NHS
Stockport
NHS Foundation Trust

INFORMATION LIFECYCLE & RECORDS MANAGEMENT POLICY

CONTENTS

EXECUTIVE SUMMARY

This document sets out a framework within which the staff responsible for managing the Trust's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs, and within which all other staff handling records can ensure compliance with the legal obligations and best practice surrounding records management.

The overall objective of this policy is to provide clear direction for the management of all Trust records, including both clinical and corporate records.

Director of Informatics

SCOPE AND PURPOSE

Records Management is the process by which an organisation manages all the 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.

The **Records Management: Code of Practice 2023** has been published by the NHS England 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 Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

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

- better use of physical and server space;
- better 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 corporate function.

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

- The Public Records Act 1958;
- The Data Protection Act 2018 and the United Kingdom General Data Protection Regulation (UK-GDPR)
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality;
- The NHS Confidentiality Code of Practice; and
- Any new legislation affecting records management as it arises

The recording of pertinent information and record-keeping are fundamental and an integral requirement for the delivery of high quality healthcare. Well documented records are essential for good professional practice.

Records are a valuable resource because of the information they contain. That information is only usable if it is correctly recorded in the first place, is regularly up-dated, and is easily accessible when it is needed. Information is essential to the delivery of high quality evidence-based health care on a day-to-day basis and an effective record management service ensures that such information is properly managed and is available whenever, and wherever there is a justified need for patient-based information, in whatever media it is required and also to:

- support patient care and continuity of care;
- support day to day business processes and procedure which underpin delivery of care;
- support evidence-based clinical practice;
- support sound administrative and managerial decision making, as part of the knowledge base for Trust services;
- meet legal requirements, including requests from patients, staff and others under the “Data Protection Act 2018 and the UK-GDPR”
- (for living individuals) and the Access to Health Records Act 1990 in relation to patient records (for deceased patients);
- support clinical and other audit processes and;
- support improvements in clinical effectiveness through research and support archival functions by taking account of the historical importance of the material and the needs for future research.

In developing this policy the Trust has given due regard to its legal requirements and obligations and the NHS Information Governance agenda and best practice standards including, but not limited to:-

- The legal and regulatory framework as set out within the “NHS Information Governance:

- Guidance on Legal & Professional Requirements"
- The "The Data Security and Protection Toolkit" and its component requirements
- The Records Management: Code of Practice 2023
- The "Information Security Management: NHS Code of Practice"
- "ISO 27001 and 27002", the International Standards for Information Security
- "ISO 27799: Health Informatics - Information Security Management in Health Using ISO-IEC 27002"
- Data Protection Act 2018 and the General Data Protection Regulations

This policy applies to Stockport NHS Foundation Trust, referred to as the 'Trust', and includes all hospitals, units and community health services managed by Stockport NHS Foundation Trust.

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

- all administrative records (eg personnel, estates, financial and accounting records, notes associated with complaints, policies, procedures, meeting minutes etc); and
- all patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)

The aim of this policy is to promote best practice and provide;

- a framework for consistent, coherent and compatible records;
- a reference point against which continuous clinical improvement and consultation can be delivered by medical, nursing, midwifery and allied professional personnel;
- a set of robust but flexible standards which are derived from the NHS Litigation Authority (NHSLA) and the requirements (standards) contained in the Information Governance Toolkit. The standards are generic and should be applied to all areas.

This policy applies to all those working in the Trust, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken as considered appropriate.

This may include formal action in line with the Trust's disciplinary or capability procedures for Trust employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

ROLES AND RESPONSIBILITIES

Chief Executive Officer (CEO):

The Chief Executive has overall responsibility for records management in the Trust. As accountable officer the job holder 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.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Medical Director/Caldicott Guardian

The Caldicott Guardian is a senior person responsible for safeguarding the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They play a key role in ensuring that the NHS, Councils with Social Services responsibilities and partner organisations satisfy the highest practicable standards for handling patient identifiable information

Deputy Director of Quality Governance

The Deputy Director of Quality Governance has responsibility for ensuring that all governance requirements with regard to records management are adhered to. This is incorporated within the CQC requirements as well as the IG Toolkit

Division Quality Groupses:

The implementation of, and compliance with, this Policy and associated strategy, in relation to clinical records is the responsibility of the individual Divisional Quality Committees.

The individual Divisional Quality Committees will ensure that records management systems and processes are developed, co-ordinated and monitored in relation to all clinical records.

Associate Director for Patient Access:

The Associate Director is responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good health records management practice and promoting compliance with the records management policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

Assistant Directorate Manager:

The Assistant Directorate Manager is responsible for ensuring that on an operational level, good health records management practice is adhered to and promoting compliance with the records management policy. The Assistant Directorate Manager should ensure that all health records staff are trained and competent in records management practices and that these practices are adhered to by all Trust staff. Monitoring, auditing and recording of these practices should be undertaken on a regular basis.

Health Records Section Managers:

The Health Records Section Managers are responsible for ensuring all standard operating procedures are adhered to, monitored and non-compliance reported. Training should be identified for all Health Records Staff, and training records maintained.

Health Records Supervisors:

The Health Records Supervisors are responsible for ensuring that all Health Records Staff are aware of all relevant standard operating procedures, and that they are fully trained and competent in applying them.

Health Records Staff:

Health Records Staff should be aware, competent and trained in all relevant polices and standard operating procedures, and promote good records practice within the Trust.

Ward Clerks:

Ward Clerks should be aware of and adhere to all standard operating procedures relating to Health Records. They should attend a Health Records Awareness Session and promote good Health Records practice throughout the Trust.

Emergency Department – Administrative & Clerical Staff:

Administrative & Clerical staff in the Emergency Department should adhere to Health Records Standards by replicating Emergency Department Records in the main health record for all patients who are admitted.

Information Governance & Security Group:

The Information Governance & Security Group is responsible for overseeing progress with the records management agenda both in relation to corporate records and clinical records. The Information Governance & Security Group will report on progress to the senior level of management in the organisation.

Director of Finance / Senior Information Risk Owner (SIRO):

The SIRO takes ownership of the risk management of information assets and assures risk assessment process to the Board and is responsible for advising the Chief Executive Officer on information related risks.

Information Asset Owners (IAO's):

IAO's are operationally responsible at senior levels for all information assets within their divisional areas. IAO's should understand and address the levels of risk in relation to the divisional assets they own and provide assurance to the SIRO on the security and use of those assets on quarterly and annual basis of review.

Information Asset Administrators (IAA's):

IAA's work at local division/departmental level and ensure that policies and procedures are in place for all information assets and that these are followed, recognise and report actual and potential security incidents, liaise with the IAO on incident management and ensure information asset registers are accurate and up to date.

Clinical Audit

The Clinical Audit team will provide advice and guidance and will facilitate Divisions to undertake the regular Clinical Records audits.

All Trust Managers:

Managers within the Trust are responsible for ensuring that the policy, and other associated policies and supporting standards and guidelines are built into local processes and that there is on-going compliance.

Managers within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policies.

Managers are responsible for the communication about and compliance with Trust policies, and must ensure that staff are adequately trained and apply the appropriate guidelines.

All Trust Staff:

All staff, whether permanent, temporary or contracted, clinical or administrative are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

All staff are responsible for any records or data they create and what they do with information they use. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

Staff should ensure they attend information governance training and awareness sessions on an annual basis to maintain their knowledge and skills. All staff who handle Health Records should also be encouraged to attend a Health Records Awareness session.

All staff have a responsibility to adhere to information governance standards which are written into the terms and conditions of their contracts of employment.

Summary:

Particular responsibilities for and within this policy are summarised below:-

Role	Responsibility
Overall Information Governance	Chief Executive & the Trust Board
Risk Management	Senior Information Risk Officer (SIRO)
Protecting patient information	Caldicott Guardian & Data Protection Officer
Review and maintenance of Records Management policies and procedures	Information Governance & Security Group Records Management Group
Approval of Records Management policies and procedures	Executive Directors/Board Assurance Committee
Local adoption of Records Management policies and procedures	Line Managers
Compliance with policy	All Employees and Contractors
Monitoring compliance with the policy	Line Managers
Monitoring compliance with standards and improvement plans	Information Governance & Security Group Records Management Group

GLOSSARY OF TERMS

Records Management

Records Management is a discipline which utilises an administrative system 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 Trust and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and

- disposal.

Records Life Cycle

The term ***Records Life Cycle*** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

Documents and Records

In this policy, ***Documents*** are defined as recorded information, in any form, created or received by the Trust. A document used in the transaction of the Trust's business or conduct of affairs that will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations becomes a **'record'**.

Information

Information is a corporate asset. All data and Trust's records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

Information Asset

Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation. This would include all databases/systems and applications and all manual records.

Person Identifiable / Confidential Information

Person identifiable / confidential information is information which could singly or compositely identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and private address or postcode, name and home telephone number etc.

All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. This includes the nationally recognised NHS number.

Sensitive Information

This is information where loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community.

This is wider than, but includes, data defined as sensitive under the Data Protection Act 2018 and the United Kingdon General Data Protection Regulation (UK-GDPR).

In addition to personal and clinical information, financial and security information is also likely to be deemed "sensitive".

Examples of sensitive information include information in relation to a person's:

- Health or physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Political views
- Criminal convictions
- Trade Union Membership

For this type of information even more stringent measures should be employed to ensure that the data remains secure.

Clinical Information

The term clinical records refers to recorded information, in any form, created or received and maintained by the Trust relating to the documentation of patient care and treatment. This includes but is not limited to the following:

- ✓ Patient health records (electronic or paper-based), and concerning all specialities;
- ✓ Records of private patients seen on NHS premises;
- ✓ Accident and Emergency, birth and other registers;
- ✓ Theatre, minor operations and other related registers;
- ✓ X-Ray and imaging reports, outputs and images;
- ✓ Photographs, slides, and other images;
- ✓ Microform (i.e. microfiche/microfilm);
- ✓ Audio and video tapes, cassettes, CD-ROMS etc.;
- ✓ E-mails relevant to patient care;
- ✓ Computerised records i.e. clinical records in all electronic formats;
- ✓ Scanned documents relevant to patient care.
- ✓ Letters relevant to patient care;
- ✓ Hand-Over sheets;
- ✓ Diaries relevant to patient care;
- ✓ MDT Lists;
- ✓ Medical Reports and;
- ✓ Clinical Trials/Audit information.

The term 'health record' (i.e. clinical record) is defined by Data Protection Act 2018 and the UK-GDPR and means any record which:

"Consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a healthcare professional in connection with the care of that individual."

Corporate / Non Clinical Information

The term corporate records or non-clinical records includes but is again not limited to the following:

All records relating to:

- ✓ Estates/Engineering;
- ✓ Information Management & Technology (IM&T);
- ✓ Personnel/Human Resources;
- ✓ Financial;
- ✓ Purchasing/Supplies;
- ✓ Complaints.

Examples would include:

- ✓ Policies
- ✓ Standard Operating Procedures
- ✓ Minutes of Meetings
- ✓ Terms of Reference
- ✓ Budget Statements
- ✓ Project Plans
- ✓ Action Plans
- ✓ Contracts
- ✓ Personnel Records
- ✓ Disciplinary Records
- ✓ Payroll Records
- ✓ Staff Surveys
- ✓ Training Records
- ✓ Audit Records

THE PROCESS

Aims of the Records Management System

Records must be maintained in a system that ensures they are properly stored and protected throughout their life cycle; this includes all electronic records, including any records that are migrated across to new systems, as well as all manual records. Therefore, before procuring new systems or putting new processes in place, organisations should take into account the need to keep up with technological progress (e.g. new hardware, software updates) to ensure that records remain accessible and retrievable when required.

The aims of the Trust's Records Management System are to ensure that:

- **records are available when needed** - from which the Trust is able to form a reconstruction of activities or events that have taken place;

- **records can be accessed** - records and the information within them are grouped in a logical structure to ensure quick and efficient filing and retrieval and so that they can be located and displayed in a way consistent with its initial use, and that the **current version is identified** where multiple versions exist. This will also aid implementation of authorised disposal arrangements, i.e. archiving or destruction;

- **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, the business process, 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. There should be suitable storage areas so that records, whether physical or electronic, remain accessible and usable throughout their life cycle, this includes ensuring that technological upgrades are supported;

- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails track all access (e.g. sign in/out logs or computer generated audit trials), use and changes. A variety of security measures should be implemented for example, authorised access to storage and filing areas, lockable storage areas, user verification, password protection and access monitoring. This would also include maintaining a log of when records are issued form and/or returned from storage areas on site or to authorised off-site facilities;

- **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 record management; and

- **cross-referencing** of electronic records to their paper counterparts (where dual systems are maintained). A formal assessment should be undertaken and reviewed by the Corporate Records Management Group or Clinical Health records Group, depending on the nature of the information, where duplicate records are required to be retained.

Inventory of Record Collections

The Trust will establish and maintain mechanisms through which departments and other units should register the records they are maintaining. The inventory will be reviewed annually. The inventory of record collections will facilitate:

- the classification of records into series;
- the recording of the responsibility of individuals creating records; and
- the auditing of records management practices.

Creation of Records

Record creation is one of the most important processes in records management and all departments should create good records in an effective system. However, creating a record is not enough unless the record is then captured or filed into a filing system created and managed by the organisation.

It is important that records are kept in their context and the best way to achieve this is to file or classify them. Records cannot be tracked or used efficiently if they are not classified or if they are classified inappropriately. Records captured or filed in a corporate filing system will possess some of the necessary characteristics to be regarded as authentic and reliable. Whatever the format of the records, they should be saved into a proper records management system.

A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily.

Staff should be aware of the differences between a document and a record. A document, as defined above, is any piece of written information in any form, produced or received by an organisation or person. It can include databases, website, email messages, word and excel files, letters, and memos. Some of these documents will be ephemeral or of very short-term value and should never end up in a records management system (such as invitations to lunch).

Some documents will need to be kept as evidence of business transactions, routine activities or as a result of legal obligations, such as policy documents. These should be placed into an official filing system and at this point, they become official records. In other words, all records start off as documents, but not all documents will ultimately become records.

Basic rules to follow when creating records:

- All documents should have a clear descriptive name that is meaningful to the department responsible for the record and that would give a clear indication of the contents of the record to anybody else.
- All documents should have a unique reference that is meaningful to the department responsible for the record.
- All documents should use version control and version numbers should be changed each time the document is amended. Previous versions should be retained for an appropriate period depending on the nature of the information within the document.
- All records and documents should be filed in an appropriately structured filing system
- Records should have a protective mark applied where appropriate.

Logging A Query

From time to time it may be necessary to amend a record. This may be as the result of a query on behalf of the patient or member of staff and may include demographic or clinical information. Extreme caution should be exercised in such circumstances and staff need to be aware that it is not acceptable to alter a record without appropriate authorisation.

If a request is received to amend/alter a patient record the process to follow should be:

- In the case of demographic information (incorrect name/address/DOB etc.) staff should contact the Medico-Legal Team to advise of the request, the reason behind the request and the details of the requester

- The Medico-Legal team will review the request, ensure legal authorisation for access to the record and the validity of the request

- The Medico-Legal team will authorise any amendment and will make arrangements for the amendment to be made.

- In the case of amendment to clinical information, staff should contact the relevant consultant in charge – who will review the information and the proposed change

- If the request to alter is a valid request, the consultant in charge can authorise the amendment and arrange for the change to be made (making a notation in the record to that effect)

- Where the consultant in charge does not agree that the change is a valid request and is not prepared to authorise, the Medical Director and the Director of Information should be notified to provide advice and guidance on next steps

Naming Conventions

Naming conventions should:

- give a unique name to each record;
- give a meaningful name which closely reflects the records contents;
- express elements of the name in a structured and predictable order;
- locate the most specific information at the beginning of the name and the most general at the end;
- give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).

Filing structures

A clear and logical filing structure that aids retrieval of records should be used. Ideally, the filing structure should reflect the way in which paper records are filed to ensure consistency. However, if it is not possible to do this, the names allocated to files and folders should allow intuitive filing.

Filing of the primary record to local drives (i.e. C drive usually 'my documents') on PCs is not permitted and on laptops is strongly discouraged.

The agreed filing structure should also help with the management of the retention and disposal of records.

File and Folder Referencing

A referencing system should be used that meets the organisation's divisionals needs, and can be easily understood by staff members that create documents and records. Several types of referencing can be used, for example, alphanumeric; alphabetical; numeric or keyword.

The most common of these is alphanumeric, as it allows letters to be allocated for a business activity, for example, HR for Human Resources, followed by a unique number for each record or document created by the HR function.

It may be more feasible in some circumstances to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format.

Tracking and Tracing

There should be tracking and tracing procedures in place that enable the movement and location of manual records to be controlled and provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a record is physically removed from or returned to its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

Tracking mechanisms to be used should include:

- the item reference number or identifier;
- a description of the item (for example the file title);
- the person, position or operational area having possession of the item;
- the date of movement.

Examples of systems for monitoring the physical movement of records include:

- location cards;
- index cards;
- docket books;
- diary cards;
- transfer or transit slips;
- bar-coding;
- computer databases (e.g. electronic document management systems);

All patient case notes/health records should be tracked on the patient administration system (PAS) in line with the Trust's case note tracking procedure.

The movement of any other manual records, including other clinical information that does not form part of the health records should be tracked.

The system adopted should maintain control of the issue of records, the transfer of records between persons or operational areas, and return of records to their home location for storage.

The simple marking of file jackets to indicate to whom the file is being sent is not in itself a sufficient safeguard against files going astray.

All records tracking systems should include regular records audits and monitoring procedures.

Appraisal, Retention and disposal

NHSEI have had a blanket legal hold on the disposal of any records since January 2018 to comply with various Independent Inquiries including the Infected Blood Inquiry (IBI) and the Independent Inquiry into Child sexual Abuse(IICSA) , therefore all records should be being retained until further notice.

Records relating to our Covid 19 response will need to be retained in line with a major incident, and therefore it is likely that a 30 year retention will apply and no records or information should be destroyed until further notice.

Further details of our response to these enquiries is documented within the Procedure for the preservation, retention, security and destruction of health/corporate records.

It is a fundamental requirement that all of the Trust'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 Trust's business functions.

The destruction of records is an irreversible act, while the cost of preserving records worthy of permanent preservation is high and continuing.

The Trust has adopted the retention periods set out in the Records Management: Code of Practice 2023, a copy of which is published on the Trust's intranet – see the Health Records or Information Governance & Security microsite.

The updated Code of Practice has a useful search function for searching the retention schedule. https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule

Records should be reviewed regularly and destroyed when the retention period set out with the Records Management: NHS Code of Practice is met. If a need to retain records beyond this period is established the manager responsible for the records should submit a risk assessment to the clinical health records group or corporate records management group, depending on the nature of the records, stating the reasons why the records need to be retained.

The retention schedules identify minimum retention periods and a local review will determine whether records are to be selected for permanent preservation, destroyed or retained by the organisation for research or litigation purposes. Whatever decisions are made they must be documented as part of a consistent and consistently applied records management policy within the organisation.

The health records manager must ensure that inactive health records are reviewed regularly, moved to secondary storage when appropriate and ultimately disposed of in a secure manner at the end of their designated retention period.

The guidelines shown below must be followed when using the retention schedules:

I. Retention periods in the retention schedules in Records Management: NHS Code of Practice are minimum retention periods and therefore local business requirements/instructions must be considered before applying retention periods in the schedules. A risk assessment should be completed where a need to retain records beyond the period documented in the NHS Records Management Code of Practice is identified.
II. Local decisions should be considered where the final action is destruction bearing in mind the need to preserve records, the use of which may not be predictable at the present time, but which may be of historic value. NHS organisations should take advice from their local approved Place of Deposit or from The National Archives;
III. Recommended minimum retention periods should be calculated from the end of the calendar year following the last entry in the record (date of last patient contact) or other specified dates as shown in the national retention schedules;
IV. The selection of files for permanent preservation is partly informed by precedent (the establishment of a continuity of selection) and partly by the historical context of the subject (the informed identification of a selection).
V. The provisions of the Data Protection Act 2018 and the UK-GDPR must also be complied with, throughout a record's lifecycle and it is necessary to provide secure storage for them. There is also a data protection requirement not to keep personal data for longer than necessary taking account of the purpose for which it was collected;
VI. The Department of Health is considering a proposal to establish a national selection policy. This policy could identify regions in which records of a specialty would have precedence in selection for permanent preservation because of a history of regional excellence or innovation in a particular discipline. The schedule does not seek to cater for all eventualities and therefore the responsible records managers need to consider whether exceptional circumstances (e.g. events of local or national significance reflected in the records) necessitate the long-term preservation of the records. It is intended that the national

Retention Schedules will be regularly updated to reflect and incorporate new and additional records types and series.

When developing or purchasing new systems the organisation should consider how retention/disposal periods will work or can be factored into the system. For paper corporate records, this may be using clearly marked labels on each folder to state the minimum retention period, and a log kept so that records can be easily appraised.

Electronic document management systems, such as the Trust's intranet, may have the functionality built within them to set the disposal period for a record based on certain defined rules.

Methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records. If contractors are used, they should be required to sign confidentiality undertakings and to produce written certification as proof of destruction.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. There is a template included as an appendix of the Trust's confidential waste policy, which can be used to record the disposal of all types of records. Disposal schedules would also constitute the basis of such a record.

Scanning of Records

BS 10008 and BIP 0008 Code of Practice standards relate to “Evidential weight and legal admissibility of information stored electronically” so that they can be relied upon in Court (Civil Evidence Act 1995). We must comply with these standards when scanning health records.

None health records also require formal documented procedures in place to ensure the integrity of records, including storage and retrieval and, auditable records of your scanning activities.

All departments and services must ensure that they follow the Trusts ‘Records Scanning Policy and Audit Methodology’. This provides the Trust with a formal assurance process to ensure the appropriate governance arrangements are in place to satisfy our legal requirements to maintain confidentiality, integrity and availability of information for records that have been scanned into digital format with the ultimate aim of destroying the original record.

Selection of NHS Records for Permanent Preservation

All NHS records are public records under the terms of the Public Record Act 1958. The timescale for retention of Public Records is reducing, over a 10 year period, from 30 to 20 years. Records selected for permanent preservation must be transferred to the Public Record Office (PRO) or kept in a place of deposit, appointed under S.4(1) of the 1958 Act. In general, records worthy of preservation from NHS organisations are appropriate for deposit in the nearest Local Authority Record Office, which has been approved by The National Archives. In a very few instances individual hospitals have made suitable arrangements and have themselves been appointed as places of deposit. It should be borne in mind that the National Archives expects the standards of storage and access to records in places of deposit to match those found in the National Archives.

The relevant standards are set out in the National Archives' own guidance Beyond the PRO: Public Records in Places of Deposit. The new standard for records repositories is available on the National Archives Website:-

http://www.nationalarchives.gov.uk/archives/framework/pdf/standard2005.pdf

Free copies of this document, and information about the nearest or most appropriate place of deposit for the records of particular NHS institutions, can be obtained from the Head of Archive Inspection, The National Archives, Kew, Richmond, Surrey, TW9 4DU (Tel: 0181-392-5262). As the resource implications of being appointed as a Place of Deposit are likely to be significant, it is strongly recommended that any NHS organisation considering making an application should first contact the National Archives Head of Archive Inspection at an early stage. It is highly unlikely that an application will succeed without a firm commitment to employ a professionally qualified archivist.

Records selected for archival preservation and no longer in regular use by the organisation should be transferred as soon as possible to an archival institution appointed by the Keeper of Public Records, exercising powers under S.4(1) of the 1958 Public Records Act, which have been delegated to her by the Lord Chancellor (for example a Place of Deposit that has adequate storage and public access facilities - see Annex E of the NHS Code). In most cases the appropriate Place of Deposit is the nearest local authority record office.

Non-active records should be transferred from creation of the record, as required by the *Public Records Act 1958*. A log of all records retained off-site should be maintained by the Trust and this log should be reviewed regularly by the Corporate Records Management Group and the Clinical Health Records Group.

Notes on Preservation of Patient Records for Historical Purposes

In the light of the latest trends in medical and historical research, it may be appropriate to select some records for permanent preservation. Selection should be performed in consultation with health/care professionals, and archivists from an approved Place of Deposit;

General rules should be drawn up locally regarding permanent preservation of records, using the profile of material which has already been selected, and the history of the organisation (including pioneering treatments and examples of excellence) within the context of the service provided to the local and wider communities;

If records are to be sampled, specialist advice should be sought from the same health/care professionals and archivists;

If an entire collection of patient records is not considered worthy of permanent preservation but nevertheless contains some material of research value, then the option of presenting these records to local record offices and other institutions under s.3(6) of the Public Records Act 1958 should be considered. Advice on the presentation procedure may be obtained from the National

Archives' Archive Inspection Services but requests should be submitted to the Corporate Records Group or Clinical Health Records Group in the first instance;

Similarly if an entire collection of patient records is considered worthy of permanent preservation but there is a lack of space in the relevant Place of Deposit to store these records, it may be appropriate to make a microfilm copy and then destroy the paper originals. Microfilms should be produced in accordance with the British and International Standard BS ISO 6199: 1991, copies of which can be purchased from the British Standards Institute.

Disposing of Unwanted Records

How long should records be retained?

The length of the retention period depends upon the type of record and its importance to the activities of the Trust. NHS England's NHS Records Management Code of Practice 2023 takes account of legal requirements and sets out the minimum retention periods for both clinical and corporate records. The Trust has, however, discretion to keep records for longer, subject to a risk assessment detailing local needs, affordability and, where records contain personal information, the requirements of the Data

Protection Act 2018 and the UK-GDPR. The retention schedule may not be a complete list of every type of record and the Trust may need to seek advice about the appropriate retention

periods for record types not contained in the Schedule. In the first instance the Trust's health records manager or Information Governance department should be consulted.

Who makes the decision?

There are two principal options for disposal of records - to destroy or to dispose for example, by passing on to another organisation. As can be seen from the Retention and Disposal Schedule, some records have fixed retention periods, whilst others will need more careful consideration. In many cases the staff in the department which ordinarily uses them should be able to decide. If not specialist guidance should be sought via the Department of Health's Records Management Mailbox recordsmanagement@dh.gsi.gov.uk

Operational managers are responsible for ensuring that all records are periodically and routinely reviewed to determine what can be disposed of in the light of local and national guidance. The Trust's Information Governance & Security Group has been established to advise on local policy, particularly for the retention, archiving, or disposal of sensitive personal health records.

What are the options for disposal?

Most Trust records should be destroyed as soon as practicable after the expiry of the relevant minimum retention period, but there are other options for disposal. Because the destruction of records is an irreversible act, it is vital to consider all the available options in order to arrive at the right decision.

Disposal does not just mean destruction. It can also mean the transfer of records from one type of media to another e.g. paper to microfilm or to computer; or from one user to another. It could involve depositing records with an organisation which wishes to carry on using it e.g. a hospital or Local Authority Record Office, the National Archives or another bona fide research body, for example a university or established research institute recognised by a Local Research Ethics Committee, or to commercial off-site storage if the organisation wishes to retain the records in original paper format but does not have the storage space available within its premises, as previously stated a log of all records retained off-site should be maintained by the Trust and this log should be reviewed regularly by the Corporate Records Management Group and the Clinical Health Records Group. Advice about these options (and the implications of the Public Record Act) is available from the National Archives.

What are the rules for destruction?

NHS health records contain sensitive and confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record including destruction and that the method used to destroy such records is fully effective and ensures their complete illegibility. Trust health records must be destroyed in accordance with the principle set out in the Trust's confidential waste policy. This can be undertaken on-site, or via an approved contractor, but it is the responsibility of the Trust to satisfy itself that the methods used throughout the process provide adequate safeguards against accidental loss, or disclosure of health record contents. It is a requirement of the Records Management: NHS Code of Practice that a record of destruction of individual health records (case-notes) is retained permanently. Where a contractor is used to destroy health records, they must be required to sign confidentiality undertakings and to produce

written certification as proof of destruction. This certificate will then form part of the record of destruction.

CLINICAL RECORDS MANAGEMENT PROCEDURE

The Trust's procedure for the management of its clinical records is detailed in Appendix 1.

The organisation has approved documentation which describes the process for managing the risks associated with clinical records in all media.

Tracking

Accurate recording and knowledge of the whereabouts of all records is crucial if the information they contain is to be located quickly and efficiently. One of the main reasons why records get misplaced or lost is because the next destination is not recorded anywhere

Tracking mechanisms should record the following (minimum) information

- The item reference number or other identifier
- A description of the item (e.g. the file title)
- The person, unit or department, or place to who it is being sent
- The date of transfer to them

Process for tracking the main hospital record

There is an electronic process for tracking the main hospital record through the PAS system and all appropriate staff will receive training in using the electronic system. Ongoing support and training is available within the Trust by a dedicated trainer.

Process for tracking A&E Admissions

Where an admission occurs as the result of an A&E attendance, the appropriate pro-forma is to be completed (either medical or surgical). Where the casenote has arrived at A&E, the pro-forma is to be filed before transfer to the ward. Where the casenote is not available to A&E staff, the pro-forma is to accompany the patient to the ward whereby the admitting Ward staff to be responsible for ensuring that the admissions pro-forma is filed within the notes appropriately.

Manually operated tracking systems

The following methods for manually tracking the movement of active records are suggested (specifically for community health records or those records held within departments):

- A paper register - a book, diary or index card to record transfers
- File " absence" or "tracer" cards put in place of absent files

- Record on a computer data base

Those teams using such manual tracking process to produce and have available procedure/guidance documentation to detail the local process.

Process for creating hospital health records

The process for the creation of records within the organisation is as followed and is a set standard for the organisation and all staff creating clinical records:

- Search the MPI (Master Patient Index) for the patient (see Patient Management System (PMS) procedure for Searching MPI)
- If the patient is not already recorded on MPI interrogate the National Strategic Tracing Service (NSTS) database for NHS number
- Search the MPI by NHS number to ensure the patient is not registered under a different name/address/date of birth
- If patient not found on MPI, register patient using ORE function. The Basic Details screen must be completed in full
- PMS will then require a casenote to be allocated. All casenotes should be allocated to "Main" file. NB: No physical record will be created until requested e.g.: by Emergency Admissions or Outpatients
- The patient' Registered GP details must be completed and any other Registration Details provided
- To complete the process an episode must be opened (see PMS procedure)
- To register a patient without an episode use PMI function following the above procedure. Use option 3 "casenotes" to allocate a casenote.

Process for creating community-based health record

Community services must adhere to the documented process for creating local health records. Copies of the local processes are available from the Integrated Care Division.

Process for retrieving records

To ensure that clinical records are retrieved in an effective timely manner the following process is to be followed:

Placement of files/records	Method for retrieving

Case notes are in the Health Records Library	Files are removed from the library storage system where they are kept in numerical order according to unique patient ID number
Hospital case notes held outside of the Health Records Library	To be tracked on PAS to requesting department, with clear instructions to advise of further movement.
Community case notes	To be tracked using the locally-approved manual tracking system (as outlined in section 7.4 above)
Case notes stored as digital image	The system and individual files are password protected. Training is given to all appropriate staff to enable effective use of the system. User enters individual password to access system, enter unique patient ID number to bring up patient notes for viewing.
In the case of missing/misfiled notes	Staff should following the procedures laid out in the Management of Patient Casenote Procedure attached as Appendix 4
In the case of records stored within the organisation's Archive Facility - Deepstore	Staff should follow the procedure laid out in Appendix 8 – A Guide to Deepstore Procedures

TRAINING

The Trust is audited on Data Security Awareness Mandatory Training Compliance as part of the Data Security and Protection Toolkit on an annual basis. The training is a requirement of all staff, regardless of roles.

Additional role-based training is required for Information Asset Owners and Information Asset Administrators.. Training compliance for IAOs and IAAs is recorded on the IAR against each asset.

MONITORING COMPLIANCE

The Trust is committed to ensuring compliance with documents and will actively monitor the effectiveness of such documents.

Process for monitoring compliance with this policy

CQC Regulated Activities	Process for monitoring e.g. audit	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/ group/ committee for review of results	Responsible individual/group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring action plan and implementation
	Internal Audit Data Protection and Security Toolkit External Audit	Information Governance & Security Group	Annually	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group

The Trust will regularly monitor and audit its records management practices for compliance with this policy.

The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to processes, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to both the policy and clinical record keeping guidance is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of audits will be reported to the Divisional Quality Boards, and Quality Governance Committee, as appropriate.

The Information Commissioner may also mandate an audit upon the Trust at any time.

Process for monitoring e.g. audit	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual / group/ committee for review of results	Responsible individual/ group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring of action plan
<u>NHSLA Monitoring</u> Records Management Policy (Clinical Records) Ad hoc audit across all Divisions to include: • Duties • Tracking records • Creating records • Retrieving records • Retention, disposal and destruction of records	Health Records Management Team	Annually	D&CS Quality Board	Health Records Management Team	Health Records Management Team
<u>Internal Monitoring</u> • Health Records Quality Dashboard • Health Records Annual Report	Health Records Management Team Health Records Manager	Monthly Annually	D&CS Divisions D&CS Quality Board	Health Records Management Team Health Records Management Team	Health Records Management Team Health Records Management Team
<u>NHSLA MONITORING</u> Standards of Health Records Planned audit to include: • Basic record-keeping standards • Contemporaneous record of care • Monitoring compliance with above.	Clinical Audit Team / Leads	Monthly	Divisional Quality Boards	Divisional Quality Boards	Divisional Quality Boards
Data Secuirty and Protection Toolkit Assessment	Information Governance & Security Group	Annually	Information Governance & Security	Information Governance & Security Group	Information Governance & Security Group

			Group		
Internal Audit	Information Governance & Security Group	Annually	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group
External Audit	Information Governance & Security Group	Ad hoc	Information Governance & Security Group	Information Governance & Security Group	Information Governance & Security Group

DOCUMENT LAUNCH AND DISSEMINATION

Launch

The responsibility of implementing this document, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff (including agency staff) to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

This document has been compiled by the Information Governance Team in consultation with Governance Leads for each Division by means of the Information Governance

Dissemination

The responsibility of implementing this document, including training and other needs that arise shall remain with the author. Line managers have the responsibility to cascade information on new and revised policies/procedures and other relevant documents to the staff for which they manage.

Line managers must ensure that departmental systems are in place to enable staff (including agency staff) to access relevant policies, procedures, guidelines and protocols and to remain up to date with the content of new and revised policies, procedures, guidelines and protocols.

This document has been compiled by the Information Governance Team in consultation with Governance Leads for each Division by means of the Information Governance Steering Group.

Once finalised, the document will be presented to the Quality Governance Committee. The document will then be displayed on the Information Governance & Security microsite on the Trust's intranet and on the Trust's website. Managers and Governance leads should ensure the information is cascaded to all staff.

This Policy will be reviewed annually or more frequently if appropriate to take into account changes to legislation that may occur, and/or guidance from the Department of Health, the NHS Executive and/or the Information Commissioners Office (ICO).

This policy is directly referenced to BS 1008 and any changes to policy need to be checked for compliance

REFERENCES AND ASSOCIATED DOCUMENTATION

Information Governance Policy
Information Security Policy
Information Governance & Security Incident Reporting/Management - SOP
IT Acceptable Use Policy
Mobile Devices & Removable Media Security Policy
Remote Access & Mobile Working Policy
Photography/Video & Audio Records of Patients
Access to Personal Information (Subject Access) Policy
Data Quality Policy
Freedom of Information Policy
Information Sharing and Transfer of Records Policy
Records Management Strategy
Confidential Waste Policy
Disciplinary Policy
Clinical Audit Standard Operating Procedure
BS 10008 – Evidential weight and legal admissibility of electronic information
Health Record Procedures
Health Record Keeping Standards
Case Note Tracking SOP
Registration of Patients SOP
Retrieval of Health Records SOP
Out of Hours Access to Health Records Libraries and Retrieval of Case Notes SOP
Filing SOP
Storage of Health Records SOP
Procedure for the preservation, retention, security and destruction of health/corporate records.
Iron Mountain Storage and Retrieval SOP
Iron Mountain Returns SOP
General Procedures for Optical Imaging SOP
Identifying Case Notes for Sorting SOP
The Records Scanning Policy and Audit Methodology

EQUALITY IMPACT ASSESSMENT

Office Use Only

Submission Date:	*27.11.24*
Approved By:	*IGSG*
Full EIA needed:	Yes/No

Equality Impact Assessment – Policies, SOP's and Services not undergoing re-design

1	**Name of the Policy/SOP/Service**	Information Lifecycle & Records Management Policy	
2	**Department/Division**	Information Governance/IM&T	
3	**Details of the Person responsible for the EIA**	**Name:**	Joan Carr
		Job Title:	I.G. Co-ordinator
		Contact Details:	Joan.carr@stockport.nhs.uk
4	**What are the main aims and objectives of the Policy/SOP/Service?**	To provide guidance to staff on the requirements, legislative and mandatory, with regard to managing Trust records.	

For the following question, please use the EIA Guidance document for reference:

5	**A) IMPACT** **Is the policy/SOP/Service likely to have a differential impact on any of the protected characteristics below? Please state whether it is positive or negative. What data do you have to evidence this?** **Consider:** • What does existing evidence show? E.g. consultations, demographic data, questionnaires, equality monitoring data, analysis of	**B) MITIGATION** **Can any potential negative impact be justified? If not, how will you mitigate any negative impacts?** ✓ Think about reasonable adjustment and/or positive action ✓ Consider how you would measure and monitor the impact going forward e.g. equality monitoring data, analysis of complaints. ✓ Assign a responsible lead. ✓ Produce action plan if further

	complaints. • Are all people from the protected characteristics equally accessing the service?	data/evidence needed ✓ Re-visit after the designated time period to check for improvement. **Lead**	
Age	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of age – this is a corporate policy which does not deal with specific identifiable subjects	
Carers	No Differential Impact	There is no differentiation within the policy relating to Carers/People with caring responsibilities – this is a corporate policy which does not deal with specific identifiable subjects	
Disability	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of disability – this is a corporate policy which does not deal with specific identifiable subjects	
Race / Ethnicity	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of race/ethnicity – this is a corporate policy which does not deal with specific identifiable subjects	
Gender	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of gender – this is a corporate policy which does not deal with specific identifiable subjects	
Gender Reassignment	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of gender reassignment – this is a corporate policy which does not deal with specific identifiable subjects	
Marriage &	No Differential Impact	There is no requirement to	

Civil Partnership		differentiate the content of the policy on the basis of marriage or civil partnership – this is a corporate policy which does not deal with specific identifiable subjects	
Pregnancy & Maternity	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of pregnancy and maternity – this is a corporate policy which does not deal with specific identifiable subjects	
Religion & Belief	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of religion and belief – this is a corporate policy which does not deal with specific identifiable subjects	
Sexual Orientation	No Differential Impact	There is no requirement to differentiate the content of the policy on the basis of sexual orientation – this is a corporate policy which does not deal with specific identifiable subjects	
General Comments across all equality strands	This Policy is available in other formats where required.		

Action Plan

What actions have been identified to ensure equal access and fairness for all?

Action	Lead	Timescales	Review & Comments

EIA Sign-Off	**Your completed EIA should be sent to Equality, Diversity & Inclusion Manager for approval:** equality@stockport.nhs.uk **0161 419 4784**

Quality

(Clinical and Quality Impact Assessment, Please record 'No Impact' if this is the case)

Date of Initial Review	18/11/2021
Date of Last Review	18/11/2021

Area of Impact		Consequence	Likelihood	Total	Potential Impact	Impact (Positive or Negative)	Action	Owner
Quality	**Duty of Quality**				How does it impact adversely the rights and pledges of the NHS Constitution?	No Impact		
					How does the impact affect the organisation's commitment to being an employer of choice?	No Impact		
				0	What is the equality impact on race, gender, age, disability, sexual orientation, religion and belief, gender reassignment, pregnancy and maternity for individuals' access to services and experience of the service?	No Impact		
	Patient Safety			**0**	How will this impact on the organisation's duty to protect children, young people, and adults?	No Impact		

					How will it impact on patient safety? • Infection rates • Medication errors • Significant untoward incidents and serious adverse events • Mortality & Morbidity • Failure to recognise a deteriorating patient • Safe staffing levels	No Impact		
					How will it impact on preventable harm? (e.g. slips, trips, falls)?	No Impact		
					How will it impact upon the reliability of safety systems? (e.g. WHO checklist)	No Impact		
					How will it impact on systems and processes for ensuring that the risk of healthcare acquired infections is reduced?	No Impact		
					How will this impact on workforce capability, care and/or skills?	No Impact		
Experience	**Patient Experience**			**0**	What impact is it likely to have on self-reported experience of patients and	No Impact		

					service users? (Response to national / local surveys / complaints / PALS/incidents)			
					How will it impact on choice?	No Impact		
					Will there be an impact on waiting times?	No Impact		
					How will it impact upon the compassionate and personalised care agenda?	No Impact		
	Staff Experience			**0**	How will it impact on recruitment of staff?	No Impact		
					What will the impact be on staff turnover and absentee rates?	No Impact		
					How will it impact on staff satisfaction surveys?	No Impact		
Effectiveness	**Clinical Effectiveness and Outcomes**			**0**	How does it impact on implementation of evidence-based practice?	No Impact		
					How will it impact on patient's length of stay?	No Impact		
					Will it reduce/impact on variations in care? (e.g. readmission rates)	No Impact		
					What will the impact be upon clinical and cost-effective care	No Impact		

					delivery?			
					How does it impact upon care pathway(s)? e.g. Mortality	No Impact		
					How will it impact on target performance?	No Impact		
Other	**Please use this section to detail any other impacts to clinical and quality that are not listed in the questions.**							

Data Protection Impact Assessment

Organisations must ensure that any third parties used to process or share personal confidential data with, will ensure the data is secure and confidential and a data processing or information sharing agreement will need to be in place.

To assess the implications of using personal data, a risk assessment called a Data Protection Impact Assessment (DPIA) is required to ensure the Trust is complying with its legal obligations under the Data Protection Act 2018 and UK GDPR

If you are doing any of the following you will need to complete a Data Protection Impact Assessment (DPIA):

- Setting up a new process using personal confidential data (PCD) that identifies individuals.
- Changing an existing process which changes the way personal confidential data is used
- Procuring a new information system which holds personal confidential data

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

The DPIA Process:
1) Complete the screening questions below – this is to determine whether or not completion of a full DPIA is required.
2) If a full DPIA is required, you will be advised by the Information Governance Team and sent the full DPIA proforma for completion.

If DPIA's are not completed, there may be data protection concerns that have not been identified which could result in breaching the Data Protection Act/GDPR.

Advice/Guidance on completing the screening questions or the full DPIA can be provided by the Information Governance (IG) Team by emailing details of the initiative to: Information.governance@stockport.nhs.uk

DPIA Screening Questions

		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification on why it is not an issue*
A)	Will the process described involve the collection of new information about individuals?		x		
B)	Does the information you are intending to process identify individuals (e.g. demographic		x		

	information such as name, address, DOB, telephone, NHS number)?				
C)	Does the information you are intending to process involve sensitive information e.g. health records, criminal records or other information people would consider particularly private or raise privacy concerns?		x		
D)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		x		
E)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?		x		
F)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		x		
G)	Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition		x		
H)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?		x		
I)	Will the initiative compel individuals to provide information about themselves?		x		

1. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and

extends to monitoring the records of senders and recipients as well as the content of messages.

If you answered YES or UNSURE to any of the above, you need to inform the IG team and continue with the full Data Protection Impact Assessment. Giving false information to any of the above that subsequently results in a yes response that you knowingly entered as a NO may result in an investigation being warranted which may invoke disciplinary procedures.

DOCUMENT INFORMATION

Type of Document	Policy
Title	Information Lifecycle & Records Management
Version Number	V10.1
Consultation	Digital and Informatics Group
Recommended by	Information Governance & Security Group
Approved by	Information Governance & Security Group
Approval Date	27th November 2024
Next Review Date	November 2026
Document Author	Information Security and Records Manager
Document Director	Director of Informatics
For use by	All Trust employees
Specialty / Ward / Department (*if local procedure document*)	

Version	Date of Change	Date of Release	Changed by	Reason for Change
10.1	Nov 2024	Nov 2024	RA	Updated reference to Code of practice 2023
10.00	Nov 2022	Nov 2022	JC	Update of Business to Division, titles and F&P to DIG
9.1	December 2021	Dec 2021	RA	Removed Records Management Group from roles and responsibilities. Updated Code of practice referenced to 2021 Code of Practice. Added further details around scanning audit policy and methodology. Added the clinical and quality impact assessment and DPIA screening questions as per updated Policy template.

8.0	Nov 2020	Nov 2020		New Trust format
7.2	Oct 2018	Oct 2018		Updating of legislation references
7.1	Apr 2018	Apr 2018		GDPR references included
7.0	Sep 2017	Sep 2017		Refresh Change of Title to include 'Information Lifecycle' Update of responsibilities to reflect current structure
6.2	Mar 2015	Mar 2015		Inclusion of paragraph to formalise query logging process
6.1	Feb 2015	Feb 2015		Inclusion of role specific information with regard to SIRO post
6.0	Sep 2014	Sep 2014		Clarification of the change in framework with regards to the now defunct Clinical Health Records Management Group Removal of job specific information with regard to SIRO post Addition of Clinical Audit team to Roles & Responsibilities Inclusion of BS1008 information Clarification of process for monitoring
5.1	Sep 2013	Sep 2013		No Changes
5.0	Aug/Sep 2012	Aug/Sep 2012		No Changes
5.0	Jun 2012	Jun 2012		Overarching Records Management Policy and Health Records Management policy combined.
3.0 / 4.0	Nov 2011	Nov 2011		Reference numbers of previous versions of the Health Records Management Policy
2.0	Nov 2011	Nov 2011		Adopted the new Trust Policy format. Significant Changes Made.
1.1	Nov 2007	Nov 2007		Policy Issued
1.0	Oct 2007	Oct 2007		Policy Developed