged or stolen if they are taken into the building. Risk assess the situation and use your professional judgement to decide whether it will be safer to take the records into the house or to leave them in the car. If left in the car the records should be placed in a locked car boot out of sight, with the car alarm on if there is one.

- Cars should be parked in a secure and well-lit location.

- At the end of a working shift records it is best practice to return the records to the base office.

- If the member of staff does not return to base at the end of a shift, records/clinical documentation must be removed from the car and care taken to ensure that members of the family or visitors cannot gain access. Ideally, records should be stored and carried in a secure case and kept out of sight. Staff should ensure that they place the secure case in a cupboard or similar, as soon as they enter the house. If they do not have a secure case, notes should be stored in a locked cupboard or cabinet with access only by the member of staff.

- If the staff member is involved in a road traffic accident / incident which necessitates the car being left on the roadside or taken to a garage, records should be removed if possible. If this is not possible the police should be informed that confidential records/clinical documentation are in the car. The line manager and/or On-Call manager should be contacted and made aware of the situation. They should ensure that an incident form is completed and do whatever they can to help retrieve the records.

- If a member of staff's car is stolen or broken into and records/clinical documentation stolen, the police should be informed, the line manager and/or on-call manager should be contacted immediately and an Incident form completed.

- Staff should not attempt to remove records/clinical documentation from a burning car. The emergency services should be informed that records are in the car. The line manager and/or on-call manager should be contacted immediately and an incident form completed.

It is inappropriate to work on records whilst travelling by public transport or in any non-NHS, non-secure environment e.g. cafes