OP07 Health Records Policy

Contents

1.0 Policy Statement

Information contained within the health record is critical to the delivery of safe and appropriate health care. For the purposes of this policy the health record is the legal document relating to an individual's care and treatment, regardless of the format this is available in e.g. paper, electronic, clinical images.

The purpose of this policy is to provide a structure to ensure adequate health records are maintained and that all aspects of an individual's health record, in any format or media type, from creation through to destruction, are controlled effectively to comply with legal and operational needs.

This policy applies to all staff that handle or contribute to the health record. It follows the health record lifecycle: creation, management and maintenance, security, storage, distribution, retention, appraisal and destruction. The principles apply to all health records, including areas where separate records are held e.g. Primary Care Services, Sexual Health, Adult Community Services.

This policy applies to all Trust employees, be they employed as permanent, fixed term or temporary contracts, contractors, students and volunteers. It also applies to external contractors who are employed to carry out work on behalf of the Trust, whether this is a temporary or time limited capacity. Third parties will be notified of their duties in the terms and conditions of their contract. Each individual is responsible for ensuring that they comply with relevant legislation and guidance for protecting the data they use.

This policy will ensure that the key data protection principles lie at the heart of our approach to the processing of patient information within the Health Record, as detailed in OP13 Information Governance and Data Protection Policy in Appendix A and Attachment 3.

In adhering to this policy, all applicable aspects of the Conflicts of Interest Policy (OP109) must be considered and addressed. In the case of any inconsistency, the Conflict of Interest Policy is to be considered the primary and overriding Policy.

2.0 Definitions

Records Management – a system to govern the processing of a patient health record, throughout its lifecycle. Records management processes must be legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record.

Health Record – includes any material created as part of the care and treatment of a patient. Such materials can be in any format e.g. written, electronic, clinical images, audio or video recordings, x-rays, test results, clinic letters, emails, minutes, research and investigations.

Subject Rights Request (SRR) – is a request made by the patient to exercise their rights under the provisions of the Data Protect Act 2018 to obtain access to, to

rectify factual inaccuracies or to restrict the processing of their personal identifiable information.

Clinical Web Portal (CWP) - is the electronic system used to present a consolidation of information from a number of IT systems, including scanned paper records, as a single patient record. It is the source of the Trust's electronic patient record.

Electronic Patient Record (EPR) - is a consolidation of information from a number of IT systems.

Data Subject – is an individual about whom we hold personal information, such as a staff member, a patient, or a member of the public.

Data Subject Access Request (DSAR) - is a request made by the patient or their representative to access their health record.

IG - Information Governance

HRAT (Health Records Access Team) - the Department that coordinates all requests to access patient information. The HRAT sits within Health Records Services.

Personal information -is information about a living (natural person), identifiable individual, patient or staff. It includes information that would identify a living individual directly or indirectly, such as name, date of birth, address, Internet Protocol (IP) address etc.

Special Category (Sensitive Personal) Data – personal data which consists of the following information:

- The racial or ethnic origin of an individual
- Political opinions
- Beliefs of a religious, philosophical or similar nature
- Membership of a trade union
- Physical or mental condition of an individual
- Genetic and biometric data
- Sexual life of an individual
- Gender Reassignment/Identity
- The commission or alleged commission of an offence or
- Any proceedings for any other offence committed or alleged to have been committed by the individual, the disposal of such proceedings or the sentence of any court in such proceedings.

Anonymised Data – data which has had identifiers removed so that an individual cannot be identified.

Pseudonymised Data – data which has had identifiers removed and replaced with a pseudonym.

Corporate information – information used in the Trust's business and administration functions (e.g. minutes, agendas, financial, meeting papers).

IAO – Information Asset Owners; please see accountability section.

IAA – Information Asset Administrator, please see accountability section.

IGSG – Information Governance Steering Group.

IGAG – Information Governance Action Group.

DPA – The Data Protection Act 2018.

GDPR – General Data Protection Regulation 2018.

Controller – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Processing has the same meaning as in the Data Protection Legislation and means the obtaining, recording, holding, altering, manipulating, transmission, disclosure, erasure or destruction of data.

Data Protection Legislation means the Data Protection Act 2018, the EU Data Protection Directive 95/46/EC, the GDPR (General Data Protection Regulations), the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive 2002/58/EC, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

EEA State has the same meaning as in the Data Protection Legislation 2018, European Economic Area.

NHS Digital - NHS Digital is the trading name of the Health and Social Care Information Centre (HSCIC), which was established in April 2013 by the Health and Social Care Act 2012. NHS Digital is responsible for collecting, transporting, storing, analysing and disseminating the nation's health and social care data.

3.0 Accountabilities

3.1 Obligations of the Organisation

The Organisation will, through appropriate management, and strict application of criteria and controls:

- Observe fully the conditions regarding the fair collection and use of information;
- Meet its legal obligations to specify the purposes for which information is used;
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- Ensure the quality of information used, through validation and checking processes with patients;
- Apply strict checks to determine the length of time information is held
- Ensure that the rights of people about whom information is held can be fully exercised under the Act;
- Take appropriate technical and organisational security measures to safeguard personal information;
- Ensure that personal information is not transferred outside of the EEA without suitable safeguards.

3.2 Senior Accountabilities

Medical Director is the appointed **Caldicott Guardian** for the Trust and has, on behalf of the Board, responsibility to act as the Guardian of patient identifiable information and chair of the Information Governance Steering Group (IGSG)

Chief Financial Officer is the **Senior Information Risk Officer** (SIRO) who acts as an advocate for information risk on the Board and understands how the strategic business goals of the Trust may be impacted by information risks.

Caldicott and **SIRO** responsibilities are:

- To oversee the development of an Information Risk Policy, and a Strategy for the Policy within the existing Information Governance Framework.
- To take ownership of risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.
- To review and agree action in respect of identified information risks.
- To ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- To provide a focal point for the resolution and/or discussion of information risk issues.
- To ensure the Board is adequately briefed on information risk issues.

Each Director is responsible for ensuring that the personal data held by their department is kept securely and used properly, within the terms of the Act. They are also responsible for informing the DPO of the types of personal data held in their

directorate and any changes or new holdings to inform the Information Commissioner as required.

Data Protection Officer (DPO) informs and advises the Trust, processors and employees of their obligations under the General Data Protection Regulation. The DPO will act independently with matters relating to GDPR to monitor compliance.

3.3 Board, Committee and Groups

The Trust Management Committee has ownership and overall responsibility for the content of Health Records through the Health Records Project Group.

Information Governance Steering Group (IGSG) The Caldicott Guardian chairs the IGSG. The group has specific terms of reference and its membership includes Divisional representation from the Trust as well as DSP Toolkit initiative leads including Health Records Services. The IG Steering Group (IGSG) has overall responsibility for overseeing the development and implementation of the IG strategy, policy and action plans. These will be subject to a periodic review and progress will be reported to the Board Assurance Committee, Trust Management Committee (TMC) and Trust Board.

Information Governance Action Group (IGAG) will monitor actions arising from the IGSG and ensure continued improvement for the DSP Toolkit and any other Information Governance Action Plans, which is fed back into the Information Governance Steering Group. Initiatives and actions are fed from and/or to IGAG from the Health Records Project Group (HRPG).

Integrated Electronic Patient Record (IEPR) Group ensures the development and effective availability of electronic patient record information systems. The IEPR Group is responsible for introducing, adapting and improving the operational effectiveness of electronic health records to clinical services.

Health Records Project Group (HRPG) will monitor compliance with this policy and is responsible for the content, format, improvement and approval of any changes of the Health Record. HRPG will review and feedback on all Directorate / Speciality Privacy Notices before they are published by Web Services or Medical Illustration.

3.4 Specialist Staff

Information Governance Manager is responsible for coordinating Information Governance improvement activities, providing advice and guidance across the Trust.

Cyber Security Manager is responsible for cyber security activities, providing advice and assistance across the Trust. Continuously assessing the shortfall between security measures in place being effective and those established at a policy level thus highlighting deficiencies for remedial action. Investigating

suspected and actual breaches of security and undertaking reporting/remedial action as required to IGAG.

Information Governance Toolkit Requirement Leads are responsible for monitoring/maintaining evidence and identifying risks associated with the respective standards that fall within the scope of their role and for embedding any of the standards across the Trust.

Information Asset Owners (IAO) will be the nominated owner(s) for one or more identified information assets. They have clear responsibility to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities in relation to information security and risks associated with the asset.

Information Asset Administrators (IAA) have responsibility for the day to day management of information assets, ensure that policies and procedures around the asset are followed, and to consult their IAO on potential or actual security incidents and risks.

Associate Chief Technology Officer will ensure that technical solutions are in place and appropriate to protect sensitive electronic information, from where this information is accessed within the Trust infrastructure platform.

Head of Health Records Services (or designated deputy) is responsible for the effective, safe and secure management of clinical paper records across the organisation and the wider healthcare community. Representing Health Records Services at the IEPR Group to ensure the effective availability of electronic patient records. The Head of Health Records Services is responsible for ensuring compliance for a wide range of national and local guidelines and regulations, including the General Data Protection Regulation (GDPR). To lead multiple health records audits and quality improvement initiatives, conducted both internally and trust wide, and ensure non-compliance is identified and appropriate actions are undertaken. The Head of Health Records Services will manage the appeals and complaints process in relation to all Subject Rights Requests. The Head of Health Records Services is also responsible for the development, implementation and monitoring of this policy.

Health Records Access Team (HRAT) is responsible for coordinating and responding to Subject Rights Requests from the public regarding their health records, in line with DPA and GDPR and for liaising internally with directorates and Healthcare Professionals, and externally with providers of data the Trust may hold. The HRAT will complete redactions and apply relevant exemptions prior to disclosure of any personal data. The Team will keep a log of requests made and ensure a formal response is provided to the requester, either by way of providing the information or else by advising of the reasons why the information will not be made available. They will ensure that the relevant time scales for responses, outlined in the law, are complied with, and compliance is reported to an overseeing group, or the Information Governance Steering Group.

Health Records Services is the custodian of the manual and electronic health record when not in use and is responsible for storage and secure keeping of the record. Whilst records are in use, the responsibility lies with whoever holds them in their possession. This includes the safe keeping and filing of loose documents. All Health Records Services Staff have a responsibility to ensure that all records are created, handled and maintained in accordance with this policy and that patient confidentiality is protected at all times.

Patient Advice and Liaison Service (PALS) is responsible for recognising Subject Rights Requests received by the Department and forwarding requests to the HRAT promptly. It is common for a SAR to be received following the outcome of a formal complaint or even during an active complaint investigation. PALS will assist the HRAT to coordinate cross Directorate requests and complaints.

3.5 All Staff

Healthcare Professionals will review all clinical data in relation to Subject Rights Requests in the form of a 'serious harm test' and to notify the Health Records Access Team of their findings within the requested timeframe (see Attachment 5). Healthcare Professionals will judge all requests on an individual case by case basis.

Managers throughout all levels of the organisation (i.e. Team Leaders, Supervisors, Matrons, Clinical Directors) have a responsibility for implementing all elements of Information Governance and providing, or accessing, appropriate levels of expertise. They are responsible for daily working practice and must report concerns through their usual route in line with **OP10 Risk Management and Patient Safety Policy**

All Departmental Managers / Matrons within the Trust are responsible for ensuring that all staff (within their remit) are aware of and adhere to this policy.

Service Managers are responsible for the management of records in line with this Health Records Policy within their remit. Quarterly and Annual Documentation Audits will be undertaken for all separately held records, reports for which will be disseminated to Divisional teams via Governance leads for action plans to be developed for areas of non-compliance. This will be monitored via the Health Records Project Group.

Directorate Managers are responsible for recognising a Subject Rights Request (SRR) and forwarding request to The Health Records Access Team (HRAT) promptly. Directorate Managers are also responsible for searching local systems and drives for information in relation to SRR's upon request of the HRAT and forwarding that information within the statutory timescale.

The Trust and all its employees, whether they are on permanent, fixed term or temporary contracts, contractors, students and/or voluntary have a legal obligation and a duty of confidence to ensure that any information processed is done in line with legal requirements and best practice.

All staff will ensure that they have read this policy and have undertaken the relevant mandatory training in Information Governance in line with the Trust's **OP41 Induction and Mandatory Training Policy**. An e-learning package is available to all staff who record information within the patient record.

It remains the responsibility of all staff members to adhere to all relevant Trust policies and procedures, current law and legislation, when dealing with personal or sensitive information during the course of their duties, in particular the Data Protection Act 2018, the Common Law Duty of Confidentiality and the Caldicott Principles.

All staff must check that whatever information they provide in connection with their own employment is accurate and up to date and accept that they have a responsibility to inform relevant departments of any errors or changes required to that information.

All staff are encouraged to report untoward incidents and identify risks, no matter how minor they appear. This would not only apply to clinical incidents but also to information security breaches, through the Trust's Risk Management processes outlined in **OP10 Risk Management and Patient Safety Policy.**

All staff, whether clinical or administrative, who handle health records, are responsible for ensuring that this policy is adhered to in their day to day duties. Staff are also responsible for upholding patient confidentiality and for the consequences of their handling, recording and passing on of all patient identifiable information. All staff must be aware that accessing information without a business or clinical need is strictly prohibited. For more information please refer to **OP97 Confidentiality Code of Conduct for Staff**.

3.6 3rd Parties

Any 3rd party with access to Trust data or processing Trust data is also bound by the Data Protection Act. The specific responsibilities for Data Controller and Data Processors will be described in the 3rd parties' contract with the Trust including any extra confidentiality or non-disclosure statements where they are needed. 3rd parties must abide by the terms of their contract.

4.0 Policy Detail

All patients' health records will be properly controlled and managed in accordance with Caldicott Principles, the Data Protection Act 2018 (DPA), the General Data Protection Regulation 2016 (GDPR), and the Records Management Code of Practice for Health and Social Care 2021. This is implemented through the protocols and procedures below.

4.1 Creation of a Health Record

4.1.1 Attachment 1: Structure and Use of a Health Record

This protocol sets out the minimum requirements when creating and using the patient's health record whether this is in an electronic or paper format, to ensure a complete and accurate record is captured within the health record.

- Principles and Standards of a Health Record: this document defines the basic principles and standards for general health record keeping.
- Creation of a Registration Process: this document details the process which must be followed in the creation of a 'new registration'. This is the process by which the Trust identifies an individual patient, and normally occurs on the receipt of the first referral, emergency attendance for the patient to the Trust or a new patient registration within Primary Care
- Structure of a Health Record: this document defines the structure contained within the health record.
- Content of a Health Record: this document describes the contents contained within the health record.
- Standard Order of a Health Record (Paper Records): this document details the standard order of the main single volume paper health record
- Primary and Secondary Documents' Procedure (Paper Records): this document details the standard order which must be followed in the event of multiple volumes of records
- Records Keeping Standards: this document defines the Trust's Generic Standards of Record keeping in line with the standards set out by the Royal College of Physicians and in line with Principle 4 (accuracy) of the General Data Protection Regulation.

4.1.2 Attachment 2: Approval of Documents Procedure

This document details the process to be followed for the approval of documents to be included within the main health record, skinny files or electronic health records.

- Document 1: Procedure for the Approval of Documents.
- Document 2: ICT Systems & Applications Services: Bantham Technologies Request For the creation or amendment of an electronic patent record

4.2 Management and Maintenance of Health Records

4.2.1 Attachment 3: Management of a Health Record

The following documents cover the management and maintenance of both the paper and electronic record.

Document 1: Data Quality and the Health Record
Provides minimum expected standards when collecting data for health records.

Document 2: Merging and Duplication Procedure
Ensures there is uniformity throughout the Trust when dealing with duplicate registrations on the Patient Management System (PAS) and the merging of health records in order to achieve a single registration for each patient.

Document 3: Transportation of Health Records Protocol
Provides the minimum standards required when transporting paper health records.

Document 4: Management of the Health Record in the absence of electronic systems and processes
Explains the manual process to follow in the absence of the Trusts electronic patient recording systems, for example Patient Administration System (PAS), Clinical Web Portal (CWP) or the Trust's ability to scan health records. A flowchart has been provided below to assist you in understand what manual process to follow.

4.2.2 Attachment 4: Access to Health Records and Subject Rights Requests

These procedures ensure all patient Subject Rights Requests are processed in line with General Data Protection Regulation and the Data Protection Act 2018. This document details the journey of a request, including the responsibilities of all staff involved in the process. This attachment covers all of the Subject Rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

This attachment also details the process for the disclosure and sharing of patient information. This is the process to follow when disclosing and sharing specific patient information to external organisations; for example the Police, the Courts, Coroner's Office and other hospitals, and what information must be redacted or exemptions applied prior to, or to prevent disclosure.

Please note that this procedure does not cover the processing of staff/employment subject access requests or Freedom of Information (FOI) requests.

4.3 Monitoring of a Health Record

4.3.1 Attachment 5: Health Records Audit & Monitoring

The Trust is required to monitor and audit staff access to patient records to ensure their legitimacy and appropriateness. Attachment 7 details the internal audit process undertaken by the Health Records Department.

- Document 1: Access to Merge Facility Audit
- Document 2: Tracking & Tracing Audit - Inpatient Episode 'Skinny File' Journey Audit
- Document 3: Tracking & Tracing – Manual Health Records Audit
- Document 4: Physical Access to the Health Records Library
- Document 5: Legitimate Access Audit
- Document 6: Subject Rights Requests Compliance Audit
- Document 7: Missing Records Audit
- Document 8: Generic Record Keeping Standards Audit

4.4 Scanning and Storage of a Health Record

4.4.1 Attachment 6: Scanning and Inpatient Documentation Process

This process follows the journey of a health record from its creation as a paper record or 'skinny file' through to its scanning on to the Clinical Web Portal. These processes are designed to ensure the electronic information can perform the same function as the paper record, maintaining its integrity, authenticity and usability for the duration of the retention period.

- Document 1: Scanning of Health Records
- Document 2: Current Process for Inpatient and outpatient Documentation
- Document 3: Inpatient Documentation Control Sheet for Skinny File
- Document 4: Standard order of a skinny file (inpatient health record)
- Document 5: Ward Attender Documentation Control Sheet
- Document 6: Inpatient Record Documentation process for a Deceased Patient

4.4.2 Attachment 7: Storage and Retrieval of a Health Record

The information held by the RWT represents one of its most valuable assets. It is therefore essential that all information for which it has responsibility is processed in a manner that complies with legal and regulatory requirements. These attachments cover the storage, security, tracking and retrieval of health records. Documents 3 to 6 detail the process of how to store, archive and retrieve community records

- Document 1: Health Records Storage & Security Process
- Document 2: Health Records Retrieval & Tracking
- Document 3: Storage and Retrieval of Community Archive Records
- Document 4: Community Records Submission form
- Document 5: Patient Record Request Form
- Document 6: Community Records Collection Schedule

4.5 Destruction of a Health Record

4.5.1 **Attachment 8: Retention, Appraisal, Disposal and Destruction**
This protocol details the appropriate standards regarding the retention, appraisal, disposal and destruction of health records. Storage limitation is a key GDPR principle, which links closely with the right of access. This principle ensures that information is kept in a form that permits the identification of patients for no longer than is necessary and only for the purposes for which the personal information is processed. This applies to all records, including those which are kept electronically i.e. Clinical Web Portal.

5.0 Financial Risk Assessment

There are no financial implications associated with the implementation of this policy.

1	Does the implementation of this policy require any additional Capital resources	No
2	Does the implementation of this policy require additional revenue resources	No
3	Does the implementation of this policy require additional manpower	No
4	Does the implementation of this policy release any manpower costs through a change in practice	No
5	Are there additional staff training costs associated with implementing this policy which cannot be delivered through current training programmes or allocated training times for staff.	No
	Other comments	

6.0 Equality Impact Assessment

An Equality Analysis has been undertaken. No adverse effects have been identified for staff, patients or the public as a result of implementing this Policy.

7.0 Maintenance

7.1 The responsibility for review of this policy lies with the Head of Health Records Services. The detail of the policy will be initially reviewed after 12 months, and then every 3 years thereafter, or in line with any major legislative changes

7.2 The associated protocols and procedures may be amended as required following ratification by the Health Records Project Group.

8.0 Communication and Training

Must include methods for targeted (as appropriate) and Trust wide communication of key deliverables within the policy. Training required and how to access this must be explicit. If training is mandatory there must be a cross reference to the Trust **OP41 Induction and Mandatory Training Policy** and training needs analysis for all staff groups.

- This policy will be made available on the Trust's Intranet site under Organisational Policies.
- All staff will be made aware of this policy at Trust Induction. An e-learning package is available via the Trust My Academy site for Health Records Keeping Standards for staff with specific roles, which involve recording of patient identifiable information. This must be co-ordinated within the individual directorate or department
- Training will be provided to staff that require access to merge records on PAS. This will be monitored and revoked if the function is not used within a 6 month period.

The following training and communication will be undertaken to ensure staff comply with Subject Rights Requests and Other Patient Information Requests, as per Attachment 5:

- Subject Access Request training is available to all staff who process requests upon request to the Health Records Access Team
- Representatives who attend the Health Records Project Group have been consulted and involved in the development of the OP07 Health Records Policy. This group will also be used to circulate the policy to all staff (as appropriate).
- The new procedures will also be communicated to staff via all user bulletins, desk top screensavers, the designated intranet pages for policies and procedures, and the IG/GDPR page.
- A series of events and workshops have been scheduled throughout 2019/2020.

Mandatory GDPR Learning package already available and rolled out across the Trust

9.0 Audit Process table

Audit Title	Lead	Monitoring Method	Frequency	Committee
Trust Wide Documentation Audit (Basic Record Keeping Standards	Head of Health Records Services	Documentation Audit of patient record keeping against Trust standards	Monthly reported Quarterly	- Health Records Project Group - Clinical Audit Group - Directorate and Divisional Governance Meetings
Access to merge facility	Head of Health Records Services	PAS audits conducted to establish access and use of merge facility	Six monthly	Merges and Duplicates Working Group
Process for tracking, tracing and appropriately reporting missing records	Head of Health Records Services	New Cross – Review of PAS against local records held. Community - review of local tracking system/database for records held/transferred.	Monthly, reported bi-monthly	Health Records Project Group
Physical Access to the Health Records Library	Head of Health Records Services	Review report to confirm legitimate access has been granted to Health Records Library	Quarterly	Health Records Project Group
Legitimate Access to Electronic Health Records	Head of Health Records Services	Clinical Web Portal Access (CWP) and Patient Administration System (PAS)	Quarterly	Health Records Project Group
Subject Rights Requests Compliance Audit	Head of Health Records Services	Review of subject rights request processing against GDPR statutory guidance to ensure compliance.	Quarterly	Health Records Project Group
Missing Records Audit	Head of Health Records Services	Review of Datix incidents and missing records log.	Monthly, reported bi-monthly	Health Records Project Group

10.0 References

10.1 Strategy

- ICT Digital Roadmap
- Information Governance Strategy

10.2 Policy

- OP10 - Risk Management & Patient Safety Policy
- OP12 - IT Security Policy
- OP13 - Information Governance & Data Protection Policy
- OP97 - Confidentiality Code of Conduct for Staff
- OP41 - Induction & Mandatory Training Policy
- OP85 - Information Sharing Policy
- OP91 - Data Quality Policy
- CP04 - Discharge Policy
- CP06 - Consent Policy
- OP111 - De-identification and Pseudonymisation Policy
- HS10 – Waste Management Policy

10.3 Other Sources

- Caldicott 2 Principles 2020
- Data Protection Act 2018
- General Data Protection Regulations 2016 (GDPR)
- Access to Health Records Act 1990
- Records Management Code of Practice for Health and Social Care 2016
- Care Quality Commission
- Data Security and Protection Toolkit (DSPT)
- Department of Health Confidentiality NHS Code of Practice (2003) Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures (2010): https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- The Records Management Code of Practice for Health and Social Care (2016): https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for- Health-and-Social-Care-2016
- The Information Commissioners Office: https://ico.org.uk/
- Information Governance Toolkit: https://www.igt.hscic.gov.uk/
- Information Governance Alliance (IGA) https://digital.nhs.uk/information-governance-alliance

11.0 Document Control

Policy number and Policy version: V5.1	**Policy Title:** OP07 Health Records Policy		**Status: Final**	**Author:** Head of Health Records Services **Director Sponsor:** Chief Finance Officer
Version / Amendment History	**Version**	**Date**	**Author**	**Reason**
	1.0	July 2011	Head of Patient Access/ Health Records Project Group.	Original Policy.
	2.0	July 2012	Head of Patient Access/ Health Records Project Group.	Review and Integration of PCT and RWT Policy. Policy incorporates Management of the Electronic Patient Record.
	2.1	November 2012	Head of Patient Access	Minor amendments made with regard to attachment 1 of the policy in relation to the use of stamps. Approval given to 'print' name and registration number where a stamp is unavailable Approval also given for electronically held operation notes to be printed in black ink
	2.2	May 2013	Head of Patient Access/ Health Records Project Group	Review and updated version of the audit criteria and audit tool in line with the Royal College of Physician for Quality Record keeping Revised procedure for Subject Access Requests
	3.0	January 2017	Head of Patient Access/ Health Records Project Group	Full Review of Policy
	4.0	January 2020	Head of Health Records Services	Full policy re-write, in line with the GDPR 2016 / DPA 2018. Merging of old attachments and creation of new

				procedures as required. Policy aligned to the journey of a patient health record. Include full audit and monitoring of compliance against OP07 and GDPR Subject Rights statutory requirements.
	5.0	June 2022	Head of Health Records Services	General review and updated version across the full policy. Main updates are removal of attachments 1 & 6. Inclusion of business continuity planning for skinny files (inpatient paper records)
	5.1	September 2022	Head of Health Records Services	Minor update to Attachment 4 and Updated Attachment 4.1

Intended Recipients: All RWT employees who create, handle, store, transport and dispose of patient health records. This will apply to both paper and electronic records.	
Consultation Group / Role Titles and Date: Health Records Project Group (HRPG), Information Governance Action Group (IGAG), Integrated Electronic Patient Record Group (IEPRG), GDPR Implementation Group.	
Name and date of Trust level group where reviewed	Trust Policy Group – August 2022 Virtual approval via Trust Policy Group – version 5.1 – September 2022
Name and date of final approval committee	Trust Management Committee – September 2022
Date of Policy issue	September 2022
Review Date and Frequency (standard review frequency is 3 yearly unless otherwise indicated)	3 years – August 2025
Training and Dissemination: Launched via Trust all users bulletin. Advice available as and when required from Health Records Management Team. Guidance given to all relevant staff as part of Trust Induction.	
To be read in conjunction with: • OP13 - Information Governance & Data Protection Policy • OP97 - Confidentiality Code of Conduct for Staff • OP10 - Risk Management & Patient Safety Policy • OP12 - IT Security Policy	
Initial Equality Impact Assessment (all policies): Completed Yes / No Full Equality Impact assessment (as required): Completed Yes / No / NA If you require this document in an alternative format e.g., larger print please contact Policy Administrator.	

Monitoring arrangements and Committee	Briefly state the monitoring report and key committee receiving the report.
Document summary/key issues covered Please provide a brief summary of the document to direct staff attention as to its main purpose and content.	
Key words for intranet searching purposes	Health Records, Data Protection, Access to Health Records, Subject Access Request, Rectification, Restriction, Scanning, Records Library, Archiving, Retention, Destruction

VALIDITY STATEMENT This document is due for review on the latest date shown above. After this date, policy and process documents may become invalid. The electronic copy of this document is the only version that is maintained. Printed copies must not be relied upon to contain the latest updates and amendments.

Part B **Ratification Assurance Statement**

Name of document: **OP07 Health Records Policy**

Name of author: **Sam Smith** Job Title: **Head of Health Records Services**

I, the above named author confirm that:

- The Strategy/Policy/Procedure/Guidelines (please delete) presented for ratification meet all legislative, best practice and other guidance issued and known to me at the time of development of the said document.
- I am not aware of any omissions to the said document, and I will bring to the attention of the Executive Director any information which may affect the validity of the document presented as soon as this becomes known.
- The document meets the requirements as outlined in the document entitled Governance of Trust- wide Strategy/Policy/Procedure/Guidelines and Local Procedure and Guidelines (OP01).
- The document meets the requirements of the NHSLA Risk Management Standards to achieve as a minimum level 2 compliance, where applicable.
- I have undertaken appropriate and thorough consultation on this document and I have detailed the names of those individuals who responded as part of the consultation within the document. I have also fed back to responders to the consultation on the changes made to the document following consultation.
- I will send the document and signed ratification checklist to the Policy Administrator for publication at my earliest opportunity following ratification.
- I will keep this document under review and ensure that it is reviewed prior to the review date.

Signature of Author:

Date:

Name of Person Ratifying this document (Chief Officer or Nominee):
Job Title:
Signature:

- I, the named Chief Officer (or their nominee) am responsible for the overall good governance and management of this document including its timely review and updates and confirming a new author should the current post-holder/author change.

To the person approving this document:

Please ensure this page has been completed correctly, then print, sign and email this page only to: The Policy Administrator

12.0 Implementation Plan

Policy number and policy version: Version 5.0	**Policy Title:** OP07 Health Records Policy	
Reviewing Group	Policy Group	Date reviewed: June 2022
Implementation lead: Sam Smith, Head of Health Records Services		

Implementation Issue to be considered (add additional issues where necessary)	**Action Summary**	**Action lead/s (Timescale for completion)**
Strategy: Implementation of ICT Strategic Roadmap to improve the integrated electronic patient record and patient access to their information via patient portals etc.	As per ICT Strategic Roadmap	IEPR/NB/SP/SS
Training: Develop e-learning package	Existing e-learning package to be reviewed, edited and re-launched.	Head of Health Records Services
Development of Forms, leaflets etc: Any forms developed for use and retention within the clinical record must be approved by Health Records Group prior to roll out. Reviewed against this policy.	Established process.	Head of Health Records Services
Strategy / Policy / Procedure communication: 1. Re-launch of updated policy to be included in 'all user' bulletin 2. This policy will be made available on the Trust's Intranet site under Organisational Policies 3. Specific training will be provided to staff that require access to merge records on PAS. 4. Subject Access Request training is available to all staff who process requests upon request to the Health Records Access Team 5. Circulated to staff via Health Records Project Group Members. 6. .	As detailed.	Head of Health Records Services

Attachment 1: Structure and Use of a Health Record

Contents

1.0 Procedure Statement

The Health Record has multiple purposes. One of primary purposes is the documentation of patient care. It represents the main communication mechanism between health care providers in the delivery of patient treatment, without it we would be unable to provide safe and effective care.

This attachment will set out the principles and standards which maximise patient safety and quality of care; support professional best practice; and assist compliance with DPA, GDPR, Information Governance and NHS Litigation Authority (CNST) Standards. These standards are applicable to any patient's health record in both paper and electronic format.

These processes are agreed by the Health Records Project Group and must not be altered without reference to the group.

2.0 Definition of a Health Record

A health record is a collection of clinical information pertaining to a patient's physical and mental health, compiled from different sources. Health records contain demographic data, next of kin, GP details, and most of the following: medical history; examinations; diagnoses; treatment (including surgical procedures and drug therapy); results of investigations—labs (e.g. biochemistry, haematology, pathology), imaging (e.g., plain films, scans); alerts and warnings (e.g., allergies, blood group, obligatory drugs, etc.); record of preventative measures (immunisations, screenings—breast, cervical, faecal, occult blood); nursing records; clinical correspondence and referrals for treatment; consent forms for surgical procedures; theatre reports; discharge letters; post-mortem reports. Health records are maintained by, or on behalf of, the health professional concerned with the patient's care and maintained as confidential documents under Caldicott guidelines.

Each patient must have an accurate Health Record whether that is in a paper or electronic format. Paper health records may comprise of more than one permanent volume. This will:

- Enable the patient to be identified by either their NHS number or Unit Number without risk or error (it is vital that the correct identity of the patient is confirmed during each attendance or admission by asking the patient to confirm their name, address and date of birth: refer to the OP52 Patient Identification Policy
- Enable the patient to receive safe and continuing care;
- Allow the doctor or professional member of staff to resume the care of the patient at any given time;
- Facilitate the collection of data for research, education and audit;
- Facilitate the use of the records for legal purposes.

2.1 Paper Health Record

A majority of the acute paper records are now historic records and held for reference only on the request of the health professional. The main health record is held electronically.

The Trust holds 4 main types of acute paper Health Record (listed below). Other types of records exist for primary care and community services which are managed separately and staff must follow local processes.

2.2 General main record - Blue (older folders prior to 2003 may be a different colour).

For those areas that still create paper records i.e. have not adopted noteless working, a general main record folder will be created at the point when the patient is registered on the PAS system, with the following exception.

- Emergency Department attendees.

- See section 4.5 for Primary Care Services.

2.3 Litigation – White with a Red diagonal stripe

These paper folders denote that the patient is part of a legal case within the Trust. The decision to file the paper records within a legal folder must only be made by the Legal Services Department. If a folder needs replacing, it must be transferred into a new legal casenote cover which can be obtained by contacting the Health Records Library.

The litigation folder replaces the normal manual health record folder cover (usually blue). A litigation file is treated in exactly the same way as the main health record, though its destruction timeframes may differ (normally 10 years for adults and 30 years for children).

2.4 Lost Records

If the original paper main health record cannot be found, an incident must be raised on Datix by the area in need of the casenotes. The incident must be assigned to the area to which the casenotes were last tracked on the casenote tracking module on PAS. The reason for non-availability of the record must be clearly documented. Incidents of non-availability must be reported through local governance forums.

Temporary pink paper casenotes will only be created by areas which have not adopted noteless working if the original paper main health record cannot be located after a thorough search has been undertaken. Pink temporary casenote folders can be requested from the Health Records Library as required. All temporary folders raised must be created on PAS (to show the existence of the temporary folder) and tracked; the status of the original folder on PAS must be updated to read ‘lost’. This will usually be completed by Patient Access ‘clinic prep’ areas.

The Health Records Team must be notified when a record is marked lost. A register is kept to ensure that on-going searches are made until the original records are

found. An email must be sent to rwh-tr.HealthRecordsIssues@nhs.net and will be monitored through the Health Records Project Group.

If the original record is found, it must be amalgamated with the temporary casenote. The casenote tracking module must also be updated to reflect that the record is no longer lost.

If the original paper health record is found, it must be amalgamated with the temporary casenote. The casenote tracking module on PAS must also be updated to reflect that the record is no longer lost and an email must be sent to rwh-tr.HealthRecordsIssues@nhs.net so that the register can be updated to reflect that the record now found.

The Head of Health Records Services will notify the Trust's Senior Information Risk Owner (SIRO) in cases of widespread non-availability, for instances such as fire or flood within storage areas.

2.5 Skinny File – (clear plastic folders)

A skinny file is used to file documentation created as part of an Inpatient episode. On discharge, the documentation will be collected by either the scanning team or the Clinical Coding team (with the exception of neonates), where it would be scanned into the patients' electronic record on CWP refer to OP07 Attachment 6 - Scanning and Inpatient Documentation

Neonates are registered and issued with their own Unit number. Skinny files are still raised in the same way as other inpatients however most of the documentation created will be scanned to Badgernet and basic information scanned to CWP by the service on discharge. However, if they do not require admission, their birth notes are kept in their mother's record until such time they require treatment in their own right or where there is safeguarding issues. In this instance, new case notes will no longer be raised and copies of all safeguarding documentation will be scanned into the child's electronic health record in CWP (with the exception of sexual abuse documentation which will be held locally) however this is currently in transition and historic paper records may still exist. It is the responsibility of the practitioner documenting within the health records for ensuring the records are detailed and appropriate and any concerns are escalated.

2.6 Electronic Patient Records (EPR)

EPR is a consolidation of information from a number of IT systems; this is presented as a single patient record within the Trust Clinical Web Portal (CWP). However, it is recognised there are a number of systems which reside outside of the CWP which hold patient information. These systems are recorded in ICT on a systems and software asset register.

2.7 Other Service Records

The records above relate to patients attending the acute Trust. For patients attending areas within Community Services, specific folders are used, relevant to the individual service provider (if services have not yet adopted noteless working).

2.8 Unavailability of Electronic Patient Record

During circumstances where elements of the EPR are unavailable, every effort will be made to obtain relevant patient information from other sources. In the event that all IT systems are unavailable each clinical service area must invoke their documented Business Continuity plans accordingly. In instances where CWP is unavailable for 15 minutes or more, 'Portal Lite' will be enacted which will provide a summary of the patient's CWP record in order to continue with patient care until such time as CWP is available.

2.9 Paper v Electronic Records

A patient record is made up of several sources. It must never be assumed that the patient Health Record is complete based on the information contained within the paper record. Many records are now stored electronically and as such the Clinical Web Portal (CWP) must be referred to as the main source of information with reference to the paper records if clinically required.

Please note - inpatient stay records are held within a paper record called "Skinny files" until such time they are scanned to CWP.

2.10 Electronically sourced reports

It is the responsibility of the service creating a report or result to ensure that it is available electronically as part the electronic patient record. This will be achieved through the individual service working in partnership with the IEPR Governance Group.

2.11 Email correspondence

Email exchanges regarding patient care must form part of the patient's electronic record and must be conducted through CWP. Emails regarding patient care must now be conducted through CWP. This automatic process relies on rwh-tr.portalnotes@nhs.net email address being copied into the email exchanges, which will then present within the patients electronic record in the notestream. For user guide refer to Attachment 1.1 - User guide for email correspondence through portal

3.0 Creation of a Registration Process

This process must be followed in the creation of a 'new registration' to ensure the Trust identifies an individual patient correctly, and normally occurs on the receipt of the first referral or emergency attendance for the patient to the Trust.

Primary registrations are listed by a unique reference number which is commonly known as the 'Unit number' or 'Hospital number' and is created on the Trust's Patient Management System (PAS).

It is important that prior to any new patient registration, every effort is made to ensure the patient is not already registered with the Trust.

Duplicate registrations may lead to clinical risks, as information with regard to patient care is held within more than one health record sometimes without knowledge of the clinician.

Only those staff who have received formal PAS module training will be permitted to register patients, and in doing so must follow the correct procedure and take responsibility for their actions. Requests for training must be submitted by line managers to rwh-tr.IT-trainingteam@nhs.net

Attach addendums for other areas i.e. primary care

3.1 Process to follow

When searching for a Patient Registration Number on PAS (The 3 Step Rule) Always start your search using the following criteria.

- **Step 1: Date of Birth Search only.** This will provide the best initial search as it will capture any common incorrect spelling of the patient name

If after following this step you do not find the patient, you must move to step 2.

- **Step 2: Surname and Forename Search. If** the patient is not shown following the DOB search, then a search on just the patient names will capture any incorrect DOB or incorrect spelling of names

If still not found, follow the final step before considering to register the patient.

- **Step 3: Surname and First Initial Only**. This search must only be used when both of the above scenarios have been followed and the patient has still not been found

If after following the above steps a potential match is found, but certain fields do not match you must consider the following:

- Has the patient's name changed e.g. marriage, divorce, separation, alias etc?
- Does the patient have a previous address?
- Has the patient been registered at a previous GP practice?

It is only after all of the above has been followed and verified that you must consider creating a new registration number

Note: If after following the 3 step rule, the patient has been identified, and has one or more registration numbers which begin with any of the prefixes A, C, P, R, T, LFB, SC, or 98/12345, you must refer to OP07 Attachment 3 - Management of a Health Record.

3.2 Creation of a New Registration

If following the search, the patient is not registered you must create a new patient record on PAS in order to generate a new unit number.

You must obtain and record as much information as possible from the patient / referrer and complete the appropriate fields:

- Patient surname and forename (ensure correct spelling)
- Gender
- Marital status
- Date of birth
- Address (including postcode)
- Telephone number (mobile and landline)
- GP details (including name, practice and telephone number)
- Religion
- NHS number
- Ethnicity
- Occupation (if necessary)
- Next of kin (including name, address, contact number and relationship to patient)

3.3 Creation of a New Casenote Folder (Paper Record)

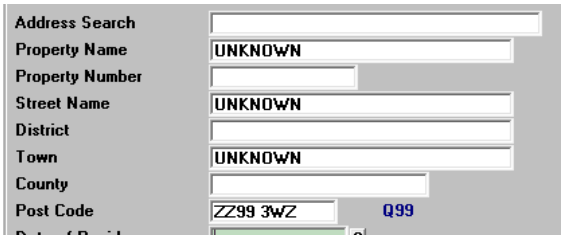
For services where paper records are still in use, a new folder must be created. You must ensure that a barcode label is produced and affixed to the front of the folder which shows the new registration number, patient name and date of birth. It is important for confidentiality reasons that no other information is written of the front cover. The inside of the folder must also be completed to record all demographic details for the patient. This must be handwritten as opposed to affixing a patient ID label in the event that the label loses its adhesive and drops off the folder.

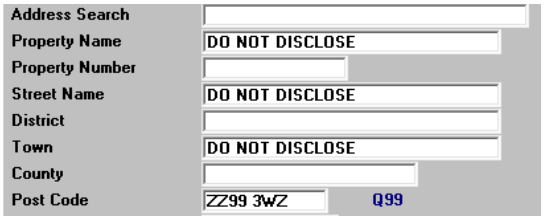
3.4 Creation of a New Electronic Record

Following the creation of a new registration on PAS, the electronic patient record will automatically be created within CWP.

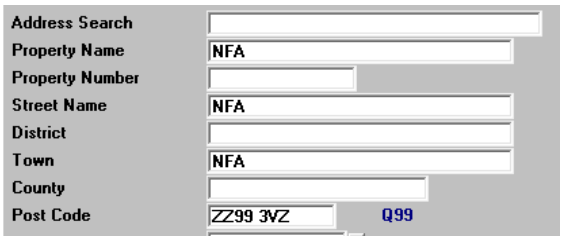
When registering on PAS patients who do not have a registered address or GP Practice please do not leave the fields blank but instead record the following data.

Address Unknown / Do Not Disclose (ZZ99 3WZ)

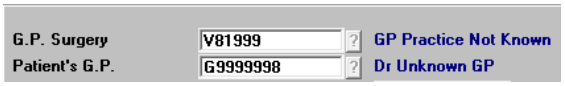




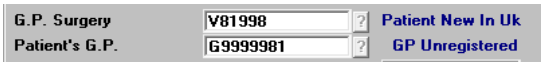
Address No Fixed Abode (ZZ99 3VZ)



GP Unknown / Unregistered (V81999)



GP Overseas (V81998)



If you have any further queries please contact the Data Quality Team on rwh-tr.dataquality@nhs.net

3.5 Adopted Children's Health Records

The records of adopted children must only be re-registered and given a new hospital number when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.

It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it was considered appropriate to do so, following the adoption. If duplicate records are found for children Refer to Attachment 3 - Management Maintenance for a Health Record.

3.6 Transgender Persons Health Records

A patient over 18 years old can request that their gender be changed in a record by statutory declaration; this gender change request on PAS can only be completed by the PAS team, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined by the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by the Gender Reassignment Panel. At this time a new NHS number can be issued and would be initiated by the GP. Refer to Attachment 3 - Management Maintenance for a Health Record.: Document 2: Merging & Duplication of Health Records Procedure section 3.7.

The Gender Recognition Act Act (2004) states that this information can be accessed and shared if it is for medical purposes by a health professional or for the safety of the person and' or those around them. The Act states that the term 'medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment.

As with all patient records, those of Trans patients are to remain confidential and any records relating to a person's Trans status or former gender or identity should be held securely. Access should only be granted to those people with a legitimate interest.

In the case of G.P referrals any changes of gender status will have been noted by the G.P. on the incoming health record/referral.

3.7 Private Patient Process

Recording the care of private patients is captured in the Private Patient Procedure

3.8 Overseas Patient Process

Recording of the care of overseas patients is captured within the Overseas Patients Procedure

4.0 Structure of a Health Record

All patients will be registered under one unique hospital number. This number will relate to the whole of the patient's health record regardless of their age, the type of treatment they are receiving or the location where it is being delivered, provided it is being delivered by Trust staff as part of the Trust business.

4.1 Sub-volumes

Sub-volumes are created within PAS for separately held paper records. They may only be created with authority of the Health Records Project Group. Where these authorised sub-volumes of notes are created the following must apply:

- On creation of the sub -volume the patient's unique hospital number must be attributed to it on PAS so all staff are aware of its existence and this unique number must be noted on all sub volumes created;
- The record must be available if and when required;
- Copies of the Emergency Department records must be made available where:
  - A referral is made to another department within the trust for continued treatment;.
  - The patient is admitted to hospital as result of that attendance.

4.2 Arrangements for separately held Health Records:

4.2.1 Oncology These records share the same hospital number and are identifiable on the Patient Management system (PAS) by the 'RISK' flag for 'ONCOLOGY'. The service operates using the Clinical Web Portal as the main electronic patient record and any current attenders will have historic records scanned into CWP under 'contemporaneous' or 'archived' notes.

The historic manual records of deceased patients (10 yrs. or less) or discharged patients are stored off site. Discharged patients who return to the service, records are requested back and scanned into the CWP before being destroyed. All paper documents created i.e. treatment sheets, radiotherapy and chemotherapy charts are scanned into portal once completed and paper copies destroyed.

4.2.2 Therapies & Dietetic Services These out-patient records carry the same hospital unit number and activity is identifiable on the PAS. Records are held electronically within their own system.

4.2.3 Maternity Health Records are pulled for clinics so that the doctors can review any previous pregnancies. No hand held notes are filed, apart from the referral letter (under current pregnancy), as these are no longer used. A record of the patient's attendance is recorded onto the Badgernet system. This system is also available for Community Midwives to record attendances on. Patients no longer have a handheld booklet; they have an App on their phones which informs them of their appointments. The same Hospital Unit Number is used and all activity is identifiable on PAS.

4.2.4 ICCU Charts

Due to their bulkiness and size these records are scanned and held electronically on the Clinical Web Portal (CWP) following a patient's discharge however there may be historic charts still held within the main paper health record.

4.2.5 Microfilmed Notes

Notes that have been microfilmed are identifiable on PAS (where applicable) and hard copies can be requested via the request line / health records library email address rwh-tr.healthrecordslibrary@nhs.net

4.2.6 Primary Care Services (RWT PCS) (GP Surgeries)

All patient's records are held electronically on the GP clinical system EMIS and within the Lloyd George physical folder. DocMan is used for the electronic transfer of letters to and from hospitals etc. and to scan and workflow documents into patient records. Historic paper records (Lloyd George) are kept at the patients GP practice. A Lloyd George envelope is still created for new babies being registered with the GP Practice. This is because when a patient leaves a GP Practice and transfers to another GP, their electronic record is printed and put into the Lloyd George envelope. This is for two main reasons; not all GP clinical systems allow the GP2GP electronic transfer and nationally GP coding policies differ, so when a record is received into the Practice via the GP2GP electronic transfer, the coding cannot be relied on and the paper record has to be summarised onto the electronic record.

When a patient leaves a GP Practice the Lloyd George folder containing the historic records and a print out of any electronic records are sent to a centralised service known as Primary Care Support England (PCSE) to be forwarded to the new GP Practice.

Following a patients death, no paper records are held by the GP Practice. As above, all data held is sent to PCSE. If records are needed to be recalled a request has to be submitted to PCSE via The Health Records Access Team.

4.2.7 Adult Community Services

There is a mixture of paper and electronic records. There will always need to be an element of paper record within the patient home for business continuity purposes. Paper records are brought out of the home environment once the patient has been discharged. Electronic records are stored on clinical databases (ie INR Star – Anticoagulation Services and Vector (Diabeta 3).

4.2.8 Paediatric Community Services

Have adopted electronic records, with the exception of Looked After Children (LAC) and adoption notes.

4.2.9 Audiology Records

These records are store on a system called Audit-base, a dedicated Audiology patient management system. No paper records are held within the department. Old paper records are held in archive managed by Health Records Services.

4.2.10 Safeguarding Records

Safeguarding health records documentation is transitioning into the electronic record and will be held in the child's record within CWP with the exception of sexual abuse documentation which will be held locally. Adult safeguarding documentation is already held electronically on CWP. For both children and adults, it is the practitioner documenting within the health record that holds the responsibility for ensuring the records are detailed and appropriate, the notestream must be updated within CWP to trigger a change in the colour of the safeguarding button to highlight concerns raised refer to: CWP Safeguarding Note(button) SOP . This is also monitored by the safeguarding teams on a daily basis. The Safeguarding team are contactable to offer support for adults: rwh-tr.safeguarding-team@nhs.net Children: rwh-tr.safeguarding-children@nhs.net

Practitioners must ensure the voice of the patient and actions taken to address any safeguarding concerns is clearly documented in the patient record.

4.2.11 Research & Development

All patient study information will be part of the patients main records which could be held in either electronic format or paper dependant on speciality and there noteless progression. Patient information is also held in study folders, held within the R&D department. Any historic patient study data is archived off site.

5.0 Content of a Health Record

Standard	The patient's Health Record for both inpatients and outpatient patients must contain:
Patient Identification (**for paper records)**	**Front cover (patient ID label content)** • Unit number • NHS number • Patient Name • Date of birth **Inside front cover (hand written)** • Full Address (including Post Code) • GP and surgery address • Telephone number (both landline and mobile) (of patient or contact) • Sex • Next of kin / appropriate representative (i.e. person with parental responsibility) - name/ relationship and contact details • Ethnicity • Religion • School
Clinical Record	• Source of referral. • Name of admitting consultant. • Alert notification (to be entered on the Alert Card for paper records). This includes information such as risk flags, allergies etc. • Every in-patient entry must be dated and timed (using 24 hour clock), and every outpatient entry must be dated. All entries must be signed and stamped with full name, designation and personal identification number of the signatory stated. Where a stamp is not available, the professional **must** write in block capitals their name, designation and identification number. • Initial consultation (must include the clinician's written codeable diagnosis or reason for admission, and the date and time of examination). • Initial patient history (must include present and past medical history, family history, details of medication, employment, social and environmental details if pertinent). • Decisions made on behalf of a person who lacks capacity must be recorded and provide evidence that these have been taken in line with the requirements of the Mental Capacity Act 2005 or

	where relevant the Mental Health Act 1983 and their associated code of practice. • Initial physical examination (a report of the examination performed by the clinician), with a record of and the patient's weight in metric units. Urinalysis must be routinely recorded. Where a patient is admitted on the ward, recording weight must be carried out as soon as feasible. The details must be recorded on the drug sheet and in the nursing notes, and height and BMI in children and should be plotted on e-growth charts • Carefully document the reasons for decision making and the context of the decision opposed to solely documenting the care. For example resources at the time, PPE usage, segregation of Covid and non Covid patients and how the hospital/area has complied with National/Trust guidance. • Therapeutic orders and orders for diagnostic tests (It is good practice to record the date and details of the tests ordered). (Refer to Policy CP50 for Management of Risks associated with Clinical Diagnostic Tests and screening) • Results of Investigations. Results which are not held electronically must be filed within the patient record (for areas where noteless working has not been adopted) or scanned into the electronic record. For electronic results which have been printed and comments made on the report, these must be re-scanned into the electronic record to ensure comments are captured. Once scanned these can be confidentially destroyed once adequate quality checking has taken place. • Details of verbal information/instructions to patients/carers (a record must be made of the issues that have been discussed and who else was there, e.g. disease management and prognosis discussed with 'X' in the presence of 'Y'). This includes changes in consent and the reasons why, and include where alternatives were offered. It must also include advance decisions to refuse treatment. • Details of ReSPect discussions and relevant communication/discussion with family where applicable. • Record the rationale for ward move decisions to ensure that scrutiny can be applied to the cohorting of patients and patient flow. • Correspondence (where there is correspondence from one consultant to another within the Trust, there will initially be two copies of the letter. The receiving consultant's secretary must discard the back copy of the referral letter when filing the top

	copy) For both children and adults it is the responsibility of the practitioner documenting within the health record that holds the responsibility for ensuring the records are detailed and appropriate and the notestream is updated within CWP to trigger a change in the colour of the safeguarding button to highlight concerns raised. Practitioners must ensure the voice of the patient and actions taken to address any safeguarding concerns is clearly documented in the patient record.
Patients undergoing surgery	• Consent for undergoing surgery refer to http://intranet.xrwh.nhs.uk/pdf/policies/CP_06_Policy.pdf . Consent must show signed evidence obtained by an appropriately trained clinician via completion of the correct consent form, obtaining informed consent for children (under the age of 16). years) • Preoperative diagnosis made by a suitably qualified medical practitioner. • An anaesthetic record. • Surgical procedure notes must be recorded on an operation note.
Clinical Web Portal Notestream	• Email exchanges regarding the patients care must be communicated through CWP to ensure rwh-tr.portalnotes@nhs.net is copied. This will captured the communication as part of the patient's electronic record. • Notes stream (on CWP) any clinical notes can be captured using the note stream within the electronic record. The safeguarding button can be activated via this area refer to 4.2.10 of this attachment for this process.
Discharge	• Every patient must have a discharge communication completed this includes self-discharging patients. The discharge communication (discharge summary) must be completed on the day of patient's discharge. • A discharge letter (for day case or areas that do not have electronic discharge) must be completed within 24 hours of the patient's discharge and sent to the GP or other institution to which the patient was discharged).)
Death	• Clinical diagnosis (provisional within 72 hours and a complete diagnosis within one month of death).

	• Post mortem reports (a copy must be sent to the consultant's secretary to place on file).

6.0 Standard Order of a Health Record (paper records)

This protocol relates to only areas that raise paper records i.e. Ophthalmology and Paediatrics. The paper main Health Record and local processes must be in place for casenotes managed separately.

6.1 Standard Order

- ReSpect form
- Patient alert card
- Patient ID labels
- Copy of kmr1 form (inpatients only)
- Post-mortem reports to be filed behind kmr1's
- Current pregnancy
- Correspondence guide card which comes as standard in all new sets of case notes. (brown card)
- Correspondence mount sheet (all correspondence including patients discharge sheets must be filed in date order on top of correspondence mount sheet - one per specialty, speciality sticker to be affixed on the top right hand corner.).
- Biochemistry mount sheet (green)*
- Microbiology mount sheet (blue)*
- Haematology mount sheet (red)*
- Radiology mount sheet (black)*
- Miscellaneous mount sheet (white)*
- Histology/cytology reports* (a4 paper with a purple line running down the right hand edge)

**These mount sheets will mainly be found in casenotes raised prior to 2012. New guidance is that as the majority of results are now held electronically paper copies must not routinely be filed within the paper record.*

- EEG Department (Guide card with sticker attached followed by results)
- Endoscopy (Guide card with sticker attached followed by results)
- Cardiology Investigations (Guide card with sticker attached followed by results, including 24 hour tapes)
- Other Investigations (Guide card with sticker attached followed by results)

For each Specialty:

- Specialty guide card with speciality sticker attached
- Letter of referral or Emergency Department record and ambulance sheet which gives rise to the consultation
- History and continuation sheets used for both inpatients and outpatients to provide a continuous medical history
- Diabetes chart

After individual Specialties:

- Anaesthetic guide card (white)
- Anaesthetic sheet (bright yellow)
- Consent guide card (consent forms to be filed behind red guide card)
- Nursing process guide card (white)
- Nursing record (all specialties - including endoscopy assessment)
- Therapy services guide card (pale yellow)
- Therapy services records
- Liability of loss of property forms
- Nursing home/residential information
- Prescription/treatment sheet (drug sheet, white cardboard booklet)
- Intervention charts
- D and v forms/stool charts/urine charts
- Electrolyte charts
- Medical photographs (must be filed in a brown envelope, hole punched and attach a patients label, you must write which speciality the photographs correspond to)
- Purple section: Social Services / Child Protection

6.2 General Principles to Follow

- The file must be maintained in a good physical condition. If not, it must be replaced with a new folder.
- All contents must be securely fastened within the file. Placing a document loose inside the folder is not permitted. The Health Records Library will not accept responsibility for the filing of loose documents and will return any received to the originator. Loose filing must not be filed on the shelving within the Library.
- If the file becomes too thick to manage it must be split into Volume 1 and Volume 2 (see attachment 2 – Document 6 Procedure “Casenotes - Primary and Secondary Documents Procedure).
- All contents filed must comply with the Health Records Contents see (Document 4) Guidelines and must be filed in accordance with Standard Order of Casenotes Procedure.

7.0 Primary and Secondary Documents Procedure (paper records)

In the event that a health record becomes unmanageable, it must be divided into two or more volumes. It is recommended that health records are split when they reach 5cm in thickness.

Health records covers must be clearly cross referenced when more than one volume of notes exists. They must always be stamped on the front cover:

i. Volume …….. of …… Volumes
ii. Date split …… / …….. / …….. Initials of staff member splitting record

Only the primary folder (Volume I) will routinely be retrieved and circulated. Volume 2 etc will remain filed in the appropriate Library unless specifically requested or in the case that it is an extension of Volume 1. In the case that volume 2 is an extension of volume 1 this must be clearly stated on the front cover that Volume 1 and 2 must be kept together.

7.1 Volume 1

Must contain primary notes only and include:

- ReSpect form
- Patient alert card
- Patient id labels
- Kmr1 forms (inpatients only)
- Post mortem reports
- Current pregnancy
- All correspondence
- Biochemistry mount sheet
- Microbiology mount sheet
- Haematology mount sheet
- Radiology mount sheet
- Miscellaneous mount sheet
- Histology/cytology results (all results to stay in volume 1)
- Cardiology investigations (guide card followed by most recent result only)
- EEG's (guide card followed by most recent result only)
- All endoscopy reports (guide card followed by all endoscopy results)
- Other investigations to include ECG's 2years and under (guide card followed by other investigations, keep most recent investigation only)
- All specialities referral letters
- All specialities history sheets
- All specialities continuation sheets
- All daycase surgery –Beynon centre documents
- All social notes (filed behind purple guide card)
- All anaesthetic records
- All operation consent forms
- Medical photographs (must be filed in a brown envelope, hole punched and attach a patients label, you must write which speciality the photographs correspond to)

7.2 Volume 2

Must include:

- Old Biochemistry Mount Sheet
- Old Microbiology Mount Sheet
- Old Haematology Mount Sheet
- Old Radiology Mount Sheet
- Old Miscellaneous Mount Sheet
- Old Cardiology Investigations (guide card followed by results, most recent investigation to remain in volume 1)
- Old EEG's (guide card followed by results, most recent to remain in volume 1)
- Old Other Investigations to include ECG's 2 years and older (guide card followed by results, most recent other investigations to remain in volume 1)
- All Nursing Process Notes
- Liability of Loss of Property Forms
- Nursing Home/Residential Information
- Prescription/Treatment Sheet (Drug sheets)
- Intervention Charts
- Stool Charts/Urine Charts
- Electrolyte Charts

In the case that Volume 2 is still too large, separate the nursing process notes; old results mount sheets and investigations and create a Volume 3. You must remember that as and when new volumes are created, all files must be updated to denote the total number of volumes in existence i.e. 1 of 2 would become 1 of 3 etc.

The Health Record must be kept in the correct order following the Standard Order of Health Records Procedure (Section 6 - Document 5 above). It must be made clear on the Health Record which volumes are to be kept together at all times. Local processes for separately managed services must be followed for managing oversized records.

7.3 Inpatient Records (Skinny files)

On admission, for those areas that have adopted noteless working a patient will have a skinny file created both physically and on PAS. Skinny files are used as opposed to the main paper Health Record and all documentation created within that episode of care must be filed within the skinny file in order and scanned into the electronic health record after discharge. Please refer to OP07 Attachment 6 - Scanning and Inpatient Documentation for further information.

8.0 Record Keeping Standards

This document sets out the Generic Standards of Record keeping as laid down by the Royal College of Physicians and in line with Principle 4 (accuracy) of the General Data Protection Regulation.

All entries made into the Health Record must comply with the Generic Standards of Record keeping as laid down by the Royal College of Physicians and in line with Principle 4 (accuracy) of the General Data Protection Regulation. When recording information the general principles apply to both paper and electronic records.

1. The patient's complete medical record must be available at all times during their stay in hospital.

2. Every page (ie front and back) of the Health Record must include the patient's name and hospital number and/or NHS number, and where possible location in the hospital

3. All documentation within the record must reflect the continuum of patient care and must be viewable in chronological order.

4. All data recorded or communicated on admission, handover or discharge must be recorded using standardised proforma.

5. Entries must include an accurate record of all decisions taken in relation to the care and treatment and make reference to discussions with individuals who use the service, their carers and those lawfully acting on their behalf.

6. Entries must only be made by staff authorised by the Trust who are involved in the management of the patient. These are Doctors, Nurses, Professional Clinical Services Staff, Social Workers (this group of staff **must** use a stamp marked **Social Worker** before writing in the notes), healthcare students under supervision and also Chaplaincy staff. The health care professionals personal identification number must be recorded for each entry, i.e. GMC, GDC, CSP, HPC, NMC etc.

7. All entries made must be factual, consistent, legible, indelible, accurate and up to date. There must not be any undue delays for entries into the record. This includes diagnostic tests, correspondence and changes to care plans following medical advice.

8. All entries, (with the exception of those stated below) must be made in **black** ink and ink colours such as blue must not be used.

9. All operation notes must be captured on the dedicated **operation note** proforma only. This information must not be captured elsewhere in the health record. This ensures that operation notes are scanned to the correct bookmark within Clinical Web Portal.

10. Pharmacy endorsements on prescription charts must be written in **green** ink where a paper process still applies (with the exception of Chemotherapy entries which are endorsed in **red** ink).

11. Each in-patient entry must be dated and timed (using 24 hour clock) as identified on a Trust computer. A stamp must also be used to denote without exception full name, designation and personal identification number of the signatory stated. Where a stamp is not available, the professional **must** write their name in block capitals with their designation and personal identification number.

12. Pencils must not be used as information can be erased and fade over time.

13. Staff must not use erasers, liquid paper or any other obliterating agents to make amendments or deletions. A single line must be used to cross out and cancel mistakes or errors. It must then be signed, dated and timed by the person making the amendment or deletion. For amendments within the electronic record using direct entry, a new direct entry must be made, stating the correction. An electronic audit can then be made showing both the incorrect entry and the revised entry. For corrections made to scanned documentation, once corrected, the document must be rescanned.

14. All entries into the Health Record must be made as soon as possible after the event, (e.g. change in clinical state, ward round, investigation etc.) and before the relevant member of staff goes off duty. If the date and time differs from that when the records were written, this must be clearly noted under the name, signature and designation of the person making the entry.

15. Every entry must identify the most senior healthcare professional present (who is responsible for the decision making) at the time the entry is made.

16. An entry must be made in the health record whenever a patient is seen by a clinician. For inpatient care, when there is no entry in the health record for more than the timeframes below, the next entry must explain why:
    - One (1) day for acute medical care;
    - Seven (7) days for long-stay continuing care.

17. The discharge record/ discharge summary should be commenced at the time a patient is admitted to hospital.

18. Every patient discharged must have an e-discharge completed including self-discharging patients.

19. Abbreviations and symbols must be kept to a minimum.

20. When the management of care for a patient is transferred to another Consultant, the name, date and time of the agreed transfer must be recorded both within the patient record and on PAS.

21. Advance directives or decisions to refuse treatment, consent and resuscitation status statements must be clearly recorded in the Health Record (refer to CP11 Resuscitation Policy). In circumstances where the patient is not the decision maker,

that person should be identified e.g. Lasting Power of Attorney. Such documentation must be scanned refer to OP07 Attachment 6 - Scanning and Inpatient Documentation. and uploaded into Clinical Web Portal (CWP).

22. In terms of Electronic record, a 'free text' facility to enter typed clinical notes is available within the 'Patient Record' of the Clinical Web Portal.

23. The facility to capture hand written and uploading documentation in CWP is available via current scanning technology.

24. An entry into the patient health record must be made when chaplaincy care is provided to a patient. At the point in which chaplaincy care is requested, it must be made clear to the patient and, or their relative that the record will be accessed by the chaplaincy to denote that care has been provided.

25. Clinical notes must contain clinically relevant information only and must not include financial information, complaints, incident data, or legal correspondence. Information of this nature must be stored corporately or on the relevant electronic system ie Datix.

26. For patients undergoing surgery, or invasive procedures, records must include evidence that informed consent has been obtained. The CP06 Consent to Treatment and Investigation Policy details the correct document to evidence discussion of risks, benefits, discussion of options and alternative treatment. This form must be contained within the inpatient documentation and scanned into CWP via the skinny file process (refer to OP07 Attachment 6 - Scanning and Inpatient Documentation.

27. All telephone communication relevant to clinical care must also be recorded within the notes stream section of the electronic patient records on CWP or within the paper record for areas where noteless working has not yet been adopted.

28. A Trust wide Health Records documentation snapshot audit will be carried out on a monthly basis to monitor the basic standards of record keeping refer to Attachment 5 Health Records Audit & Monitoring

DRAFT

Updated: 2/10/2019

User Guide for Emails to become notes and part of the patient record

Introduction

Portal notes emails have been introduced as a way of extracting emails (sent to a specific account) – into the notes section of Portal. The system has been designed so that it can cope with email conversations, inline images and normal formatting (including email signatures) of a potential email dialogue between clinicians.

For them to be able to add notes in this way emails must be sent to portal.notes@nhs.net (either in the To, CC or BCC). In addition for the system to extract the correct patient information from the subject line, it has to be formatted in a specific way. (See Email Subject)

Individuals that have "Clinical Access" to Clinical Web Portal (i.e. would have normal access to be able to add a clinical note) can have access to be able to send portal emails in this way.

The system does not support email attachments at this time.

DRAFT

Updated: 2/10/2019

Email Subject

The subject line must be in the following format , the “Note” keyword indicates that this is to become a clinical note. All other emails sent to that mailbox will be ignored.

Subject line format: (in any order)

Note: <Hospital Number> <NHS Number> <Name>

Note: <Hospital Number> <Name>

Note: <NHS Number> <Name>

Note: <NHS Number> <Name>

Note: <Name> <Hospital Number>

Note: <Name> <NHS Number>

Examples:

- ✓ Note: Minnie MOUSE 9990027714 N434264
- ✓ Note: N434264 9990027714 Minnie MOUSE
- ✓ Note: 9990027714 N434264 Minnie MOUSE
- ✓ Note: N434264 Minnie MOUSE
- ✓ Note: 9990027714 Minnie MOUSE
- ✓ Note: Minnie MOUSE N434264
- ✓ Note: Minnie MOUSE 9990027714

- x Note: N434264
- x Note: Minnie Mouse
- x Note: 9990027714

Reply and forward prefixes (“RE:” and “FW:”)

The system, does recognise this and will still interpret emails that begin with “Re: Note: …..” , and “Fw: Note: …..”. Which is important as outlook automatically add these prefixes when replying or forwarding the emails.

The system doesn’t accept an email note, if only one patient identifier is available. This is because the system cannot cross check to ensure that emails are added to the correct patient record. Therefore two identifiers must always be supplied in the subject.

If you do send an email to portal notes, with the incorrect patient identifiers an email will be sent to you confirming that the note has **failed** to be added to clinical web portal.

DRAFT

Updated: 2/10/2019

Email Body

The email body will support inline images – however please keep these to an absolute minimum.

Email Conversations

The system will record a conversation dialogue and present this as an organised conversation (similar to what you see in outlook).

In the notes section you will see the original email that was considered the “start” of the conversation. All of the other relevant conversation items appear as linked items that can be clicked on to see the email.

Confirmation emails

You will receive a confirmation email if you email has been successfully added as a portal note. If it is part of conversation, it will say that it has been added as a conversation item.

Examples of added emails:

You will receive emails if you have attempted to add a note this way bit have been unsuccessful. The email will detail why it has been unsuccessful.

DRAFT

Updated: 2/10/2019

Emails in Portal

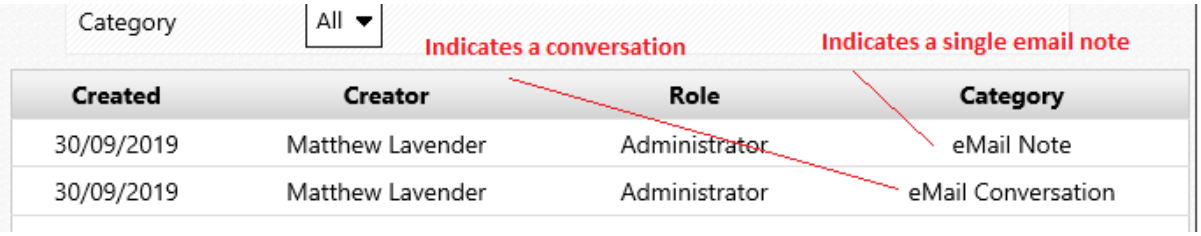
Panel entries

Emails will appear in portal in the notes section. They will appear under their own category of either “eMail Note” or “eMail Conversation”.

An **email note** is a single email that has included portal.notes@nsh.net in the distribution.

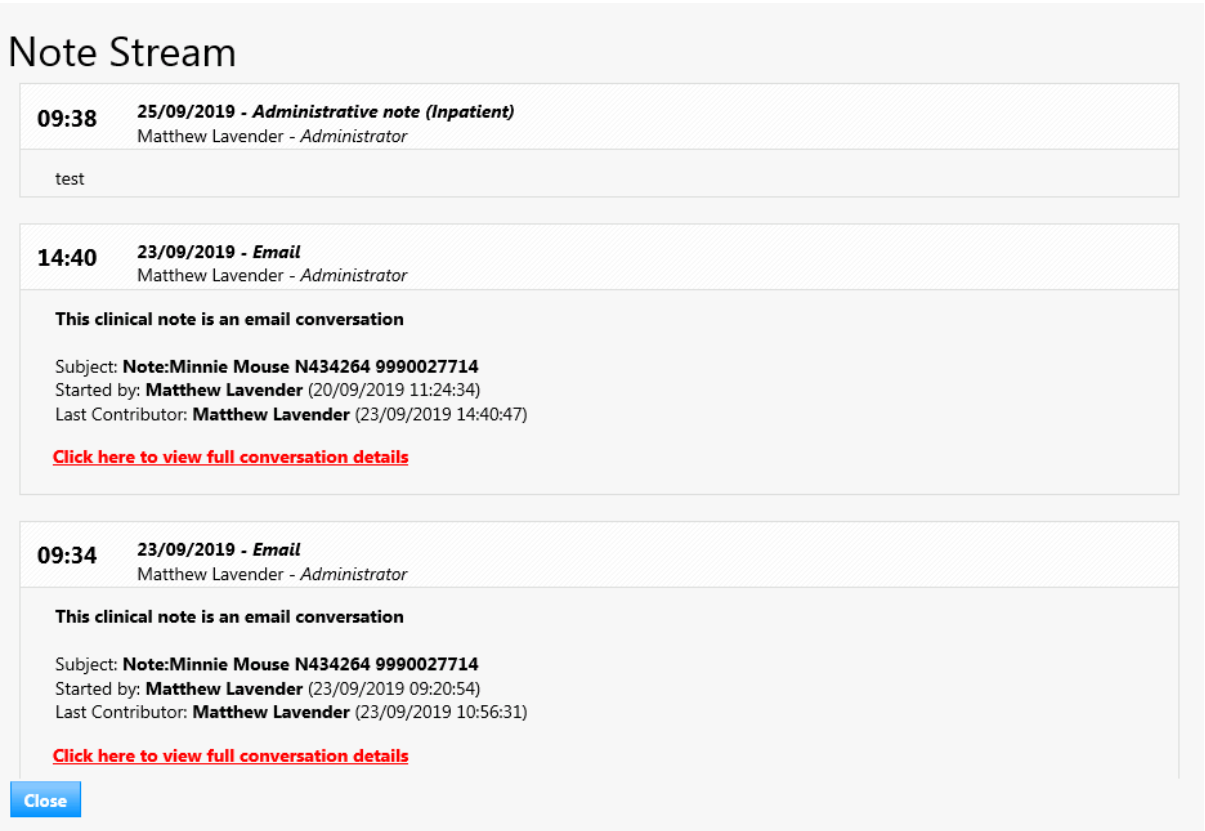
An **email conversation** is potentially multiple emails that are considered part of an email conversation. (i.e. multiple replies from multiple recipients but regarding the same original email).

Either entry will call the “Email Viewer”:



Notes Stream

Email notes and conversations will not appear directly in the notes stream, a summary of the note/conversation will appear with a corresponding link to the “Email Viewer”.



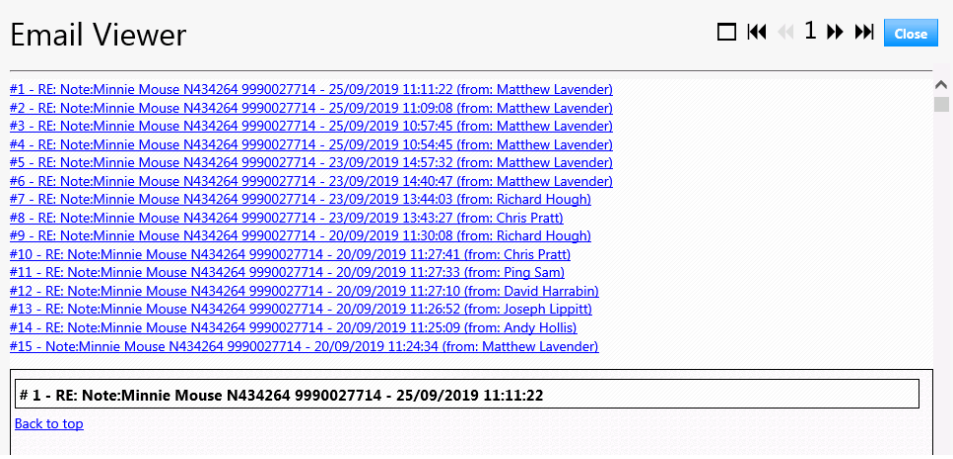
DRAFT

Updated: 2/10/2019

Email Viewer

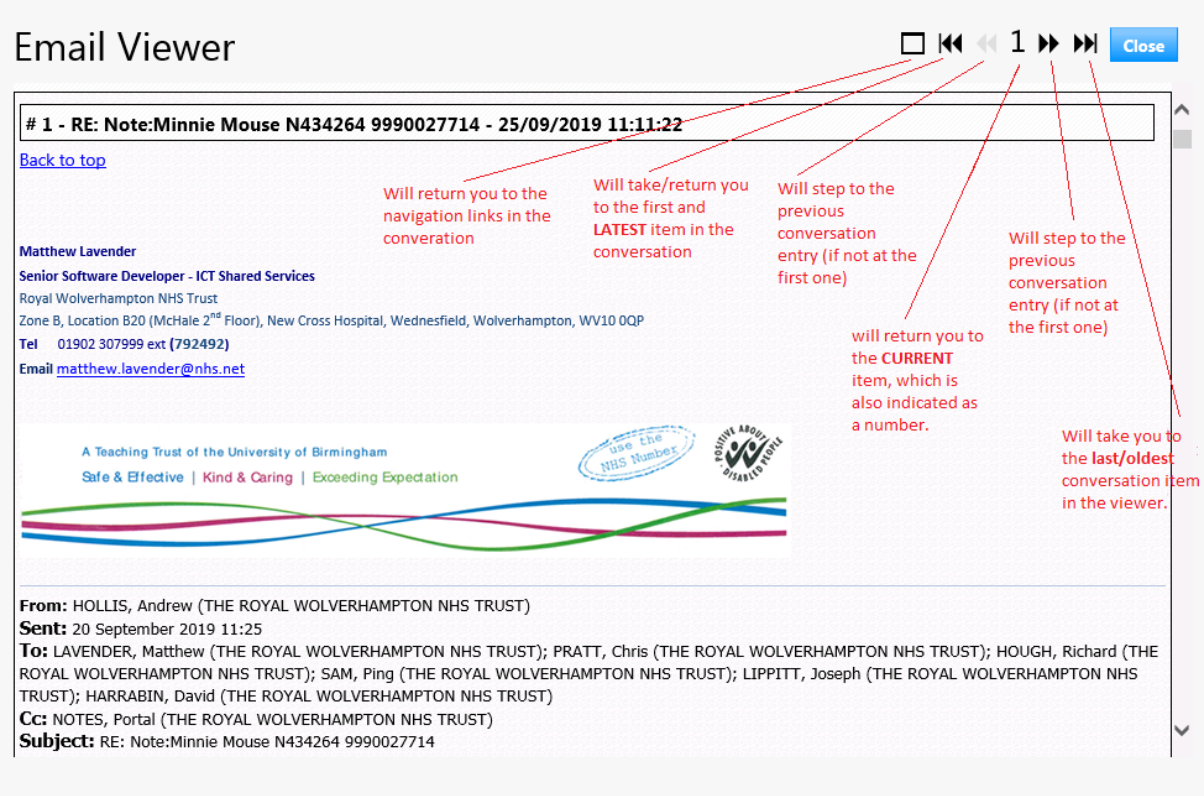
The email view allows you to view all emails that are sent to the notes section. It allows conversations of emails, to help prevent any unnecessary clouding of the notes section.

The email view allows you to navigate the individual emails within the conversation, and to easily traverse them.



Each of the links above (dependant on number of emails in the conversation) will scroll to the appropriate email entry. The navigation options (explained below) will allow you to return to these links if you need to. You may then step through or click to directly to a particular message.

If you use the scroll bar, clicking on the item number will return you to that item.



DRAFT

Updated: 2/10/2019

Security / Restrictions

Only authorised users or are allowed to add notes onto clinical web portal will be allowed to email. This has been restricted to clinical access web portal users only.

Audit

All notes added in this way will be audited. Both the sending and receiving of the email by portal.ntoes@nhs.net will also be kept for record keeping purposes.

STANDARD OPERATION PROCEDURE

Title: Clinical Web Portal Safeguarding Note (Button) Process to add an entry	**Procedure No:** **1**	**Document commenced:** February 2019		**Version:** 1
Procedure written by: Fiona Pickford Lesley Walker	**Procedure Approved By:** Trust Safeguarding Group	**Approved Date:** October 2019	**Review Date:** February 2020 **(currently under review June 2022)**	**Pages:** 3

1. **Objective**

   To ensure governance arrangements of the processes in relation to the Clinical Web Portal safeguarding note/button.

2. **Scope**

   The Royal Wolverhampton NHS Trust – all staff

3. **Supporting Policies**

   3.1. CP41 Safeguarding Children policy
   3.2. CP53 Safeguarding Adults policy
   3.3. OP12 IT Security Policy
   3.4. OP13 Information Governance policy
   3.5. OP07 Health Records policy

4. **Process**

Safeguarding concern identified – refer to CP41 Safeguarding Children policy and CP53 Safeguarding Adults policy.
Consider discussion with the Safeguarding Team.

↓

Safeguarding note to be raised via Clinical Web Portal.
All staff with access to CWP can create a note.

↓

Process to add safeguarding note

- Access Clinical Web Portal
- Search for patient
- Go to the 'Notes' section and select 'Create Note'
- Re-enter password
- In the 'New Note' Screen, select a category* from the drop down list under the **Safeguarding** criteria
- Disregard 'Tags'
- Select Yes or No to the question – 'Have you reported your Safeguarding concerns by following Trust Policy for this patient?'
- In the free text section - add brief details of the concern and contact details of the referrer
- Select 'Publish'

It is the referrer's responsibility to update the Safeguarding Note.
If an incorrect entry is made, the user should contact
ICT Systems & Applications Services Team - rwh-tr.softwareservices@nhs.net.

***Category List (see policy)**
- Adult – Deprivation of Liberty
- Adult – Discriminatory
- Adult – Domestic Abuse
- Adult – Emotional/Psychological
- Adult – Exploitation (Modern Day Slavery / Honour Based Violence)
- Adult – Financial
- Adult – Neglect by 3rd Party
- Adult – Organisational
- Adult – Physical
- Adult – PREVENT
- Adult – Self Neglect
- Adult – Sexual Abuse
- Adult – Sexual Exploitation
- Adult – Other
- Child – Development of child, health, behaviour, family relationships
- Child – Emotional harm
- Child – Medical Assessment
- Child – Missing
- Child – Neglect
- Child – Other
- Child – Physical abuse
- Child – Safety and protection, emotional warmth, stimulation
- Child – Section 17/Disability
- Child – Sexual Abuse
- Child – Sexual Exploitation
- Child – Child Protection Plan – Emotional Abuse
- Child – Child Protection Plan – Neglect
- Child – Child Protection Plan – Physical Abuse
- Child – Child Protection Plan – Sexual Abuse
- Mother – Unborn Child
- Safeguarding Note only
- Safeguarding Team Review

Process to review safeguarding note within 1 working day (by the Safeguarding Team)

- Reports will be generated by RWT Safeguarding Administration team on a daily basis and forwarded to the nominated nurse on call for review of entries against the Safeguarding Note.

Role of the Nominated Safeguarding Nurse

- Access Clinical Web Portal
- Select patient
- Access the 'Safeguarding Note' button (top right hand side of screen).
- Exit 'Safeguarding Note' button.
- Select 'Create Note' (in Notes section)
- Re-enter password
- Select 'Safeguarding Team Review' from the category list under the **Safeguarding** criteria
- Disregard 'Tags'
- Select No to the question – 'Have you reported your Safeguarding concerns by following Trust Policy for this patient?'
- In the free text section - add the preferred wording of 'Read and Acknowledged' plus any additional narrative required. Ensure contact details of referrer are recorded.
- Select Publish

- MASH checks are to be entered on the Safeguarding Note – use Adult or Child Other category. Add the preferred wording of 'MASH check completed' in the free text section.

If an incorrect entry is made, the user should contact Application Support

A monthly report will be presented to Trust Safeguarding Group for assurance, detailing the number of new entries on the Safeguarding Note and the number of reviews completed within timescale. This report will also state any missed reviews from the previous month, to provide assurance that they have been acted on.

Attachment 2: Approval of Documents and e-Documents Procedure

Purpose

The purpose of these processes are to ensure there is clear standardisation across all documentation produced and added to the patient's health record.

Prior to any new or amended documentation being introduced to the patient health record in either a paper or electronic format, it must first follow the below processes and be submitted for approval to the Health Records Documentation Approval Group (HRDAG). Refer to HRDAG Terms of Reference

Refer to printable flow chart in addition to detailed procedure below - Health Records Documentation Approval Process for Paper and EDoc

Procedure to Follow for paper documents:

All new documentation is subject to appropriate consultation within the local Directorate in which it is to be used prior to submission to the HRDAG

If medication forms part of the document this must also be approved through **MMG (Medicines Management Group)** prior to submission**.**

Initial draft must go through the medical illustration team who will format the document to the below standard requirements then issue a unique (MI) reference number or update version for amended documents

Following local consultation and processed by medical illustration, the final document will need to be submitted to rwh-tr.healthrecordsdocumenationapproval@nhs.net for advice and format approval.

Completion of the Documentation Approval Request form (Attachment 2.3 New/amended Documentation Approval Request Form) must also accompany the submitted document to support the panel in approving the document. It must include the reason for its implementation and the plan for where it is to be filed, scanned or designed into either the paper or electronic patient record. **With the implementation of electronic records, consideration must be made as to whether the new document can be produced and stored in an electronic format**

Following discussion and agreement, the final draft of the document will be added to the agenda for the next HRDAG by the Head of Health Records Services and the author will be invited to present the document.

The Group will either approve the document or suggest amendments to be made. If amendments are required, the document must be resent to the Medical Illustration Team for changes to be made then returned back to the Head of Health Records Services for final approval within 3 months of the changes requested. If amendments have not been applied within this timeframe the document will be removed from the outstanding list and a resubmission to the group with attendance will be required

The final approved document must be forwarded to the medical illustration team by the Head of Health Records Services confirming final approval for use for use

Standard Requirements for all paper documents

- Trust Logo (to be on the top right hand side of the document)
- First page, space on top right hand corner of the document for a large patient ID label or small label if document is held at the bedside. For additional pages (either double sided, or a booklet) across the top of each page must state
  Name …… NHS number …… Unit number……..
  Or space on the top right hand side of each page to house a small ID label. This is so that in the event of the document or booklet being scanned, the document to whom the patient belongs can be identified should it need to be reproduced at a later date
- Document Title (to be printed on top left hand corner of document)
- Where entries are made within the document, there must be space to allow the following information to be recorded
  Signature…….Designation…….....……Stamp……..Date……
- Reference number – provided by medical illustration prior to submission to the Health Records Documentation Approval Group
- For amendments to current documentation track changes to the document must be clearly made
- Paging number format e.g. page 1 of 1 if a single page or page 1 of 3 , 2 of 3…. for additional pages.
- Documents containing initials (with exception of charts) will need an evidence of initial section containing Name, Designation, Signature, Stamp and initial.

Procedure to Follow for requesting electronic designed documents:

A paper document must have approval through HRDAG (above process) prior to request submitted to convert to electronic design, to request this follow the below process:

Approved document to be sent to the IT rwh-tr.itservicedeliveryteam@nhs.net . Completion of an IT Request for Change (RFC) (Document 2 ICT Systems & Applications Services: Bantham Technologies Request For the creation or amendment of an electronic patient record)

Electronic draft will be completed as close to original approved paper document as possible and sent for draft approval to author.

Once author has approved draft author to submit draft to the Head of Health Records Services for virtual approval through HRDAG

The Group will either approve the document or suggest amendments to be made. If amendments are required, the draft must be resent to the IT rwh-tr.itservicedeliveryteam@nhs.net for changes to be made then returned back to the Head of Health Records Services for final approval.

The final approved draft must be forwarded to the IT rwh-tr.itservicedeliveryteam@nhs.net who will approve and implement final draft for use

Standard Requirements for all electronic documents

- **Original paper document must follow the above approval process prior to requesting conversion to electronic version**
- **Electronic design must reflect original paper document as much as possible**

Health Records Documentation Approval Group

TERMS OF REFERENCE

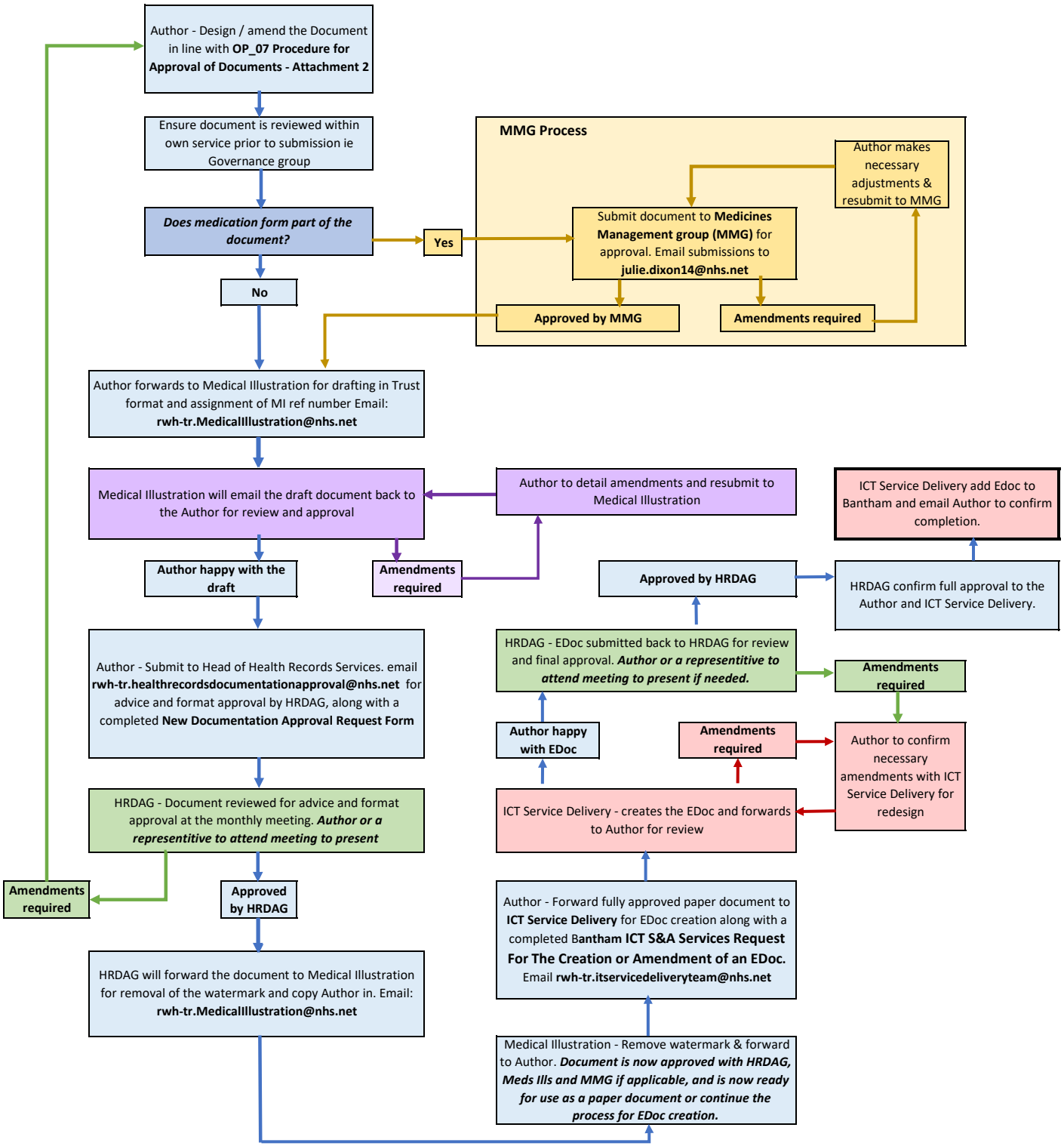
Trust Strategic Objectives	- Proactively seek opportunities to develop our services. - To have an effective and well integrated local health and care system that operates efficiently. - Be in the top 25% of all key performance indicators.
Meeting Purpose/Remit	The purpose of the Health Records Documentation Approval Group (HRDAG) is to review current and proposed new health records documentation against the OP07 Health Records Policy including care plans, clinical forms and any documentation that may become part of a patient's health record. The HRDAG will support the implementation of a fully integrated patient health record, feeding into the Health Records Project Group (HRPG) Group and other relevant projects as required.
Responsibilities	• To review, make recommendations and approve new and amended health records documentation across the Trust against Health Records OP07 Policy ensuring the principles of a standardised approach are upheld in both paper and electronic format. • Ensure any recommendations are implemented • Provide assurance to HRPG on compliance to health records keeping • To support the implementation of the Trusts migration to ensure alignment to an electronic patient record. • To support the development of electronic patient records
Authority & Accountabilities	- The group is chaired by the Head of Health Records Services or nominated Deputy and is directly accountable to the HRPG for the delivery of its Terms of Reference (TOR) and those of its reporting subgroups. - The group will review, make recommendations or sign off newly

	created or amended health records documentation in all its formats. - The group is authorised to seek any information it requires from any working group or specialist lead; all directorates are directed to co-operate with any request made by the Group. - To provide assurance to commissioners - Author of the documentation is responsible for submission to the group in a standard format against standards set within the Health Records OP07 policy - Authors are accountable for ensuring any recommendations made by the group are make and resubmitted for final approval before use. - To be a point of guidance for health records documentation related issues
Reporting Arrangements	Health Records Documentation Approval Group will provide quarterly update reports to the Health Records Project Group (HRPG).
Members	Regular members required to attend or send an appropriate deputy. - Chair (Head of Health Records Services) - Deputy Chair (Deputy Head of Health Records Services) - Division 1 Representative (Surgical) - Division 2 Representative (Medical) - Division 3 Representative (Community & Support Services) - Informatics Representative (Invite basis, specifically relating to electronic data capture forms in the main) - Quality Representative - Data Quality/coding Representative
Chair	Head of Health Records Services
Quorum	The Group will be quorate when the following members or their representatives are present: - Chair / Deputy Chair - Representative from 2 Divisions (either Division 1,2 or 3) - Representative from Quality - Clinician, AHP/Medical representation if document to be presented is AHP/Medical related

Frequency of meetings	Monthly or as required held last Tuesday of the Month and cut off date for submission of documents 8 days before
Administrative support	Health Records Services will provide secretarial support. Papers to be circulated one week prior to each meeting.
Standards	Royal College of Physicians Health Records keeping
Standard Agenda	**Core items** Apologies for absence Minutes of the Previous Meeting timeslots for authors Issues of significance / matters for escalation Any Other Business
Subgroups	
Date Approved	June 2022
Date Review	June 2024

Health Records Documentation Approval Process for Paper and EDoc

The Royal Wolverhampton NHS Trust



Guide to Review Boards and Meeting Schedules	
HRDAG	**Health Records Documentation Approval Group** - Meeting held last Tuesday of every month. Submissions needed 8 days prior to the meeting
MMG	**Medicines Management Group** - Meeting held First Thursday of every month. Submission of documents to be emailed to julie.dixon14@nhs.net

New/amended Documentation Approval Request Form

This form must be completed for requests for new or amended documentation which forms part of either the patient's paper or Electronic Health Record.

When completed it must be forwarded electronically to the Head of Health Records Services together with the draft version document which has been processed as per Attachment 2 Procedure for Approval of Documents The document will be reviewed to ensure it meets the standard requirements prior to submission to the Health Records Documentation Approval Group.

1	Document Title:
2	Does the document meet the specified standard requirements as set out in Attachment 2, Paragraph 8.0 Records Keeping Standards: YES/NO
3	Is this a new, existing document or Pilot? (Please state) For amended documentation is track changes clearly labelled? YES/NO Medical Illustration Reference Number:
4	Where appropriate, does the document consider accessible information standards (AIS), (e.g., communication barriers have been considered and recommendations made if required) YES/NO
5	Purpose of the document. (Please provide a brief description)
6	How will the document be stored (Electronically/Paper)? Is this document held at the bed side? Where in the record (Electronic or paper) will the document be filed/scanned to?

	Who will be responsible for filing or scanning the document?
7	What Groups / Committees has the document been discussed and agreed? Must have been through local meetings including governance, If medication forms part of the document this must also been through **MMG (Medicines Management Group)** Please include dates:
8	Please provide any further information you wish to be considered

Attachment 3: Management and Maintenance of a Health Record

Contents

1.0 Procedure Statement

This attachment sets out the standard for managing and maintaining health records in line with the Data Protection Act 2018, General Data Protection Regulation 2018, and the Records Management Code of Practice for Health and Social Care 2021. It explains the importance of data quality within the health record. This procedure details the merging and duplicates process and example scenarios to explain how to manage different types of duplicate records. This procedure also covers the transportation of records, including records required for domiciliary visits.

2.0 Document 1: Data Quality and the Health Record

Data Quality plays a vital role in providing high standards of patient care. We need accurate and timely information to deliver patients' treatment correctly and efficiently. Duplication of information can be a clinical risk to the patient therefore uniformity throughout the Trust is essential when dealing with duplicate registrations on the Patient Management System (PAS) and merging of health records in order to achieve a single registration for each patient.

In line with the Data Protection Act 2018, principle 4, information must be 'Accurate and kept up to date.

2.1 What is Data Quality?

Data quality is a measure of the appropriateness and integrity of information collected and used in operations, decision making and planning. The Trust defines data quality as being reflected in the criteria below. Data must be:

- **Complete** (in terms of having been captured in full)
- **Accurate** (the proximity of the figures to the exact or true values)
- **Relevant** (the degree to which the data meets current and potential user's needs)
- **Accessible** (data must be retrievable in order to be used and in order to assess its quality)
- **Timely** (recorded and available as soon after the event as possible)
- **Valid** (within an agreed format which conforms to recognised national standards)
- **Defined** (understood by all staff who need to know and reflected in Procedural documents)
- **Appropriately sought** (in terms of being collected or checked only once during an episode)
- **Appropriately recorded** (in both paper and electronic records)

This does not only apply to the recording of clinical information, but equally ensuring that patient demographic details are correct and up to date. Accurate and up to date information also minimises the risk of duplicate registrations which may lead to clinical risks (refer to OP91 Data Quality Policy).

At each visit, when checking patient details, you must ask the patient to confirm the details rather than you inform the patient of the details you hold.

- Can you confirm your **full name?**
- What is your **date of birth**?

- What is **full address and postcode?**
- Can you confirm your **telephone number** (landline and mobile)?
- Can you confirm your **GP** and practice details?
- Who is your **next of kin and what are their contact details?**
- Confirm your **ethnicity**
- Confirm your **religion**
- **Overseas visitor status** (refer to Overseas Patients Procedure)

For example, do not ask the question "**Is your GP Dr……?**", instead the question should be **"Please confirm your GP".** By asking the question in this way, you are more likely to obtain the most accurate information and avoid misidentification of a patient.

Deceased Patients
For staff that have the facility to record a patient as deceased on PAS, there are 2 steps to this process which must be followed. Firstly, you must mark the patient as deceased with the date of death. Secondly you must complete the "Remove Activity" function this will ensure any outstanding appointments or referrals are cancelled- in the system. This is to ensure that no further correspondence is sent to the patient's address, causing undue distress to the patients relatives.

If the patient has a main historic health record registered in "Manage Casenotes by patient" on PAS these paper records must also be obtained and updated to denote the patient's death by notifying the Health Records Library via email rwh-tr.HealthRecordsLibrary@nhs.net

Primary care
Once patient is marked deceased the record must be archived electronically.

Community The patient's paper record must also be obtained and updated to denote the patient's death.

Data Quality Monitoring
The collection of demographic patient information is monitored for accuracy and completion on a monthly basis, and compliance is reviewed by the Activity and Data Quality sub group (refer to OP91 Data Quality Policy or report can found here: Standards (xrwh.nhs.uk)

3.0 Document 2: Merging & Duplication of Health Records Procedure

The Head of Health Records Services (or designated deputy) is responsible for authorising access/training to the merge facility on PAS. Staff must undertake the relevant training prior to access being given. Access will be monitored refer to **Attachment 5: Health Records Audit and Monitoring**. When an authorised user has not used the function within 6 months access will be revoked and refresher training required for access to be re-instated.

Those authorised to merge must adhere to the procedure below:

3.1 Definition of a Duplicate

A duplicate is when there are 2 or more registrations that exist for the same patient on a system ie PAS, LILY and EMIS etc.

3.2 Definition of a Merge

A merge is the amalgamation of 2 or more registrations or health records that exist for one patient. The records must be merged in order to make one complete record.

3.3 Definition of Registration Numbers (PAS only)

Old registration numbers are registrations which must no longer be used:
Including those with only numeric numbers such as **98/12345**
or starting with prefix : **A C P R T LFB SC**

Current registration numbers are still to be used and include:
Starting with prefix : **B D E F G H K L M N V W**

3.4 Process to follow

There are many scenarios you may come across in the system and may require a different process. If you cannot find in the below table the process that fits your scenario for advise please contact the health records administration team on extension 88096 or email **rwh-tr.HealthRecordsIssues@nhs.net**

Patient has the following	**Administrative process on PAS**	**Process with Casenotes** (Note: casenotes must only be raised for areas where noteless working **has not** been adopted)	**Noteless Process**
One current registration with casenotes	No action required	Use these casenotes	Do not create notes use current registration number
One current registration without	Re-instate the current registration	Create a new set of casenotes using the	Do not create notes use

casenotes	number. Create this number within the casenotes tracking module	current registration number	current registration number
Two current registration numbers both with casenotes	Merge into current registration number with most history	Merge into current casenotes with most history as per PAS process	Merge into current registration number with most history and use this number
Two current registration numbers both without casenotes	Merge into the most current registration number	Create a new set of casenotes using the current registration number	Merge into the most current registration number and use this number
Two current registration numbers, one with casenotes and one without	Merge into current registration number with casenotes	Use the casenotes of the current registration number	Create a new registration number and merge x 2 previous numbers into new number created
Two current registration numbers. One with casenotes and one with microfilmed casenotes	Merge the microfilmed registration number into current registration number	Use the casenotes of the current registration number	Merge the microfilmed registration number into current registration number with notes and use this number
Two current registration numbers One with casenotes and one scanned casenotes	Merge the scanned registration number into the current registration number with casenotes	Use the casenotes of the current registration number	Merge the scanned registration number into the current registration number with casenotes and use this number
Two current registration numbers	Merge the microfilmed registration number	Create casenotes of the current registration number	Merge the microfilmed registration

One without casenotes and one with microfilmed casenotes	into current registration number		number into current registration number and use this number
Two current registration numbers One without casenotes and one scanned casenotes	Merge the scanned registration number into the current registration number	Create the casenotes of the current registration number	Merge the scanned registration number into the current registration number and use this number
Two microfilmed registration numbers	Re-issue to most current number and merge with the older registration number	Create new casenotes using the re-issued number	Create new casenote number and merge the 2 microfilmed numbers into the new created registration number
Two scanned registration numbers	Create a new registration number and merge both scanned registration numbers into the new registration number	Create new casenotes using the new registration number	Create a new registration number and merge both scanned registration numbers into the new registration number
One microfilmed current registration number and one scanned registration number	Re-issue the microfilmed number and merge with the scanned number	Re-issue casenotes for the microfilmed number	Merge scanned number into the microfilmed registration number and use this number
One microfilmed old registration number and one current scanned registration number	Create new registration and merge with the old microfilmed and scanned number	Create new casenotes for the new registration	Re-register patient and merge scanned and microfilmed

			numbers into new registration created and use the new number
One microfilmed old registration number and one old scanned registration number	Create a new registration number and merge both old registration numbers into the new registration number	Create new casenotes for the new registration	Re-register patient and merge scanned and microfilmed numbers into new registration created and use the new number
One old registration number with notes	Create a new registration number and merge the old registration number into the new registration number	Create new casenotes using the new registration number and merge the old casenotes into new casenotes	Create a new registration number and merge the old registration number into the new registration number and use this number
One old registration number with no notes	Create a new registration number and merge the old registration number into the new registration number	Create new casenotes using the new registration number	Create a new registration number and merge the old registration number into the new registration number and use this number
Old registration number and current registration number both with casenotes	Merge old registration number into current registration	Merge old registration casenotes into the current registration number	Merge old registration number into current registration and use this number
Old registration number with casenotes and	Merge the old registration number into the current	Create new notes for current registration number and merge	Merge the old registration number into

current registration number without notes	registration number	old casenotes into current registration number	the current registration number and use this number
Old registration number without casenotes and current registration number with casenotes	Merge the old registration number into the current registration number	Use the casenotes of the current registration number	Merge the old registration number into the current registration number and use this number
Old registration number with no casenotes and old microfilmed registration number	Create new registration number and merge both the old registration number and the microfilmed registration number into the new Registration	Create new casenotes for the new registration. Inside the new casenotes Record the microfilmed numbers	Create new registration number and merge both the old registration number and the microfilmed registration number into the new registration number and use this number
Old registration number with casenotes and old microfilmed registration number	Create new registration number and merge both the old registration number and the microfilmed registration number into the new registration	Create new casenotes for the new registration and merge the old registration casenotes into the new registration casenotes. Inside the new casenotes record the microfilmed numbers	Create new registration number and merge both the old registration number and the microfilmed registration number into the new registration number and use this

3.5 Demographic details

Where a merge is undertaken, every effort must be made to ensure that all up to date demographic details are transferred from the minor registration number

(referred to old number or number to be merged) into the major registration number (referred to new number or number to be retained and used) prior to the merge taking place in order to ensure that no data is lost.

3.6 Children's Adoption Records

Extra care must be taken for children's records which have 2 registrations with different NHS numbers. This may indicate that the child has gone through an adoption process. Both patient details must be sent to rwt-tr.lachealthassessments@nhs.net for local process to be followed.

The records of adopted children can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.

3.7 Transgender Persons

Patients over the age of 18 may request to change gender on their patient record at any time and do not need to have undergone any form of gender reassignment treatment in order to do so or possess a. (as defined by the Gender Recognition Act 2004) a Gender Reassignment Certificate which is issued by the Gender Reassignment Panel. At this time a new NHS number can be issued however this process would be initiated by the GP. A re- registration on PAS can be created, if it is the wish of the patient. It is important for the clinician involved in the patient care to discuss with the patient what records are to be moved into the newly created record, this should be usual practice to merge all existing records into the new records created. The previous record should be archived and only accessed for valid clinical reasons for doing so.

3.8 Title Change

It is good practice to have change requests in writing from the patient if possible. A title change can be made to a patients record on request.

3.9 Name Changing

It is good practice to have change requests in writing from the patient if possible. A full name change can be changed on systems however evidence of a deed pole name change must be shown to apply these changes to the records. A copy of the deed pole certificate must be taken and kept within the patients record for electronic records on CWP this can be scanned under advanced directives. For marital surname changes the same applies a copy of the marriage certificate is required.

3.10 Incorrect Merge of Records

Every care must be taken to ensure that all merges are carried out correctly, however if a merge is undertaken in error, you must contact The Administration Team in Health Records Services on Ext.88096 or email rwh-tr.returns@nhs.net for further advice and investigation.

3.11 Incident Reporting of Incorrect Merges

Where an incorrect merge is found the Administration Team in Health Records Services will establish the area which created the error and an incident will be raised on the Datix system. All such incidents will be monitored and reported via the Merges and Duplicate Group.

4.0 Document 3: Transportation of Health Records

Confidentiality must be maintained at all times when transporting patients' Health Records. The following rules must be followed:

- You must always place records in a sealed envelope or document wallet when carrying records from ward to ward. This prevents pages being accidentally lost and prevents people from reading personal information written/printed on the folder.

- It is forbidden for patients to transport their own records, even in the event of them being required for adjoining appointments. When sending notes between departments via the internal mail system, you must ensure that the envelope clearly states the name and department of the recipient. In the case of sending notes in a previously used envelope, you must ensure that all previous names and departments have been clearly crossed through, to avoid delivery to the incorrect department.

- When transporting large bundles of records around the site, they must be delivered using appropriate covered trolleys.

- Health Records must never under any circumstances be left unattended during transportation.

- Original health records must not be sent out of the Trust. Records must be photocopied, unless in very exceptional circumstances (please see Attachment 5 for further information). When a Primary Care Services patient moves GP surgery, the original record must be sent back to the CAPITA Primary Care Service (centralised service).

- In all cases where records are sent to another department, the records must be appropriately tracked (refer to Attachment 6 Storage and Retrieval of a Health Record – Document 2 Health Records Retrieval and Tracking).

- Only Trust approved methods of transporting confidential information must be used. For internal transfers, this will be via internal postal system. For external transfers, this must be sent by recorded delivery, or by contacting Switchboard or the internal Hospital transport for use of the Trust approved external transport.

- Requests for Health Records or other confidential information made by external agencies such as Police, other hospitals etc. must be forwarded to the Health Records Access Co-ordinators for processing on Ext. 85544 or email rwh-tr.healthrecordsaccess@nhs.net (refer to Attachment 4 - Subject Rights Requests and Other Patient Information Requests)

When transporting patient notes for domiciliary visits, you must only take the notes relating to the individual patient you are treating into the patient's home. Service providers must ensure that sealed containers ie a bag or box of any description with a facility to secure house patient records and provide a safe store for all records contained within the vehicle. It must be mandatory that at the end of the working

day all patient records must be returned to the service area. If, under exceptional circumstances, patient information cannot be returned by the end of the working day the member of staff responsible for them must contact a team leader or senior member of staff to discuss and agree any alternative arrangement. It is the responsible for the member of staff to transport patient records safely and securely whilst in their possession.

Adult Community Services Group have a separate SOP for the safe Transfer of Sensitive and Confidential Information (Refer to G22 Safe Transfer of Sensitive and Confidential Information Adult Community V5.0)

5.0 Document 4: Management and Maintenance of the Health Record in the Absence of Electronic Systems and Processes

This section explains the manual process to follow in the absence of the Trusts electronic patient recording systems ie Patient Administration System (PAS). This system is used to track the patient and their Skinny File (current inpatient episode of care) and any other manual records. A process has been provided below to assist in understanding which process(es) to follow and which documentation to complete.

Please print the documentation applicable to your Area for your in case of emergency. In the case of a Major Incident please refer to your local Business Continuity Plan.

5.1 Chart 1: Patient Admission via ED (no PAS) Process

Flow chart detailing management of patient record (Skinny File) in the event of total loss of Patient Administration System (PAS): Chart 1: Patient Admission via Emergency Department

5.2 Chart 2: Elective Surgery Areas

Flow chart detailing management of patient record (Skinny File) in the event of total loss of Patient Administration System (PAS): Chart 2: Elective Surgery– No PAS Process

5.3 Skinny File Creation Log

In the event of total loss of the Patient Administration System (PAS) all patients admitted where a Skinny File is created, must be recorded. PAS must be updated (once available) by the Team creating the SK. If patient transferred to another Ward / Area please complete the tracking log (Skinny File Creation Log Template).

5.4 Ward Tracking Patient Skinny Files In/Out Log

In the absence of a Ward transfer book, use this log to track skinny files in and out of the Ward. This is required in the event of total loss of the Patient Administration System (PAS). Ward Tracking Patient Skinny Files In-Out Log Template 4

Chart 1: Patient Admission via Emergency Department

Flow chart detailing management of patient record (Skinny File) in the event of total loss of Patient Administration System (PAS).

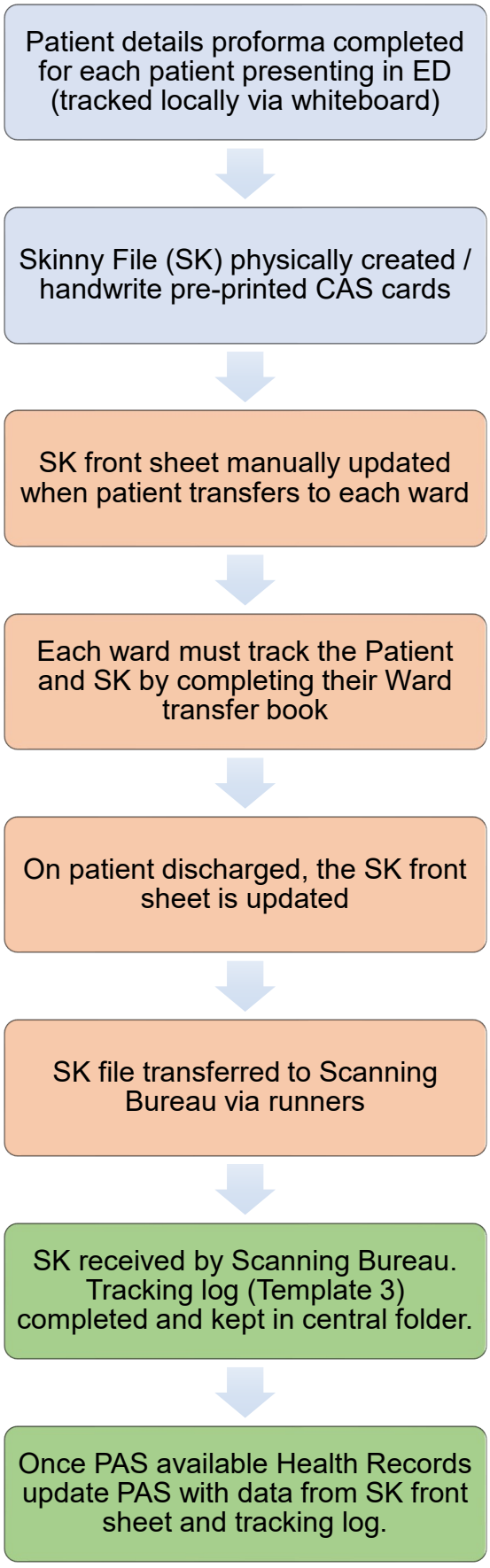
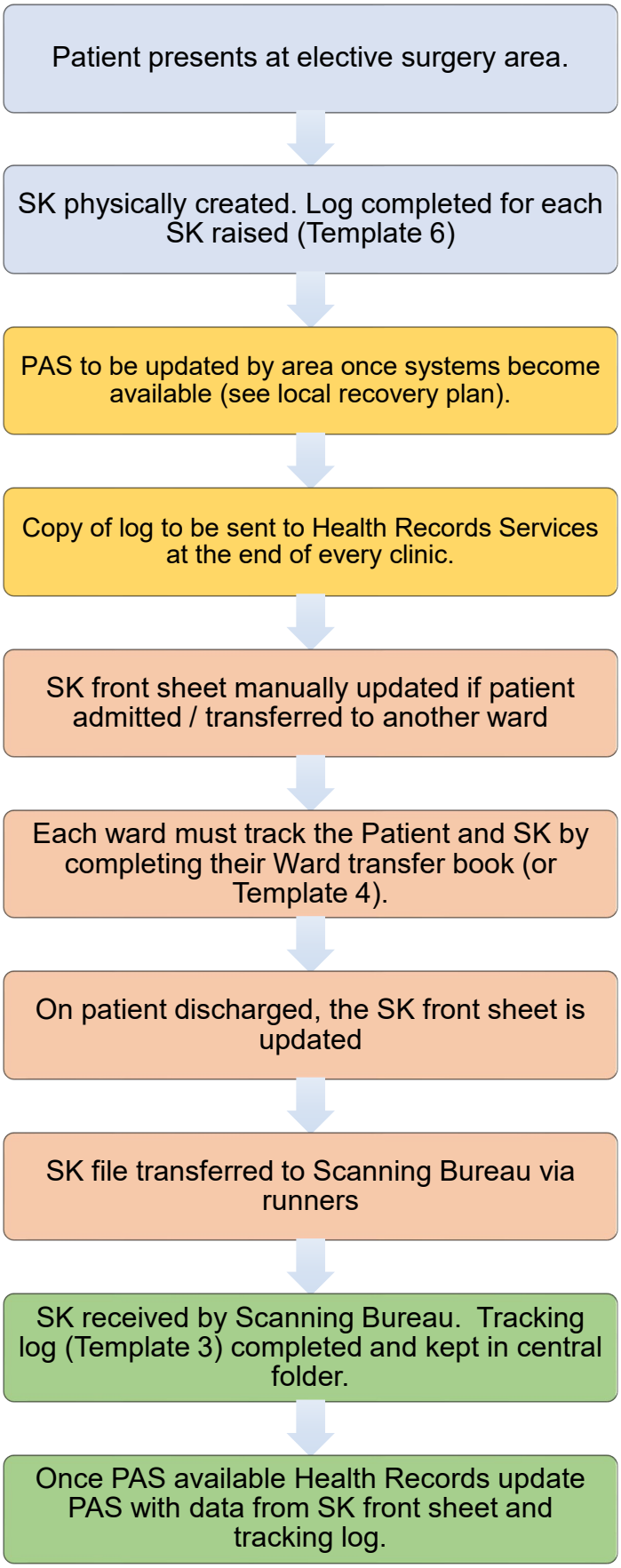


Chart 2: Elective Surgery– No PAS Process

Flow chart detailing management of patient record (Skinny File) in the event of total loss of Patient Administration System (PAS).



Skinny File Creation Log

In the event of total loss of the Patient Administration System (PAS) all patients admitted where a Skinny File is created, must be recorded. PAS must be updated (once available) by the Team creating the SK. If patient transferred to another Ward / Area please complete the tracking log (Template 4).

Staff Member	Patient Name	Hospital Number	Patient D.O.B	Date of Admission	Time of Admission	Area / Ward

Attachment 4: Access to Health Records and Subject Rights Requests Procedure

Contents

1.0 Procedure Statement

The purpose of this procedure is to ensure that all requests for patient information, including Subject Rights Requests, received by the Trust are processed in line with the General Data Protection Regulation, the Data Protection Act 2018, and the Access to Health Records Act 1990 (in the case of deceased patients). This procedure includes the following individual rights:

- The right of access
- The right to rectification
- The right to restrict processing
- The right to erasure
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

This protocol also details the provisions for accessing the health records of deceased patients, and also provides the processes to follow when disclosing and sharing specific patient information to external organisations; for example the Police, the Courts, Coroner's Office, and other hospitals, including what information must be redacted or exemptions applied prior to, or to prevent disclosure.

OP85 Information Sharing Policy sets out the principles and standards that staff must follow when sharing personal data. The procedures detailed within this protocol ensure those standards are met, confidentiality is maintained, and statutory requirements adhered to.

Please note that this procedure does not cover the processing of staff/employment subject access requests or Freedom of Information (FOI) requests. More information on Staff requests can be found in HR09, Personal Files.

2.0 The Right of Access

2.1 What is a Data Subject Access Request?

All patients (or their next of kin or suitable patient representative with authority to act on their behalf) have a legal right to view or have copies of their personal information and any supplementary information that the Trust processes (refer to OP07 Attachment 1 for further information). The right of access allows individuals to be aware of and verify the lawfulness of the processing of their information, though this must also be covered by a comprehensive privacy notice. This request for information is officially known as a Data Subject Access Request (DSAR).

The GDPR applies to all personal identifiable data in all formats including, but not limited to, paper records, electronic records, emails, faxes, registers, inventories, audit logs, CCTV footage, genetic and biometric data. Patients are entitled to know exactly what, and have access to, all information the Trust processes about them, whether or not it is held in the primary health record.

2.2 What do I do if I receive a Subject Rights Request?

It is vital that confidentiality is maintained at all times and that all requests are dealt with in accordance with the OP13 Information Governance and Data Protection Policy as specific information is required from the patient in order to process their request and validate their identity.

All requests must be forwarded to: Health Records Access Team, Health Records Library, Location B19, McHale Centre, New Cross Hospital. Telephone: 01902 307999 ext. 85544 / 85545 or 88093 or email: rwh-tr.healthrecordsaccess@nhs.net

2.3 What might a DSAR look like?

Patients are entitled to any information the Trust processed about them including their health record, electronic records, emails, investigations, CCTV footage and audit logs of who has accessed their electronic records. They may apply the right of access verbally or in writing; this could include face to face, over the telephone or via social media. The request can be made to any department, or member of staff of the Trust, and not necessarily to a specific person or contact point i.e. the Health Records Access Team. A request does not have to include the phrase 'subject access request' or Article 15 of the GDPR, as long as it is clear that the individual is asking for their own personal data.

2.3.1 Standard Application Form

A standard DSAR application form, which facilitates the Health Records Access Team to undertake scoping and fulfil the request, is available for the patient to complete and submit in paper form or via email. Although we can invite patients to use this standard form, we must make it clear that that is not compulsory, and we cannot use this as a way of extending the 30-day time limit for responding. Subject Rights Request Form

A patient may only request access to certain parts of their record, or a particular speciality or period of time. Alternatively, they may request copies of emails from a particular Healthcare Professional relating to their care, or the patient may request access to all of the information the Trust holds about them.

2.3.2 Verbal Requests

If a request for information is made in person, for example if the patient is a current inpatient or is attending an outpatient clinic, you must adhere to the following process:

- Confirm the details of the data subject (patient)
- Confirm the details of the requestor (if different from above)
- Understand what information they are requesting copies of
- If the request is for copies of health records, multiple items, complex information etc, notify the requestor that this will be processed by the Health Records Access Team and that you will forward their details to the Team who will contact them within 2 working days.

2.3.3 Procedure for Copying Letters to Patients

If the patient requests a single letter or report, check that the Healthcare Professional in charge of their care is happy for the patient to receive a copy and arrange for this to be provided, refer to guidance and standards below:

Introduction

The NHS Plan, published in July 2000, made a commitment that patients should be able to receive copies of clinical letters written about them.

"As a general rule and where patients agree, letters written by one healthcare professional to another about a patient should be copied to the patient or, where appropriate, parent or legal guardian. The general principle is that all letters that help to improve a patient's understanding of their health and the care they are receiving should be copied to them as of right. Where the patient is not legally responsible for their own care (for instance a young child or a child in care), letters should be copied to the person with legal responsibility, for instance a parent or guardian."

This would also apply to patients with learning disabilities and/or lacking mental capacity when letters should be copied to the person with legal responsibility, for instance a carer or a person holding Lasting Power of Attorney or a Court Appointed Deputy.

What constitutes a 'letter'?

A 'letter' includes communications between different health professionals, for instance from and to GPs, hospital doctors, nurses, therapists and other healthcare professionals. Different types of letter include (among others):

- Letters or forms of referral from primary care health professionals to other NHS services;
- Letters from NHS health professionals to other agencies (such as social services, housing, employers or insurance companies);
- Letters to primary care from hospital consultants or other healthcare professionals following discharge or following an outpatient consultation or episode of treatment.

Benefits of copying letters to patients

The Copying Letters to Patients Good Practice Guidelines outline a number of potential benefits, these include:

- Increased level of trust between patients and professionals;
- Better informed patients: patients and carers have a better understanding of their condition and how they can help themselves;
- Better decisions: patients are better informed and make informed decisions about treatment options;
- Improved compliance with treatment;
- More accurate records: errors can be identified and actioned accordingly;
- Better consultations: patients should be less anxious, professionals will be prompted to explain fully all aspects of diagnosis and treatment;
- Health promotion: letters reinforce advice on lifestyle and self-care;

- Better communication between professionals: letters written in plain English, which avoid jargon;

However, it is recognised that not all patients wish to receive copies of correspondence and not necessarily for each and every consultation.

Notification to Patients Appointment letters to patients will include a statement to the effect that if the patient wishes to receive a copy of the letter relating to a particular outpatient visit, then during the consultation they should ask the consultant or other clinician undertaking the consultation, to send them one. If the patient does not raise the issue the clinician may nevertheless wish to discuss copying the letter with the patient.

The appointment letter will include the following statement:
"If you would like a copy of the letter that will be sent to your GP please ask the doctor or specialist when you are being seen." Patients who choose to receive copy letters must receive these communications in a form that ensures compliance with:

- The Equality Act 2010;
- The Data Protection Act 2018;
- The Accessible Information Standard 2016.

Recording of patient requests for a copy letter if a patient requests a copy of their letter, the clinician must note this when dictating their letter for typing. The Secretary will then copy the patient (or their appointed representative) into the letter. Directorates are to agree how this will be recorded and managed locally.

When should letters not be copied?
There are occasions when it is not appropriate for letters to be copied.

- When the patient does not want a copy.
- Where the letter contains potentially distressing information arising from investigations that have not previously been discussed with the patient. A copy letter should only be sent following discussion with the patient
- Where the letter includes information about a third party (such as a neighbour or family member) who has not consented to their information being provided to the patient.

In addition, there are some services where confidentiality is particularly important and where it may not be prudent to send copy letters to the patient's home. In such cases, concerns and alternative methods should be discussed with the patient. Sexual Health is an example of such a service, but this point may be applicable in any service dependent on the content of the letter.

For advice on the disclosure of patient information to patients or their representatives contact the Health Records Access Team on ext. 85544 or email rwh-tr.healthrecordsaccess@nhs.net.

Letters between healthcare professionals contain 'personal data' that form part of the patient's medical record and are therefore subject to the requirements of the Data Protection Act 2018. It is important that all letters are:

- Accurate and adequate for their purpose.
- Written clearly.
- Avoid unnecessarily complex language and subjective statements.
- Use plain English to improve readability.
- Avoid (where possible) technical terminology and acronyms.
- Set out facts and avoid unnecessary speculation.
- Confirm information given in discussion with the patient.

A balance is required between simplification for the patient's understanding and what is needed for the primary purpose of the letter between healthcare professionals discussing symptoms, test results and possible diagnoses and treatment. Clinical accuracy and ensuring the professional receiving the letter has all the information he/she needs is the main purpose of the letter and it is important not to compromise this in favour of making it easier to understand.

Note: although the letter itself should not be compromised in favour of making it easier to understand, the clinician is legally obliged to comply with the Accessible Information Standard 2016 whereby patients with a disability, impairment or sensory loss must be provided with the information they need and can easily understand. This might necessitate a separate explanation relating to the contents of the letter. The letter must clearly annotate when a copy has been sent to the patient.

Further information for patients
Some patients may want further information about the content of their letter or an explanation of terms. This may generate an increase in telephone calls to both the clinician and the GP - patients may contact the person named on the letterhead of the copy letter.

Should a patient request that the copy letter be emailed to them then this can be arranged, although clinicians must use the NHSmail encryption feature when sending the copy letter to patients with insecure or non-credited email services (see Sharing Sensitive Information Guide for NHSmail – for any queries regarding this feature, please contact the IT Service Desk.

Children and young people
Young people aged 13 and over are legally able to make decisions about their own healthcare and should be asked directly if they wish to receive copy letters. During consultations with younger children an assessment needs to be made as to whether the child concerned is able to make an informed decision about whether to receive a copy letter or whether a parent or carer would be more appropriate.

Correcting inaccurate records
Evidence suggests that healthcare professionals who routinely share records with patient's report that they often identify minor inaccuracies and mistakes. If a request is received directly to the service regarding an error in a letter, the service must first consider the extent of the correction: if the correction is minor i.e. incorrect

medication or incorrect history captured from this attendance and isolated to the letter concerned, this can be processed locally and does not need to be processed as a "Right to Rectification" request by the Health Records Access Team. However, it is important that any changes that are made, the original copy of the letter is retained (and not destroyed) and the amended letter added to the patient's record and sent to the patient.

Protecting confidentiality
Procedures are in place to minimise the risk of breaches in confidentiality. Personal details are checked with patients when they visit the hospital and information about them receiving copy letters will be included in both appointment and admission letters and on posters within local departments. Copy letters to patients will be marked 'Private and confidential'.

2.3.4 Solicitors acting on behalf of the patient

All solicitor requests for medical records must be forwarded to the Health Records Access Team (HRAT) who are responsible for processing Subject Access Requests where a Solicitor is acting on behalf of a patient. The Health records Access Team do not process Solicitor requests where the intention for requesting the medical records is to bring forth litigation against the Trust. Solicitor requests where litigation is intended against the Trust are forwarded to the Legal Services Team.

In the case of Solicitors, an official letter requesting patient information must be provided. It must also include written consent from the patient on a separate form of authority. Access will only be limited to the information or episode of care specified by the patient and the form of authority will only be valid if it has been signed by the patient within the last 6 months.

If the patient has specifically expressed that some or all of the information should not be disclosed (normally detailed on the solicitors consent form) or if they have provided the Trust with information on the assumption that it will not be disclosed, the information should be withheld until consent is obtained from them. Similarly, the records may contain information about the person that they (the subject) may not think is relevant to the application (e.g. change of gender, medical status or assaults they have suffered). Their consent should be obtained before providing sensitive personal information to their representative, for example, we would not normally include the subject's sexual health data unless specifically requested or without checking with the data subject first

As with all DSARs a 30-day statutory timeframe for completing the request will apply, unless the request is deemed manifestly unfounded or excessive and are only chargeable if they are classed as repetitive request. (Request for identical information that has been disclosed by the HRAT within the past 12 months) In the event that a request is deemed chargeable the HRAT will raise an invoice with the Finance department. Serious Harm Tests are completed by the treating Healthcare professionals prior to disclosure of medical records (see Section 5 below).

2.4 How do we validate a DSAR?

All requests received by the Trust must be recorded on the Subject Rights Request Database (by the Health Records Access Team). All requests are checked to

ensure that the 'data subject' is a patient of this Trust and that information is held about them.

If requests are made on behalf of the patient, then the requestor must have proper authority. This could be a consent form signed by the patient, or a valid power of attorney 'health & wellbeing' document. For children under 13 years old this may be the ID and birth certificate of both the parent and child.

2.5 What are the time frames for a Subject Rights Request?

It is vital that a request is logged with the Health Records Access Team without delay as the information requested by the patient must be provided within 30 days of receipt of the request and any information required to validate the identity of the requestor. The 30-day timeframe applies to all Subject Rights Requests (not just the right of access). The clock starts when the request is received by the Trust, regardless of how and where it comes into the organisation. An extension to the deadline may be granted if the request is particularly complex or extensive (see 2.6 below), giving the Trust a total of 90 days to respond in full. The patient will be notified of this by the Health Records Access Team as soon as the request has been validated.

2.6 Complex Requests

A request which is deemed to be particularly complex can increase its timescale to 90 days. Complexity is agreed on a case by case basis, considering the number of Directorates involved in the request, where records are held on microfilm or offsite storage, whether the request is part of a wider complaint or investigation process, if there are numerous requests received from the same individual, or if a number of systems to be searched, for example call logs, access audits, locally held (Directorate) systems or processes which rely on other bodies, such as NHS Mail email requests. A request being labour intensive does not mean it should be treated as complex.

2.7 Can we charge a fee?

DSARs are processed free of charge; however, the Trust has the right to charge a 'reasonable fee' to cover administrative costs if a request is deemed to be manifestly unfounded or excessive, particularly if it is repetitive. This will be assessed by the Health Records Access Team and charged accordingly.

2.8 What data do we normally disclose as part of a DSAR?

When a requestor asks for 'all' of their information, it is vital that we are clear about what this means. This is mainly due to vast number of systems utilised by the Trust with information not stored centrally or directly accessible by the Health Records Access Team.

a) Automatically included:

- The main physical / paper health record (blue notes)
- Scanned and 'skinny file' notes recorded on Clinical Web Portal
- Microfilmed records
- Adult Community Services
- Paediatric Community Services
- Emergency Department Records (CAS Card/MSS)

- Minor Injuries Unit (MIU) records at Cannock Chase Hospital
- Physiotherapy and Occupational Therapy
- Clinical Images
- Radiology
- Pathology (Vitalpac, CV Web, TD Web, ICE)
- Information included in the notestream on CWP, including any clinical emails uploaded

b) Not automatically included, unless specifically requested:

- Audit trails of access to the systems used by the Trust
- Email correspondence searches
- Directorate level software & system searches
- Wolverhampton Special Care Dental Service
- Sexual Health Services
- The Maltings
- Foot Health Services
- The Phoenix Walk-In Centre
- Datix Risk and Incident Management System
- GP Records (Primary Care Service Practices)
- Safeguarding Information (as appropriate)

c) Information held locally

All Directorates, when requested to by the Health Records Access Team, must ensure that all systems, both manual or electronic, are reviewed to identify all identifiable information and provide it to the Health Records Access Team, to ensure that the Trust is providing the requestor with all available information, regardless of what format the information is kept in.

2.9 What about information held separately to the main health record?

2.9.1 Separately Held Records

Requests to access records held separately to the main Trust wide systems, for example the Children's Health Visiting, Adult Community Nursing Teams, or Sexual Health Services, must be coordinated by the Health Records Access Team. Requests must be reported to the Health Records Access Team without delay. The community service must then collate the information requested and provide that to the Health Records Access Team for redaction and to apply exemptions as appropriate (see Section 7 below). All community-based services must ensure that all systems, both manual and/or electronic, are reviewed to ensure we are providing the patient with all of the information they have requested. Any breaches to timescales will be reported to the Directorate Manager.

2.9.2 Primary Care Services

Requests to access records received by or involving Primary Care Services (i.e. RWT GP Practices) must be coordinated by the Health Records Access Team. Any new requests received by the GP Practice must be forwarded immediately to the Health Records Access Team so that the request can be formally acknowledged, logged, and processed. Although the HRAT have direct access to the PCN electronic records, the Practice will be required to collate and scan in any

information not already available via the EMIS or Docman systems, such as the Lloyd George record cards. Any breaches to timescales will be reported to Primary Care Services Central Team.

2.9.3 Local Systems and Directorate/Speciality Level Data

If patients request specific information which does not normally form part of their main health record, such as information held on a local database, the Health Records Access Team will inform the Directorate Manager for that area. The Directorate Manager will refer to their local Information Asset Register to understand what information may be held locally. Information Asset Owners must then provide copies of this data to the Health Records Access Team within the statutory timescale for review, redaction and to apply any relevant exemptions.

2.9.4 Email Correspondence

The NHS mailbox of any employee engaged in an individual patient's care can be audited or integrated into the patient's health record. NHS mail allows detection of emails that include patient identifiable data. Staff NHS Email accounts may be subject to searches for identifiable patient information. This includes any emails uploaded to the Clinical Web Portal Notestream.

You may be asked to provide copies of emails that identify a data subject (normally a patient, their family or personal representatives) to the Health Records Access Team.

For emails not uploaded to Clinical Web Portal Notestream (see Attachment 2 for further information), the Health Records Access Team will contact NHS Mail mailbox owners and notify them that a search is taking place and outline the process to provide assurance that any data 'about them' and not the data subject, including their personal contact details etc, will be redacted from the emails prior to disclosure.

2.9.5 Audit Logs

If An audit trail of access to the patient's electronic health information is required. This could include any system that contains electronic patient personal data. If the request is part of a DSAR, and the data is held on the Patient Administration System (PAS) or Clinical Web Portal (CWP) a request is completed by the Health Records Manager, authorised by the Head of Health Records Services, forwarded to the Head of Software Services, and ultimately approved by the ATCO.

For systems held locally, the HRAT will send request to the Information Asset Owner and Directorate Manager, to request an audit trail is reported and a copy is sent to the HRAT to be disclosed as part of the DSAR. This audit trail will be reviewed and redacted as appropriate (in line with GDPR) and exemptions applied as appropriate. Directorates must provide assurance that access to their systems, to the best of their knowledge, is legitimate.

2.9.6 CCTV footage

All requests to view CCTV footage will be sent to the Local Security Management Specialist. Requests for CCTV images must follow the same principles as a

Subject Access Request. For more information, please contact him directly on Ext. 84382 or email paul.smith8@nhs.net.

2.10 Time of Birth Requests

Requests for 'Time of Birth' will be processed in the same way as Subject Access Requests, the only difference being that consent must be received from the mother, as that is where the information pertaining to the time of birth is recorded. In the event that the mother's consent cannot be obtained (and the records still exist) then a decision will be made on a case-by-case basis.

2.11 Requests for information about children

Even if a child is too young to understand the implications of their subject access rights (normally 13 years of age, subject to an assessment of competency under the Gillick Competency Framework), it is still the right of the child, rather than of anyone else such as a parent or guardian i.e. it is the child who has a right of access to the data held about them, even though we recognise that in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, we must consider whether the child can understand their rights. This is considered to be 13 years of age. If the Healthcare Professional involved in the child's care is confident that the child understands their rights, then we would usually respond directly to the child through the normal process. We may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

When considering cases, you must take into account, among other things:

- the child's level of maturity and their ability to make decisions like this
- the nature of the personal data requested
- any court orders relating to parental access or responsibility that may apply
- any duty of confidence owed to the child or young person
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment
- any detriment to the child or young person if individuals with parental responsibility cannot access this information
- any views the child or young person has on whether their parents should have access to information about them.

3.0 Requesting to view a patient's health records

A request can be made to view the records rather than request copies. In this case, the information requested must be collated within the 30 / 90-day timeframe (as agreed), and a suitable date and time arranged for the patient/requestor to meet with a member of the Health Records Access Team or an appropriate Healthcare Professional to view the information. The Health Records Access Team must still check for any third-party data, exemptions and redactions before the information is disclosed.

3.1 Meeting with a member of the Health Records Access Team

The presence of the Health Records Access Team member is to ensure the safety of the information only and the staff member must not comment on the information in any way. If during the meeting the requestor raises any queries or concerns about the information, this will then be managed as a Subject Rights Request as applicable.

3.2 Meeting with an appropriate Healthcare Professional

The Health Records Access Team will escalate this request to the most appropriate Healthcare Professional to arrange a meeting. The Health Records Access Team will provide the records, attend the meeting, and advise from a Data Protection perspective, and coordinate any further actions agreed at the meeting.

4.0 Other Types of Requests to Disclose Information

Sharing data across and between organisations can be a complex process. Information exchanges must always take place within the legislative framework; essentially Data Protection Legislation; Human Rights Act 1998; Children's Act 2004; Care Act 2014; the Crime and Disorder Act 1998 and various statutory provisions and common-law rules for exchange or prohibitions on disclosure. If not covered below, please refer to OP85 Information Sharing Policy.

4.1 **Access to Deceased Patient Records**

Access to the health record of a deceased person is governed by the Access to Health Records Act (1990). This legislation relates to deceased patients only. Such disclosure should be made within 40 calendar days.

Under this legislation, when a patient has died, only their personal representative (evidenced by Grant of Probate, Letter of Administration, Certified Copy of the Last Will & Testament) or anyone having a claim resulting from their death (this could be a relative or another person), has the right to apply for access to the deceased's health records. Requestors must provide sufficient information to support their application and evidence that they have authority to act on the patient's behalf.

The grounds for refusing such requests include:

- the disclosure is likely to cause serious harm (the physical or mental health) of anyone
- It relates to a 3rd party (not the health care professional) who has not given consent for the information to be disclosed
- The Information was provided by the data subject (patient) in expectation of and/or specifically indicated that it should not be disclosed
- Disclosure is restricted by a court order.

All requests will be looked at on a case-by-case basis. All Access to health Records Act requests are coordinated by the HRAT.

AHRA application Form

4.2 Health Care Professional within the Trust

It is strictly prohibited for staff who are not directly involved in the care of a patient to access their records. For more information, please see OP97 Confidentiality Code

of Conduct for Staff. Staff can access a patient's record for the delivery of, or the administration of, their direct care and treatment e.g. directly caring for and treating the patient, recording the care provided, booking their appointments etc. The legitimate access of health records is routinely monitored by Health Records Services (see Attachment 5: Health Records Audit and Monitoring).

4.3 Health Care Professionals outside of the Trust

When receiving requests from external Healthcare Professionals, for example GP's, other hospitals, private healthcare providers, HMP Prison Services, access must be restricted to the information that is relevant to the patient's continuing care only and RWT consultants are required to review the information prior to disclosure. Any requests from a healthcare professional outside of RWT must be forwarded to the Health Records Access Team (unless this is overridden by an agreed local process between two Services).

4.4 Police Requests Procedure

4.4.1 Police request for Medical Records

In the event that the police require medical records, the request must be forwarded to the Health Record Access Team as soon as possible, from wherever it may be received within the Trust.

The Police will be asked to provide a completed Data Protection form (normally a W170) as it is the safest way to ensure that the application being made is wholly accurate, comprehensive and valid, prior to the Health Records Access Team obtaining medical records. All Data Protection forms will require a signature from the Police Officer requesting the information and a counter signature from their senior officer (normally Detective Inspector). It is important to note that a Data Protection form is not a mandatory requirement and information can be released without one, again on a case-by-case basis, however a formal written application must still be received

Patient consent to access the records must also be provided however this is not always possible and all requests for information must be viewed on a case-by-case basis as it may be that information can be released if it is in the best interest of the patient or an appropriate exemption is applied (i.e. prevention or detection of a crime, prosecution and apprehension of offenders). Consent is not always required, and the Police must state the legislation that they are requesting the information under.

All such requests where the authority of the patient has not been sought or is not appropriate, or where a court order has not been obtained, should be referred to Legal Services for advice and support, but must be escalated to the Data Protection Officer for ultimate approval.

All Police requests received are logged by the Health Records Access Team. Copies of the requested information is recorded to serve as evidence of disclosure.

4.4.2 Police Request for a Medical Statement

In the event that the Police require a medical statement from a Healthcare professional the request must be forwarded to the Health Records Access Team Asap who will determine which Healthcare Professional the request must be forwarded to.

The statement will normally relate to a particular episode of care. The relevant Healthcare Professional can be located by viewing the patient's electronic record via clinical web portal, once it is determined who is responsible for providing a medical statement, the details can then be passed to the Police who can liaise directly with the appropriate clinician.

4.4.3 Urgent Police Requests

There are times where the police may require copies of records urgently. Reasons for this could include:

- holding a suspect in 24-hour custody and records will assist the police in making a charging decision
- Severity of the crime committed, and the urgency required in obtaining the records (case by case basis)
- If information is not provided, it will place one or more persons at risk of harm
- In the public interest, e.g. murder, safeguarding children or adults at risk, gun or knife injuries, significant public health risks, significant risk to one or more individuals etc.
- Patient is a current inpatient (and records are not accessible to the Health Records Access Team)

Further to the urgent nature of the above scenarios, the Police can attend the Hospital and with the Ward Manager's discretion receive copies of the records. The original records must not be given.

If it is established that the request is deemed urgent, and the information is released, only the minimum of information must be supplied, and the rationale behind the decision to release the information must be clearly recorded.

4.4.4 Urgent Police Requests - Out of Hours Process

If outside of normal office hours, please carry out the check below before releasing health records to the police:

- Reason for the request must be established. If the request is not of an urgent nature, it must be referred to the Health Records Access Team the next working day.
- Police can provide the completed data protection form (not required but helpful for accuracy)
- Check what information the police are requesting and that it is relevant to the purpose stated on the form
- Check it is signed by the appropriate authority
- The identity of the police officer must be established (check ID if on site and ask at which station they are based).

- You must then contact switchboard and ask them to connect you to '101' plus the extension number you have been given. You can then select the station and confirm the details
- If the request is made by phone, you must take the details and inform the Police that you will call them back
- If this cannot be confirmed, no information should be released, and it must be referred to the Health Records Access Team the next working day
- Check that they have given a time period which is within scope of the investigation
- If required, check with a relevant health professional if there are any issues of capacity or mental health issues which need to be considered before disclosure. If there are concerns about the validity of a request in line with the purpose, then refer to the Legal Services Department as it may need a court order.

4.5 Coroner's Office

Coroner's requests are one of the few exceptions where original case notes/ skinny files must be forwarded as opposed to sending photocopies. If the original skinny file is yet to be scanned the Health Records Scanning Team must be allowed time to scan the file. Once it is showing on CWP (as scanned) the original skinny file is then collected from the scanning team to either be sent or taken to the Mortuary, alternatively the records may be collected by a member of the mortuary team.

For Trust related inquests, the Coroner will contact Legal Services department who then obtain the patient's records via the Health Records Access Team who will ensure the records are name checked prior to being sent to Legal Services.

For requests which are non-Trust related inquests, these will be processed directly by the Health Records Access Team and forwarded to the Coroner. These are received directly from the Coroners. No consent is required for these requests, and they are to be treated as a matter of urgency.

They will request the relevant information they require. It is advisable to clarify a specific timeframe for the medical records which are requested.

All notes forwarded to the Coroner's office must be correctly tracked out to ensure the whereabouts of the notes are known at all times. If inpatient stay(s) (skinny files) are required and have already been scanned on to the CWP the originals will have been destroyed (normally 30 days post discharge), if this is the case a printed version is acceptable as original paperwork. This will then be put in a skinny file and marked 'Coroner's copy only - original viewable on portal' this will be returned to the Health Records Access Team to be destroyed once no longer required. Refer to OP07 Attachment 8 Document 6. Admin Process in the Event of Bereavement, for more information.

4.6 Court requests for medical records and medical statements

All court ordered requests for medical records must be forwarded to the Health Records Access Team who will process the request in line with the deadline provided on the Court Order.

The Health Records Access Team will only provide records that have been requested and outlined on the Court Order, this can range from a specific part of the patient record or the entirety of the medical records. No records will be released until the Health Records Access Team are in receipt of a copy of the sealed court order.

In the case of requests for child records, where a child protection medical (CP Medical) has been requested, the records will be copied from the paper records. CP medicals must not be uploaded to Portal. If there is a delay in the courts receiving the medical information they have requested, an explanation must be provided by the Trust.

Requests for medical statements are to be forwarded by the Health Records Access Team to the Healthcare Professional responsible for treating the patient for required episode of care. The appropriate clinician will be listed on the Court Order

The HRAT work with the Healthcare Professional involved in the patients care to ensure that all relevant information is supplied as stipulated by the Court Order.

4.7 Regulatory and Supervising Authorities

Requests for regulatory or supervising authorities should be reviewed by the Health Records Access Team. A form of authority is generally included, detailing the patient's consent to release their records. These requests must be signed off by the Trust's Caldicott Guardian. Requests can be received from:

- General Medical Council (GMC)
- NHS England
- The Care Quality Commission (CQC)
- The Commissioner (CCG)
- The General Optical Council
- Research Sponsor Organisations (Research & Development)

4.8 All other requests

To be determined on an individual, case by case basis. Refer to Health Records Access Team for advice and guidance.

5.0 The Serious Harm Test

5.1 Clinical Approval to Disclose Patient Information

Once the requested information has been collated, an email is sent, along with the original request, to the Healthcare Professional(s) involved in the patient's care. This is to review potential harm or distress caused to the patient following release of the information.

In the event that the Healthcare Professional raises concerns with all or part of the record, a response would be provided to the patient in line with their recommendations. Sometimes, as required on a case-by-case basis, a meeting is arranged between the patient and the Healthcare Professional to discuss the information before it is released to them. This must all take place within the 30/90 day timeframe, as applicable.

In some cases, access to information may not be appropriate. Such cases include where providing access with regard to an individual's physical or mental health or condition would likely cause serious harm to them or to another person's health or conditions. All such cases must be discussed with the Healthcare Professional responsible for the clinical care of the patient before deciding if the exemption applies. If information is denied or restricted justification for the decision must be clearly documented within the record and the patient must be informed.

5.2 Safeguarding

A named officer with the Trust's Safeguarding Department will provide support to the Health Records Access Team in applying appropriate exemptions prior to disclosure of information to requestors in relation to cases where a safeguarding concern has been raised.

6.0 Information Obtained from Other Sources

Information obtained by the Trust from other sources (such as Social Care, Police etc) is normally held within the patient's health record. The Health Records Access Team may need to contact the originator of the information to inform them of the requested disclosure and consider any objections to this.

7.0 Exemptions and Redactions

Before any information is disclosed to the requestor, and in line with the finding from the serious harm test (above), the information is reviewed by the Health Records Access Team to determine whether there are any appropriate exemptions to be applied prior to disclosure of the information. Any information that should not be disclosed, such as third-party data, is also redacted at this point. Redactions can be completed both electronically using redaction software or manually (black marker and Tippex).

The Trust must provide reasons to the requestor for any redactions or exemptions applied, so that they may understand what has / has not been disclosed and why. The Health records Access Team record exactly what information has been disclosed or redacted within the request folder; so that this may be referred to if the case is reviewed through the appeals process.

Exemptions are to be applied on a case-by-case basis, and the context of the DSAR is important (consider why DSAR the request has been made) but some common exemptions to consider include:

- Safeguarding
- Parental orders
- Adoption records
- Human fertilisation and embryology
- Surrogacy
- Legal advice / litigation
- Child protection medical reports
- Victims of crime and prisoners
- Apprehension of offenders
- Where there is a current investigation in progress (prejudice the case)

7.1 Third Party Information

In general, information from or relating to third parties (including family members) should not be released to the Data Subject without first seeking the view/consent of that third party. However, it is only pertinent to ask for consent to release data when the data is solely about that person and not also about the data subject.

7.2 Relatives

The Health Records Access Team will need to distinguish between a relative's personal information and information about that relative that is simultaneously information about the person that we wish to release.

For example, "The child was voluntarily accommodated as mum was unable to cope due to post-natal depression" could be edited as "The child was voluntarily accommodated ~~as mum was unable to cope due to post-natal depression~~"

In balancing the Subject's right to know with mum's right to privacy, disclosing in line with the second option provides a context that would probably have been shared through life story work without disclosing mum's mental health issues.

7.3 Third Party Opinion

If an external professional is stating facts that the Data Subject has already been told (e.g. within a multi-agency meeting where the client was involved in the discussion) they can be disclosed. However, where a third party is giving an opinion then this would not normally be released without that person or their organisation giving consent. Even so, where we do not have consent, we still need to consider whether it would be reasonable to release the statement as it is likely that this opinion would have affected the way that the Trust has dealt with the person.

7.4 Medical Professionals

Where the disclosure of information relating to the subject's mental or physical health is likely to result in harm to the person or another individual then this should not be disclosed without first obtaining the view of the relevant medical professional. This could be the professional who treated the person and wrote the report/letter/opinion, or a current medical practitioner. We do not need the person's consent to contact a medical practitioner as we are asking the practitioner whether releasing the information would harm the person's physical or mental health.

7.5 Crime

Information can be withheld if its disclosure would prejudice the prevention or detection of a crime or the apprehension or prosecution of offenders. Similarly, information may also be disclosed without the expressed consent of the individual if it facilitates the apprehension and prosecution of offenders or the prevention or detection of a crime. The Health Records Access Team will review all available information before withholding or disclosing any information.

7.6 Social Work

Information held for Social Work purposes can be withheld if its disclosure would prejudice the carrying out of Social Work because of the likelihood of serious harm

to the patient or another person arising out of the release of the information. There must however be a quantifiable likelihood of serious harm to a person before this exemption is applied.

7.7 Legal Privilege

Discussions with and advice from our legal advisors are privileged and should not be disclosed. No emails, letters, or advice from the Trust's legal advisor can be provided to the applicant. Court documents including Court ordered statements are the property of the Court and should not be released. The requestor should be directed to their own legal representative or the Court to obtain these documents.

7.8 Staff Names

The Information Commissioner's advice is that staff names are disclosed provided there is no risk of harm to the staff involved. The names of the staff that have provided direct services to the person will usually already be known. It may still be appropriate to redact direct dial or mobile telephone numbers and email addresses in order to protect our staff from potential harassment.

8.0 Right to Rectification

Information must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal information that is found to be inaccurate, having considered the purposes for which it is being processed, is rectified (or erased) without delay. Patients have the right to request amendments and deletions to factual inaccuracies where the information the Trust processes about them is found to be inaccurate or incomplete amendments to records and adding addendums is the method we use for managing rectification requests, although deletions may be unavoidable; for example if the wrong patient data has been included in another patients record, and also where the 'right to erasure' applies (see section 11 below).

An opinion or judgement recorded by a health professional, whether accurate or not, must not be deleted. Retaining relevant information is essential for understanding the clinical decisions that were made and to audit the quality of care provided.

Where a patient feels that information recorded within their health record is incorrect, they must firstly contact the Health Records Access Team, who will raise the concern with the Healthcare Professional in charge of their care. Where both the Healthcare Professional and the patient agree that the information is factually inaccurate, it must be amended to clearly display the correction whilst ensuring that the original information is still legible. An explanation for the correction must also be added.

Where the health professional and patient disagree about the accuracy of the entry, the patient must be allowed to include a statement within their record to the effect that they disagree with the content. The Health Records Access Team will upload statements to Clinical Web Portal as required.

Where the information in question has been shared with other data processors, each recipient must be contacted to inform them of the rectification, unless this

proves impossible or involves disproportionate effort. If asked to, the Trust must also inform the patients about these recipients.

Where information is factually accurate, but the patient is dissatisfied with the information that has been recorded, the Directorate are responsible for providing an adequate response to the patient, as this will be treated as a complaint and not a true 'right to rectification' request. The Health Records Access Team will identify which Directorates must be involved in a coordinating this unified response.

9.0 Right to Restrict Processing

Patients are entitled to request the restriction or suppression of the processing of their information. This means that the record cannot be processed in any way while the restriction is in place (which could be permanently). This right sits closely to the right to rectification. When processing is restricted, the personal data can still be stored, but cannot be further used. Individuals should be aware that their health record cannot be entirely restricted as it needs to be made available to clinicians for their continuing care and treatment.

To prevent the further processing of factually incorrect information, and in line with the minimisation principle of GDPR, it may be agreed by the Data Protection Officer (DPO) for the data to be removed from Clinical Web Portal and/or manual health record, and a single copy be held centrally by the Health Records Access Team in line with Attachment 8: Retention, Appraisal, Disposal and Destruction.

Where an applicant has made a request to rectify the processing of their data, then the individual may have a right to restrict processing whilst these rights are being assessed, so both rights should be considered at the same time. As a matter of good practice, the Health Records Access Team may automatically restrict the processing of records whilst considering its accuracy or the legitimate grounds for processing the personal data in question.

The right to restrict is not an absolute right and could apply in the following circumstances:

- the individual contests the accuracy of their personal data and the accuracy is being verified by the Trust
- the personal data is no longer needed in line with retention but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data and you are considering whether your lawful basis for processing override those of the individual.
- the data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead

10.0 RSTR 'Restriction' Flag

When a Right to Rectification or a Right to Restriction is received, the right to restrict processing is automatically applied. Both rights are identified and highlighted by the Health Records Access Team when the request is received, via a flagging system on Clinical Web Portal (CWP) via the Patient Administration System

(PAS). RSTR is an abbreviation for restriction. If you see a 'RSTR' risk flag on a patient record then please contact the Health Records Access Team for more information before processing that record or acting on the information contained within it.

- Any 'Right to Restrict' requests received must be flagged by the Health Records Access Team on the above systems within 2 working days of receiving the request.

- An email and follow up telephone call must then be made to all Consultants/Healthcare Professionals involved in any current case or upcoming appointments, to make them aware of the restriction and what this means in terms of processing of the patient's information.

- Upon completion of the request, the restriction must be reviewed and removed where applicable (dependent on the outcome of the application of other individual rights).

11.0 Right to Erasure

The right to erasure is also known as the 'right to be forgotten'. It introduces a right for individuals to have personal data erased. A request for erasure can be made verbally or in writing, therefore processes should be put in place to ensure both types of request can be logged and monitored. The right to erasure is not an absolute right and should only apply in the following circumstances:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed
- consent was the lawful basis for holding the data, and the individual withdraws their consent
- 'legitimate interests' was the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- the data is processed for direct marketing purposes and the individual objects to that processing
- the personal data has been processed unlawfully (i.e. in breach of the lawfulness requirement of the first principle of the GDPR)
- to comply with a legal obligation

Directorates should identify any data processing activities where the above circumstances may apply and ensure there is a system in place to process a patient's 'right to erasure' request. This must also include any third parties processing data on our behalf. More information can be found in OP13 Information Governance Policy (xrwh.nhs.uk)

12.0 Right to Data Portability

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. The process should allow for moving, copying or transfer of personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability is not an absolute right and only applies when:

- processing is based on the individual's consent or
- for the performance of a contract and
- when processing is carried out by automated means

Therefore, for care purposes, where data is processed under a statutory legal basis, the right to data portability would not apply. However, where data is processed under the performance of a contract, with the individuals consent or the processing involves automated means, this right should be facilitated.

Directorates should identify any data processing activities where the above circumstances may apply and ensure there is a system in place to process a patient's 'right to Data Portability'. This must also include any third parties processing data on our behalf. More information can be found in OP13 Information Governance Policy (xrwh.nhs.uk).

13.0 Right to Object

The right to object only applies to information held where consent has been used as the legal basis for processing. The right to object means that data should cease to be processed. Individuals have the right to object to processing of their data where:

- Processing is based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); see Attachment 1 for legal basis for processing).
- It is used for direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics (this does not include statutory reporting).

Directorates should identify any data processing activities where the above circumstances may apply and ensure there is a system in place to process a patient's 'right to object'. This must also include any third parties processing data on our behalf. More information can be found in OP13 Information Governance Policy (xrwh.nhs.uk).

14.0 Rights in relation to automated decision making and profiling

The GDPR introduces a new right for individuals to not be subject to automated decision making and profiling. This is the process of making a decision solely by automated means without any human involvement, usually via a computer algorithm or formula. Profiling is automated processing of personal data to evaluate certain things about an individual. Profiling can also be part of an automated decision-making process.

An example of this in a healthcare setting may be a referral system which automatically prioritises patients as urgent or routine based on a standard set of information or uses pre-programmed algorithms to accept or decline patient referrals.

Directorates must identify whether any of these techniques are being used, either by the Trust (Data Controller) or by third parties on our behalf (Data Processor), and if so, the following guidance must be followed:

- Ensure there is a lawful basis to carry out profiling and/or automated decision making and document this on the Directorate's Information Asset Register
- Send patients a link to the Directorate's privacy statement, especially where we have obtained their data indirectly
- Explain to your patients how they can access details of the information used to create their profile
- Tell patients how they can object to profiling (including profiling for marketing purposes)
- Have additional checks in place for profiling/automated decision-making systems to protect any vulnerable groups (including children)
- Have a procedure in place for patients to access their personal data input into the profiles so they can review and edit for any accuracy issues.
- Only collect the minimum amount of data needed and have a clear retention policy for the profiles created, and where possible use anonymised or pseudonymised data for profiling activities

Directorates should identify any data processing activities where the above circumstances may apply and ensure there is a system in place to process a patient's 'right to object'. This must also include any third parties processing data on our behalf. More information can be found in Attachment 1.

For further information about automated decision making and profiling please contact Jane Lawrence, Head of Information, email jaynelawrence1@nhs.net or call ext. 88463.

15.0 Manifestly Unfounded Requests

The Trust can refuse to comply with a request if it is deemed to be manifestly unfounded. The Trust's definition of manifestly unfounded is "the unjustified, inappropriate or improper use of a formal procedure". A request may be manifestly unfounded if:

- the individual clearly has no intention to exercise their right of access. For example an individual makes a request but then offers to withdraw it in return for some form of benefit from the Trust; or
- the request is malicious in intent and is being used to harass an organisation with no real purposes other than to cause disruption. For example, the individual has explicitly stated, in the request itself or in other communications, that they intend to cause disruption; or
- the request makes unsubstantiated accusations against the Trust or specific employees; or
- the individual is targeting a particular employee against whom they have some personal grudge; or
- the individual systematically sends different requests to you as part of a campaign, e.g., once a week, with the intention of causing disruption.

This is not a simple tick list exercise that automatically means a request is manifestly unfounded. The Trust must consider a request in the context in which it is made, and the Trust is responsible for demonstrating that the request it is manifestly unfounded.

Understanding whether a request is vexatious or manifestly unfounded, and how we then manage the request, is determined on a case-by-case basis by the Health Records Management Team. Any extremely complex request or concerns raised around a particular request will be reviewed by the Head of Health Records Services.

16.0 Excessive Requests

The Trust can refuse to comply with a request if it is deemed to be excessive. A request may be excessive if it repeats the substance of previous requests and a reasonable interval has not elapsed, or it overlaps with other requests. However, it depends on the circumstances. It will not necessarily be excessive just because the individual:

- requested a large amount of information (even if you find the request burdensome)
- wanted to receive a further copy of information they have requested previously.
- made an overlapping request relating to a completely separate set of information
- previously submitted requests which have been manifestly unfounded or excessive.

When deciding whether a reasonable interval has elapsed between requests for information, the Health Records Access Team consider:

- the nature of the data – this could include whether it is particularly sensitive
- the purposes of the processing – these could include whether the processing is likely to cause harm to the requester if disclosed; and
- how often the data is altered – if information is unlikely to have changed between requests, you may decide you do not need to respond to the same request twice. However, if the Trust has deleted or changed information since the last request, we must inform the individual of this

17.0 What should we do if we refuse to comply with a request?

You must inform the individual without undue delay and within one month of receipt of the request. The Health Records Access Team will inform the individual about:

- the reasons you are not taking action
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

The Trust cannot presume that a request is manifestly unfounded or excessive on the basis that the individual has previously submitted requests which have been deemed to be manifestly unfounded or excessive.

18.0 Complaint and Appeal Process

If the patient is unhappy with the outcome of their request or the way in which their rights have been applied the patient must be advised to follow the following appeal procedure:

- All complaints and appeals must be escalated to Health Records Manager for initial review, further action, and response to the requestor in writing.

- If the requestor remains unhappy with the way in which their rights have been applied, this should be escalated to the Head of Health Records Services for a full and final response to the requestor in writing, addressing their concerns and advising them of their right to complain to the Data Protection Officer (DPO) and the Information Commissioners Office (ICO). This should be done within 30 working days of receiving the escalated complaint, in line with the Trust's complaint management policy.

- Data Protection Officer (DPO) will conduct a full review of the entire process and understand what has been disclosed, withheld, correspondence sent and received, and a timeline of events. She will make recommendations at this point. The DPO will advise of timescales for response at this stage.

- The patient always has the right to complain to the Information Commissioners Officer (ICO) at any stage of the process, but the expectation will be that the patient has exhausted our internal process before they investigate further.

Complaints outside of the Subjects Rights process will be managed in line with the Trust's complaint procedure.

19.0 Requests that fall outside the Health Records Access Team Remit

Sometimes requests are received that have several elements, though they may present as a subject access request, but may also contain concerns around clinical quality and care. It is vital that a coordinated response is provided to the requestor. The Health Records Access Team will work with Directorates and the Patient Advice and Liaison Service in order to facilitate a coordinated response.

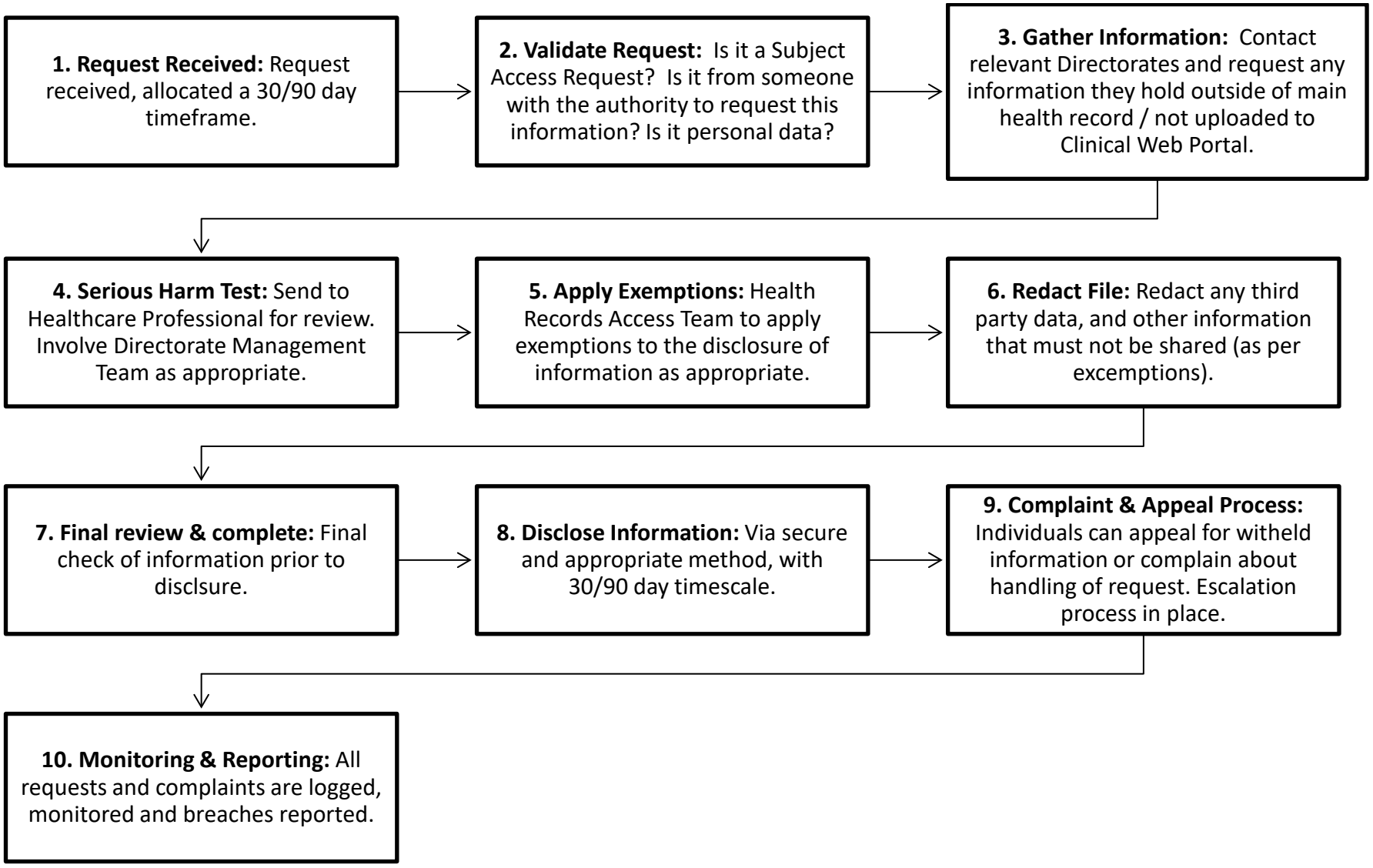
20.0 Destruction of Patient Information Request Documentation

In line with national guidance, requests and disclosure correspondence will be reviewed and destroyed 3 years post disclosure if no longer needed. Where there has been a subsequent appeal following disclosure, all correspondence will be kept for 6 years, reviewed, and destroyed if no longer required. All other patient data is held in line with the Attachment 8: Retention, Appraisal and Destruction

21.0 Further Information

For further information about requests for patient information please contact the Health Records Access Team, Health Records Library, Location B19, McHale Centre, New Cross Hospital. Telephone 01902 307999 ext. 85544 / 85545 or 88093 or email: rwh-tr.healthrecordsaccess@nhs.net

22.0 Table 1: Subject Rights Request Journey



Subject Rights Request Form

Requesting copies of personal information processed by The Royal Wolverhampton NHS Trust.

This form can be completed and returned in the post, via email or completed over the telephone with a member of the Health Records Access Team. For help completing this form please call the team on 01902 695544, 695545 or 01902 307999 ext.88093.

In line with data protection legislation, you can expect to receive your requested information within 30 days. Where requests are complex or numerous, this may be increased to 90 days. You will be sent an acknowledgement letter on receipt of your request which will detail the appropriate timeframe. There will be no charge for accessing your health records (however we can charge a reasonable administrative fee should your request be repetitive).

SECTION 1: Patient details (the data subject)

Full name of patient			
Title (please circle)	Mr/Mrs/Miss/Ms/Dr/Other	Date of Birth	
Previous / other name(s)			
Hospital/NHS Number	(if known)		
Current Address			
Previous Address(es) (use separate sheet if necessary)			
Telephone Number			
Email Address			

SECTION 2: Details of the information that you are requesting

If you require a particular section of your Health Record, please give details:

Period of Disclosure	From / To, or a specific episode of care	
Department(s)/Speciality	If applicable / if known	
Consultant(s)	If applicable / if known	

Routine Requests
If you require all health records, the following information will be routinely supplied as part of your Subject Access Request (unless you have indicated that only certain information is required above). This will be processed within 30 days of receiving your request and Identification documents.

- Emergency Department Records (A&E record card)
- Urgent Care Centre Records*
- Minor Injuries Unit (MIU) records at Cannock Chase Hospital
- Scanned health records (electronically stored on our Clinical Web Portal system)
- The main physical health record (paper records)
- Microfilmed (archived) records
- Radiology images i.e. X-rays, scans and reports
- Clinical Images (Medical Photography)
- Pathology (blood tests etc.)
- Observation recordings (via a system called Vitalpac)
- Prescription summary report
- Maternity Services
- Physiotherapy Records

**Prior to 1st April 2021 the Urgent Care Centre at New Cross Hospital (above the Emergency Department) was not part of the Trust and was provided by Vocare. Requests for Vocare records must be sent directly to* wm.governance@nhs.net

Complex Requests
We do not automatically include the following information as it is held on separate systems that we do not have immediate access to. Please tick which records you require (if any). Please note that the law allows us additional time to process complex and/or numerous requests, so may take us up to 90 days to process, dependent on the number of department/specialities involved.

- ❑ Full Electronic Prescribing and Medicines Administration System (ePMA) records
- ❑ Information held separately by Individual departments/specialities
- ❑ Paediatric Community Services inc. health visiting and school nursing service
- ❑ Audit trails (of which staff have accessed your electronic record)
- ❑ Datix Risk and Incident Management System
- ❑ Wolverhampton Special Care Dental Service
- ❑ Sexual Health Services (The Fowler Centre)
- ❑ The Maltings Mobility Service (prosthetic and wheelchair services)
- ❑ Foot Health Services
- ❑ The Phoenix Walk-In Centre

Primary Care Services
The following GP Practices are part of the Royal Wolverhampton NHS Trust. Please tick your surgery below IF you would like a copy of your GP records.

❑ Alfred Squire Road Health Centre ❑ Coalway Road Surgery

❑ Lea Road Medical Practice ❑ Oxley Surgery ❑ Penn Manor Medical Centre

❑ Thornley Street Surgery ❑ Warstones Health Centre ❑ West Park Surgery

SECTION 3: Who is requesting this information?

☐	I am requesting my own information.
☐	I am the parent/legal guardian of the patient and have responsibility for the patient who is under the age of 13 years old (formal evidence of this responsibility may be required)
☐	I have been asked to act on behalf of the patient (attach the patient's written authorisation)
☐	The patient is unable to make this request, and I am appointed by the Court to manage this on their behalf (attach confirmation of appointment)

SECTION 4: Details of requestor (only complete this section if you are not the patient)

Full name of requestor	
Relationship to patient	
Current Address	
Telephone Number	
Email Address	

SECTION 5: Please indicate how you wish to receive the records

☐	I wish to make an appointment to view the requested records with a member of Health Records Services (no medical information will be discussed at this session)
☐	I wish to collect copies of the records (ID will be required on collection)
☐	Please send me copies of the records by recorded delivery
☐	I would prefer to receive the records via secure email (where possible)

SECTION 6: Rectification and/or Restriction of Inaccurate Data

If any of the information supplied by the Trust is found to be factually inaccurate or incomplete, the patient has the right to have this information rectified. If this is the case, then please let the Health Records Access Team know. The information will then be reviewed (alongside the appropriate Healthcare Professionals) and amended as required. The timescale involved for completing this type of request is the statutory 30- or 90-day deadline as described above.

SECTION 7: Declaration

It is a criminal offence to unlawfully obtain or attempt to obtain data.

We require proof of your identity before we can disclose any personal information. You will need to provide copies of two documents, such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The documents should include your full name and current address. If you have changed your name, please supply relevant documents evidencing the change**.**

A) Requesting Your Own Record's
I am applying to access health records held by The Royal Wolverhampton NHS Trust (RWT). I certify that to the best of my knowledge the information provided on this form is correct, and that I am the person to whom it relates. I understand that RWT is obliged to confirm proof of identity and it may be necessary to obtain further information in order to exercise my right of access.

Sign: …… Print: …… Date: ……

I have enclosed <u>two</u> types of identity with this form one Photo and one address (please tick):

❑ Birth Certificate (For Child Application)
❑ Passport
❑ Driving Licence
❑ Official letter to my address

B) Requesting Someone Else's Records
I, the requester, apply for access to the health records of the above-named patient, under the General Data Protection Regulation (GDPR) Right of Access. I certify that to the best of my knowledge the information provided on this form is correct and that **I am legally authorised to act on behalf of the patient**. I understand that RWT is obliged to confirm proof of authority and it may be necessary to obtain further information in order to comply with this subject access request.

Sign: …… Print: …… Date: ……

Proof(s) of legal authorisation enclosed with form (please tick)

❑ Letter of authority from patient ❑ Lasting or Enduring Power of Attorney (Health and Welfare)

❑ Evidence of Parental Responsibility ❑ Other - please state: ……

Please return completed form to: The Health Records Access Team c/o The Health Records Library, Location B19, McHale Centre, New Cross Hospital, Wolverhampton, WV10 0QP or send via email to rwh-tr.healthrecordsaccess@nhs.net or telephone 01902 695544, 695545 or 01902 307999 ext.88093 for assistance.

Application Form: Access to Health Records

Access to the health records of a deceased person is governed by the Access to Health Records Act (1990). Under this legislation when a patient has died, only their personal representative, executor or administrator of their will, or anyone having a claim resulting from the death (this could be a relative or another person), has the right to apply for access to the deceased's health records.

The Royal Wolverhampton NHS Trust determines a health record to include "any material created as part of the care and treatment of a patient. Such materials can be in any format, and be contained within the paper health record or attached to the electronic record (referred to as Clinical Web Portal).

Please consider the following information before completing this application form:

- If you are the executor/administrator or the personal representative of a deceased person you will need to provide documentary evidence of this.
- To make an application, you must provide evidence of your identity. This must include one form of personal photographic ID and one form of proof of address. Further information of what forms of identification can be accepted is given within the application form.
- If you are making the application on behalf of a patient, as their legal representative (e.g. you are a solicitor or insurance company), you must provide written authorisation from the applicant to act on their behalf and explicit permission to obtain a copy of their medical record.
- Applicants who may have a claim arising out of a patient's death have a right of access to information in the deceased patients record directly relevant to the claim. We will provide those parts of the medical record relevant to your request. We may request additional information to support your application if the information provided is insufficient.
- Incomplete applications will be returned, with correspondence stating what further information would be required for the application to be considered.
- Once your completed application form, together with your ID and any documents in support of your request are received, your application will be deemed to be valid.
- We are then required to provide you with the relevant information within 40 days.

Please note that there are certain circumstances in which the Trust may deny access to the complete record or to certain parts of the record. These are:

- If parts of the record are not within the scope of the request.
- Where an individual other than the patient (and appropriate health professionals) could be identified from the information. This is known as third party data.
- The deceased patient stated they did not wish for any part of their records to be released after death, or the information contained within the records was such that the deceased person expected them to remain confidential.
- Where records have been destroyed in line with the Trust's retention policy.

1. PATIENTS DETAILS

Surname	
Forename(s)	
Previous / other names	
Date of Birth	
NHS Number (If known)	
Date of Death (If known)	
Address and postcode	

2. APPLICANT DETAILS (Solicitors etc must insert their client's details below)

Surname	
Forename(s)	
Address and postcode	
Telephone number	
Contact email	
Relationship to patient	

3. REQUEST DETAIL

3.1 Information required: Please give details about the information you require.

3.2 Reason for access: Please explain why you wish to access these records (this will help us to clarify the scope of your request)

3.3 Period of disclosure: Dates or particular episodes of care required

4. AUTHORISING A SOLICITOR/AGENT/INSURANCE COMPANY (IF APPLICABLE)

I have appointed the following company to act upon my behalf:

……

I understand that filling in this section gives the Royal Wolverhampton NHS Trust permission to disclose copies of the medical records to the company detailed above. Please provide the company identified above copies of the health record in line with the Access to Health Records Act 1990 within 40 days.

Your Signature: ……

5. DECLARATION BY APPLICANT

I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health record referred to under the provisions of the Access to Health Records Act 1990.

a) ☐ I am the deceased patient's personal representative and attach a copy of confirmation of my appointment (Grant of Probate, Letter of Administration, Certified Copy of the Last Will & Testament) OR I or can provide sufficient information to support my application and evidence that I have authority to act on the patient's behalf.

b) ☐ I have a claim arising from the patient's death. Please provide comprehensive details to support your claim.

I understand it is a criminal offence to unlawfully obtain or attempt to obtain data.

Print Your Name: ……

Your Signature: ……

Date: ……

6. Consent to email your completed request via secure email

Where possible we try to send records via secure email. Please confirm if you happy for us to do this and specify the email address that the records should be sent to.

☐ Yes, I am happy to receive the outcome of my request via email to the below email address.

☐ No, I wish for the records to be sent via recorded delivery as a paper copy.

Email Address: ……

Please send your completed application form, copies of relevant identification and any supporting documentation to the **Health Records Access Team c/o The Health Records Library, Location B19, The McHale Centre, New Cross Hospital, Wolverhampton, West Midlands, WV10 0QP** or via email to rwh-tr.healthrecordsaccess@nhs.net.

For help completing this form please call the team on 01902 695544 / 695545. Any information you provide will be treated in confidence. It will only be used for the purpose of processing your request in accordance with the Access to Health Records Act 1990. After your request is completed, your information will be retained for the statutory time period (currently 3 years), after which it will be securely destroyed.

Attachment 5: Health Records Audit and Monitoring

Contents

Procedure Statement

This procedure details all of the audits undertaken by Health Records Services to audit and monitor compliance against the OP07 Policy and provide assurance that the General Data Protection Regulation (GDPR) statutory requirements are being adhered to across the Trust in terms of the provision and use of Health Records.

Document 1: Access to Merge Facility Audit

1.1 Purpose

The merge facility is not routinely provided to all staff. This function is released following merge training with the Patient Administration System (PAS) Training Team, and approval by the Head of Health Records Services. The function allows staff to merge volumes (of records) electronically (on PAS) to reduce duplicate registrations.

1.2 Aim

The aim of this audit is to identify those accounts that have been granted access but are not using this function. This is because Health Records Services limit the number of staff who are able to merge volumes (of records) electronically to reduce the likelihood of error by staff who are not regularly using the system. Irregular users will have their access reviewed and removed if appropriate.

1.3 Standards

The expectation is that staff members access the merge facility at least once in a six-month period.

1.4 Method

PAS Administration Team provides the Head of Health Records with a bi-annual report detailing the utilisation of the merge facility. This is released to the Deputy Health Records Managers (who Chair the Merges and Duplicates Group), who review the report and send out to the group members prior to their next meeting.

The audit is conducted every six months (bi-annual).

1.5 Results and Actions

Results are reported to the Merges and Duplicates Group meeting quarterly for discussion and minuting. Removals are discussed and agreed and sent on to the Head of Health Records Services for approval. Individuals identified that require their access removed are then reported to the PAS team in ICT Services for removal. Audit results will be reported to the Health Records Project Group on a quarterly basis

Document 2: Tracking & Tracing Audit - Inpatient Episode 'Skinny File' Journey

2.1 Purpose

The location of Health Records must be traceable at all times. Staff who transfer Health Records are responsible for ensuring the new location is accurately entered onto PAS. It must state the exact location and extension number of the person to where the notes are being forwarded to.

2.2 Aim

This audit follows the journey of an inpatient episode, and measures whether the 'skinny file' is created and tracked on PAS correctly throughout the patient's stay. By auditing whether records are correctly tracked to their location we aim to provide assurance that the correct tracking process is adhered to across the Trust, and to identify any areas of non-compliance or good practice, and ultimately reduce the number of missing records and therefore any clinical risk to the patient.

2.3 Standards

Records must be 'tracked' on PAS to their current location on entry to that department /area. It is the responsibility of both the sender and the receiver to do this as a priority. 'Tracking' is logging the exact location of the paper record on the Patient Administration System (PAS).

2.4 Method

This audit will be undertaken by Health Records Services. The Case Note Tracking (CNT) module of PAS will be audited bi-monthly, using a random selection of 20 patient records per audit. The patient history will be cross referenced to the tracking module to ensure they match. This is to identify whether there has been a failure to track the record at any point during the patient's stay.

2.5 Local Audit Log

A basic audit log sheet is completed when identifying which patient journey will be audited. This is so that the final audit results can be pseudonymised (by only using the audit number indicated in any future reporting). To maintain patient confidentiality, the log sheet and the results template should not be stored together.

Audit Date	Ref No	Hospital Number	Patient Initials	Audited By
	1			
	2			
	3			

2.6 Audit Results Template –Inpatient Episode 'Skinny File' Journey

Date of Audit: Auditor By:

Ref No	CNT checked: Yes/No/Reason	Exact location and Ext number recorded on CNT: Yes/No/Reason	PAS & CNT match ward transfers for inpatient stay: Yes/No/Reason	CNT completed by transferring ward: Yes/No/Reason	CNT completed by receiving ward: Yes/No/Reason	Comments / Actions Required
1						
2						
3						

2.7 Results and Actions

Collation of results will be undertaken by the Health Records Services Management Team and then reported to the Head of Health Records Services for discussion Audit results will be reported to the Health Records Project Group on a quarterly basis including trends analysis, and any agreed actions

Any inaccuracies are emailed to the relevant manager of the department for feedback to relevant staff, to avoid any future inaccuracies.

Document 3: Tracking & Tracing – Manual Health Records Audit

3.1 Purpose

The location of Health Records must be traceable at all times. Staff who transfer manual health records are responsible for ensuring the new location is accurately recorded on the approved system. It must state the exact location and extension number of the person to whom the notes are being forwarded.

3.2 Aim

This audit establishes whether the manual health record is correctly tracked to its current location. By auditing whether records are correctly tracked to their location we aim to provide assurance that the correct tracking process is adhered to across the Trust, and to identify any areas of non-compliance or good practice, and ultimately reduce the number of missing records and therefore any clinical risk to the patient.

3.3 Standards

Records must be 'tracked' on the approved system ie PAS, tracer cards, booking in book, locally held records management system etc, to their current location. It is the responsibility of both the sender and the receiver to do this as a priority.

3.4 Method

Audit undertaken by all areas that hold manual health records, specifically;

- Health Records Library
- Ophthalmology
- Paediatrics Acute

The audit will be undertaken on a bi-monthly basis, with areas that hold manual records randomly selecting 10 patients per location. This is to identify whether there has been a failure to track the record to its current location and identify any missing records.

3.5 Local Audit Log

A basic audit log sheet is completed when identifying which patient journey will be audited. This is so that the final audit results can be pseudonymised. To maintain patient confidentiality, the log sheet and the results template should not be stored together.

Audit Date	No	Hospital Number	Patient Initials	Audited By

3.6 Audit Results Template – Locally Held Manual Records

To be returned to Health Records Services Manager (Bi-Monthly)

Date of Audit: Auditor By:
Directorate/Service: Tracking System:

Ref No	Exact Location of Manual Record Selected	Did location on tracking system match?	Comments / Actions Required

3.7 Results and Actions

Collation of results will be undertaken by the local area and sent to the Health Record Services Manager. Results will then be reported to the Head of Health Records Services for discussion. Audit results will be reported to the Health Records Project Group on a quarterly basis
including trend analysis, and any agreed actions

Any inaccuracies are emailed to the relevant manager of the department for feedback to relevant staff, to avoid any future inaccuracies.

Document 4: Physical Access to the Health Records Library

4.1 Purpose

The purpose of this audit is to ensure that only authorised personnel have access to the Health Records Library.

4.2 Aim

The aim of restricting access to the Library is to provide a secure environment for patient records. The aim of the audit is to provide assurance that access is given to authorised personnel only and that 'leavers' are removed from the authorised access list.

4.3 Standards

The authorised access list is expected to include current Health Records Library, Scanning Bureau, Health Records Access Team, Patient Administration & GP Correspondence Team, specific Porters and specific Hotel Services staff, and the ICT Senior Management Team.

4.4 Method

Audit will be undertaken by Health Records Services Management Team. A report is generated on request by the Security Management Team. This audit is undertaken quarterly. All staff included on the report will have their access reviewed, and if no longer required or appropriate it will be reported to the Head of Health Records Services.

Access may be removed if the staff member has changed roles, has left the Trust, and has not accessed the department for several months.

4.5 Results and Actions

Any staff that should no longer have access to the department will be removed immediately by reporting those individuals to ID Card Services. Audit results will be reported to the Health Records Project Group on a quarterly basis

Document 5: Legitimate Access Audit

5.1 Purpose

The Trust is required to monitor staff access to patient records to ensure their legitimacy. The purpose of the audit is to provide assurance that staff access to health records systems is legitimate. Clinical Web Portal (CWP) and Patient Administration System (PAS) audits will be conducted by Health Records Services Management Team.

Information Asset Owners must adopt a similar local audit process to provide assurances for access to their information assets, in line with the below.

5.2 Aim

We aim to provide data to line managers to identify where access to health records has taken place, whether or not that access was legitimate, and subsequently identify trends of inappropriate behaviours, where immediate actions and/or staff training may be required.

5.3 Standards

Standards are as per the Confidentiality Code of Conduct. Staff must not access their own Health Records or those of their family and friends.

5.4 Method

4 recent inpatients are selected at random every quarter by Health Records Services Management Team, and an audit trail is requested from Software Services (ICT), detailing the access to said records via Clinical Web Portal (CWP) and the Patient Administration System (PAS) and EMIS.

Health Records Services Management Team then split the audit results by the staff member accessing the patient's electronic records, and an email detailing their access is sent to their Line Manager, and request they confirm that the access was necessary and part of the staff member's duties.

5.5 Results and Actions

Any anomalies or breach of policy will be reported on Datix (risk and incident management system) and escalated to the Data Security and Protection Team for further investigation. The staff member's Head of Department and Human Resources will be informed of the breach of policy where appropriate. Audit results will be reported to the Health Records Project Group on a quarterly basis

Document 6: Subject Rights Requests Compliance Audit

6.1 Purpose

The purpose of this audit is to provide assurance that Subject Rights Requests received by the Trust from or on behalf of patients, are being processed in line with the GDPR statutory guidance and timeframes.

6.2 Aim

The aim of the audit is to identify any areas of poor compliance within the Health Records Access Team and implement actions to address any concerns raised. The audit also aims to highlight areas of good practice and any barriers preventing timely and comprehensive compliance, sharing any lessons learned with colleagues as appropriate.

6.3 Standards

We will audit the processing of Subject Rights Requests against the regulations and statutory timeframes set out by the General Data Protection regulation (GDPR), including but not limited to:

- Completed within the 30 / 90 day timeframe
- If the request was extended to 90 days, was it correctly identified as complex?
- Completed free of charge, if not was there a valid reason
- Was the request acknowledged in an acceptable time frame (5 days)
- What were the barriers for completing the request on time and/or in full
- Were any complaints or appeals correctly managed and in line with policy timeframes
- Were any requests escalated to the Data Protection Officer (DPO) and if so were there any lessons learnt / actions to be implemented
- Were any requests escalated to the Information Commissioner's Office (ICO) and if so were there any lessons learnt / actions to be implemented

6.4 Method

This audit will be conducted bi-monthly by the Health Records Services Management Team, using the Health Records Access Team's Request Database. A 5% sample will be audited, and will be undertaken quarterly (currently equating to approximately 175 of the 3500 requests received per annum).

6.5 Results and Actions

Audit results will be reported to the Health Records Project Group on a quarterly basis. Any areas of non-compliance will be reviewed by the Head of Health Records Services and the Health Records Manager to agree SMART actions to be implemented to ensure all statutory standards and timeframes are met.

Document 7: Missing Records Audit

7.1 Purpose

Health Records Services hold a central missing records log which contains manual records (main records and skinny files) that have been reported as missing and marked accordingly on the PAS system.

7.2 Aim

The aim of this audit is to identify if the manual records within the central missing records log have been found. The audit will aim to continually investigate missing records on a monthly basis that have been reported to the Health Records Service as missing.

7.3 Standards

Health Records Management Team will audit the central missing records log and identify if each record has been found against the PAS system. If found the log will be updated accordingly. If the records are still showing as missing on the PAS system then a further investigation will be made in the attempts to find the record and the log will be updated with actions taken.

7.4 Method

This audit will be conducted monthly by the Health Records Services Management Team and reported to the Head of Health Records Services and the Health Records Services Manager

7.5 Results and Actions

Audit results will be reported to the Health Records Project Group on a quarterly basis. Update the Datix (Risk Management System) to show that the record has since been found.

Document 8: Generic Record Keeping Standards Audit

Generic Record Keeping Standards - Inpatient Paper Record 'Skinny File' Audit Tool

8.1 Purpose

OP07 Attachment 2, Section 7 (Records Keeping Standards) sets the Trust's standards for general medical record keeping. The purpose of these standards are to maximise patient safety and quality of care; support professional best practice; assist compliance with Information Governance, Principle 4 (accuracy) of the General Data Protection Regulation and NHS Litigation Authority (CNST) Standards. These generic medical record keeping standards are applicable to every patient's medical record.

8.2 Aim

The Trust is required to audit the accuracy and quality of their health records. The record keeping standards set out in Attachment 2 have been reflected in the audit tool below. Auditing these standards will provide Health Records Project Group with assurance that these standards are being met within the Inpatient areas that still create paper records. These are known as skinny files; containing the patients current episode of care. On discharge the folders are sent to the Scanning Bureau for scanning to Clinical Web Portal.

8.3 Method

This audit will be conducted monthly and reported quarterly by the Health Records Services Management Team. 10 skinny files will be selected from a different specialty each month. Ward areas will be selected based on the number of health records and/or data quality incidents reported for that area via Datix.

Once the audit has been completed the data will be inputted to a locally held spreadsheet. A note of the database ID will be made on each pro-forma, which will then be scanned to a protected shared drive. Any paper proformas will be will then be shredded.

8.4 Exclusions and Exemptions

Some Directorates will be excluded from this audit as they do not hold patient records, for example Pathology, Patient Services and Pharmacy. Primary Care Services are also excluded from this audit. Directorates who operate a fully electronic system (i.e. electronic at point of care and no paper is generated), and whereby the required standards are met by mandatory fields within said system, are also exempt from participation in this audit. Directorates who are currently exempt on this basis are:

- Radiology
- Audiology (Inpatient and Outpatient)
- Community Paediatrics
- Special Care Dental Services (Inpatient and Outpatient)
- Tissue Viability (Inpatient and Outpatient)
- Obstetrics (Inpatient and Outpatient)
- Audiology

8.5 Measurement of Compliance

A figure of 75% has been agreed by the Trust as a threshold for compliance.

Red 0%-50%	Amber 51%-74%	Green 75%-100%

8.6 Feedback to Specialties

Health Records Services Managers will present quarterly reports to the Health Records Project Group, and ensure SMART actions are agreed to address any areas of low compliance. Directorates audited will be provided with the audit findings for local discussion and actions to be agreed at their Directorate Governance Meeting. Local action plans to be monitored by the Directorate and reported back to the Health Records Project Group.

Generic Record Keeping Standards - Inpatient Paper Record 'Skinny File' Audit Tool

Patient ID:	Consultant:	Speciality:
Ward:	Date of Audit:	Auditor:

	Yes	No	N/A
Q1) Does every page for paper records or every entry for electronic records of the current attendance/admission include the patient's full name?			
Q2) Does every page for paper records or every entry for electronic records of the current attendance/admission include the patient's Hospital number?			
Q3) Does the Documentation reflect the continuum of patient care and is viewable in chronological order for the current attendance/admission?			
Q4a) For inpatient admissions, is there an entry in the Health Record whenever a patient is seen by a clinician 1 day for medical care (or) 7 days for long stay continuing care?			
Q4b) If 'no' does the next entry within the record explain reason why?			
Q5) Are all entries dated?			
Q6) Are all entries timed using 24 hour clock, where applicable?			
Q7) Are all entries legible?			
Q8) Are all entries signed?			
Q9) Do all entries have the health professional name printed or stamped?			
Q10) Do all entries have the health professional ID number printed or stamped?			
Q11) Do all entries include the health professional designation printed or stamped?			
Q12) Are all deletions and alterations signed?			
Q13) Are extra information sheets (e.g. blood gases, ECG traces etc.) on separate pages? (i.e. not covering / obstructing other information)			
Q14) Are all pharmacy notes in green ink (except aseptics/chemotherapy in red ink)			
Q15) Are operation notes recorded on the specific 'operation note' proforma?			
Q16) Have all other entries been made in black ink?			
Q17) Was the health record in an acceptable condition? e.g. Was there any loose documentation? Was the folder torn or in poor condition?			
Q18) If viewing the records via Clinical Web Portal, is the documentation legible?			

NB: The use of a stamp will ensure compliance with the criterion Q9, Q10, & Q11. If no stamp is available, all these details must be clearly printed.

Attachment 6: Scanning and Inpatient Documentation Process

Contents

1.0 Procedure Statement

As the Trust adopts electronic ways of working, the scanning of patient records plays a vital part in recording and storing patient information in order to provide accessibility to clinical staff providing patient care.

Paper case notes are becoming less frequently used as more and more information is created and scanned electronically. Historic paper records are held within the health records library and can be made available on request.

When patient information is scanned, the main consideration is that the information can perform the same function as the paper record both for the care of the patient as well as the legal requirements it brings if challenged in court. It is therefore vital the scanned document maintains its integrity, authenticity and usability for the duration of the retention period, in the same way as the paper record.

This protocol sets out the necessary guidelines to assist all employees on the responsibilities and practices in place, in relation to the scanning process. This ensures that documents are scanned to a standard so that electronic images can be used as evidence in legal situations.

The trust aims to implement processes which will improve staff time in terms of accessibility to records, and to also reduce the amount of physical filing required.

This procedure must be followed when paper records are transferred on to an electronic system.

2.0 Document 1: Scanning of Health Records

2.1 What to Scan

Any physical documentation that would form part of the patient's health record needs to be scanned to the relevant system.

Any documents that can be created electronically in the first instance must be considered and completed electronically without physical duplication.

Duplicate documents must not be scanned if already in the health record. Once a document is scanned it should not be re-printed with the exception of the provision of records to outside agencies (If no electronic transfer method is available) or a subject access request.

2.2 How to Scan

2.2.1 Preparing Documents

Before scanning of a document can take place, the following actions must be carried out:

- The general condition of the document must be examined to ensure each page is in a good condition to process through the scanner without damage ie pages are not stuck together or damaged (if damaged the page may be photocopied on to a new page before being scanned)
- Any notes or post-it notes attached to the any document must be placed on a blank sheet of paper for scanning.
- Remove any staples or paperclips
- Ensure all pages are in chronological order.
- Ensure the front page has the following details:
    - Full Name
    - Date of Birth
    - NHS Number/unit number
- Any numbered blank pages within a record must not be removed and must be scanned in the order they appear within the original document.
- Remove any poly-pockets / plastic wallets
- Check that all the information in the document pertains to the same patient (NHS number, name and date of birth). If misfiled information is found it must be removed and relocated in the appropriate record. See point 2.6 (misfiled Documentation)

2.2.2 Scanning Equipment

All scanning must be carried out using a Trust approved machine and the following resolution settings

- Black and White images – 200 DPI (Dots per Inch)
- Coloured Images – 300 DPI
- Photographs – 300 DPI

2.2.3 Indexing

Document indexing (sometimes referred to as metadata) enables a user to quickly and efficiently locate documents, either through a folder structure, database or electronic document management system. Some areas within the Trust may index scanned documents in a different way depending on the different needs for information and the different systems used. However, all scanned documents must be scanned to a specific set of indexing/metadata.

2.2.4 Quality Control

The quality checking stage of a scanned image is essential and must be carried out at the end of the scanning process and as soon as the scanning has taken place. If this is not followed the document is not legally admissible and the original cannot be destroyed. This checking stage should be completed by a different member of staff that has scanned the document. To ensure all documents are scanned to a satisfactory quality, staff must ensure:

- Every piece of a document is scanned, including any numbered blank pages and double-sided documents.
- Any scanned document is unchanged from its original format.
- All aspects of the scanned document are legible.
- Pages should be positioned correctly and not at an angle or upside down.

The % of sample quality checking will depend on the service, level of risk and assurance. This should never fall below the British standards of 5%.

2.3 Legal Admissibility

Any scanned document will be managed in accordance with the attachment 8 Retention, Appraisal, Disposal and Destruction. The scanned copy will, for legal purposes, become the definitive record and will then be subject to correct records management and retention policies set in place for digital documentation.

Scanned documents are admissible in court but can differ depending on the court action. In criminal cases a certified scanned copy can be used *with* proper authentication including how it was scanned and notations declaring it unaltered. In civil action cases, scanned copies can be produced with the court deciding on the evidential weight issued to the document. These principles arise from the Civil Evidence Act 1995 and the Policy and Criminal Evidence Act 1984.

2.4 Misfiled Documentation

If when viewing an electronic patient record, an incorrect document relating to a different patient is found, you must contact the Health Records Scanning team on extension 88100/85540 or email rwh-tr.HealthRecordsIssues@nhs.net who will arrange for the file to be removed and rescanned into the correct patient file. Health Records will complete a Datix incident report against the department responsible for the error.

2.5 Security and Protection

- Records that contain personal identifiable data should only be scanned by staff who are authorised to handle the information.
- The scanned images must be immediately quality checked and stored within the correct system.

- The original document must be confidentially destroyed as soon as possible after storing the scanned document. The paper version must not be kept for the department needs. If you are unsure about destroying a document contact the Health Records Management Team for advice. There should never be two versions of a document.
- Scanning of records should take place in a secure environment where only authorised personnel have access.

2.6 Documentation Retention

All physical documentation should be kept until sufficient quality checks have been carried out on a scanned image. An appropriate quality check process and retention timeframe must be agreed locally, in alignment with the advice within this document.

A scanned document must be securely stored and correctly indexed before destroying a physical record.

Original Physical Documents can be destroyed once the scanned:

- image is securely stored
- document is correctly indexed
- document has been thoroughly quality checked to ensure the electronic version is a true and accurate copy of the original.

Once these checks have been carried out, the original document can now be destroyed confidentially. Confidential shredding bins are provided by the Trust, please refer to Attachment 8 Retention, Appraisal, Disposal and Destruction for more information.

3.0 Document 2: Current Process for Inpatient and Outpatient Documentation

The Scanning Bureau is based within the Health Records Library on the New Cross Hospital Site. Its main function is to scan patient documentation created as a result of an inpatient episode. Skinny files (clear plastic folders) have been introduced across ward areas in order to provide a process for the management of patient documentation during an Inpatient stay until the records are scanned onto the CWP following discharge.

On admission, a patient must have a skinny file created both physically and on PAS. For planned admissions, the file will be raised by the waiting list staff, and for emergencies and unplanned admissions the file will raised within the admissions unit.

3.1 Flow Chart for Inpatient Documentation

Patients admitted via elective or emergency admission

Step 1 - Create a skinny file folder with a front control sheet

Step 2 - Raise a SK (skinny file) volume on PAS (ensure correct ID SK label is used on the front of the control sheet)

Step 3 - Track SK volume on PAS to current location

Step 4 - Skinny file will be added to continuously throughout the inpatient stay

Step 5 - If skinny file moves location throughout the inpatient stay ensure tracking is updated accordingly on PAS

Step 6 - On patient discharge check skinny file is in the standard order for scanning

Step 7 - Check if there is any loose filing on the ward for the patient and interfile into skinny file

Step 8 - Place skinny file ready for collection by Clinical Coding or Scanning Team within 24 hours after discharge

Steps explained in more detail:
Step 1 & 2: When raising a paper skinny file (see Document 4 below) record the first document must be a front control sheet (Document 3) which must contain a patient SK ID label when raised on PAS so that it will provide a visible identification of the correct corresponding file for the patient on PAS. This will ensure that the correct volume is tracked accordingly on PAS when the skinny file moves location.

A new volume must be created on PAS using 'Create new Casenote'

The casenote number will be that of the patient hospital number followed by the suffix 'SK'

For example, if the main unit number is H123456, the skinny file number to be created for the inpatient stay would be H123456SK.Patient ID labels must then be generated with this number to be attached to the front control sheet

Whilst a patient remains on a ward, it is the responsibility of the ward manager to ensure processes are in place that a health records 'skinny file' is raised for each patient and an 'SK' number is created on PAS. The record must also be tracked on PAS so that the whereabouts of the record is known at any given time.

Step 3: Update PAS with the current location of the skinny and enter as much information in the field as possible e.g. extension number of location etc.

Step 4: The skinny file will follow the patient to record all clinical details during the inpatient stay. If a patient is transferred to another ward within the hospital or to West Park or Cannock Hospital, the skinny file must also transfer with the patient to ensure the continuity of care.

Step 5: It is essential that the tracking (see attachment 7 Document 2: Health Records Retrieval & Tracking) of the skinny file reflects the current location. It is the responsibility of both sender and recipient to check PAS and track accordingly

Step 6: Following discharge, the 'skinny file' must be checked by the ward clerk to ensure the standard order of the documents (Document 4) are in the correct order in readiness for scanning to take place. This comprises of 17 sections which will be book marked against when scanned to CWP.

Step 7: Any loose filing must be collated and interfiled into the patient's skinny file prior to collection for scanning. Additional documentation cannot be added to the original inpatient stay documentation after scanning has been completed.

Step 8: Once steps 6 and 7 have been completed the skinny file will be made available for collection by the scanning team within a maximum period of 24 hours (with the exception of weekends) following discharge in order for it to be scanned onto the CWP, It is the responsibility of ward managers to ensure that processes are in place to ensure that 'skinny files' are ready and available in a timely manner

3.2 Scanning Bureau

Within a maximum of 24 hours (with the exception of weekends) following receipt, the inpatient records will be scanned and available to view on the Clinical Web Portal.

From the standard order for skinny file the corresponding barcodes are added to the record to ensure that all documents are clearly indexed and correctly filed into the electronic record. There are 20 barcodes (Document 4) in total however only the relevant barcode is used against documentation that is created at the time of admission.

After quality checks have taken place the paper copy of the scanned record will be retained for a period of 1 month before being confidentially destroyed.

3.3 Scanning of Ward Attenders

If a patient attends a ward following discharge for a ward appointment a ward attender documentation control sheet (Document 5) must be created for each attendance and accompany the paperwork created. This documentation will be ready for collection within 24 hours (with the exception of weekends) of attendance for the scanning team to collect.

Within a maximum of 24 hours following receipt into the scanning team, the ward attendance records will be scanned and available to view on the Clinical Web Portal.

After quality checks have taken place the paper copy of the scanned record will be retained for a period of 1 month before being confidentially destroyed

3.4 Inpatient Record Documentation for a deceased patient

In the event of bereavement this document sets out the journey of the patient's record (skinny file) from the ward to Bereavement Office then to the scanning team Inpatient Record Documentation Process for a Deceased Patient.

3.5 Scanning of ICCU charts

ICCU charts are collected on a weekly basis by the Scanning Team. Charts are scanned and viewable on the CWP with 48 hours of receipt. Charts are kept for one month following scanning date then destroyed.

3.6 Scanning of outpatient documentation through POD

For outpatient areas where they are note less as part of the clinic preparation process, an Outpatient Continuation Sheet will be provided for use in clinic areas, to record the discussions and outcomes of the consultation.

At the end of clinic, all continuation sheets will be forwarded to or collected by the medical secretary who will then upload the continuation sheet into CWP via Patient Online Documentation (POD).

It is the responsibility of the directorates to ensure that the guidelines set in this protocol from preparing the documents through to the security and protection are adhered to.

4.0 Document 3:
Inpatient Documentation Control Sheet for Skinny File

Vol	Unit No(SK)
Surname	
Forename	
	NHS No
DOB	
Barcode	
(or affix patient SK ID label)	

This file contains inpatient episode documentation from:

WARD: _____

Episode Date: **Start _____End _____**

Tracking of this skinny file is essential and must be updated on PAS should the location change throughout the inpatient stay.

After discharge, record documentation must be standardised into order and any loose filing interfiled prior to record collection for scanning. Any loose filing sent to the scanning team after this record is scanned will not be scanned into the original episode of care on Clinical Web Portal (patient's electronic record) and will be scanned separately.

Skinny files should be prepared and ready for collection from the ward by the scanning team/coding team within 24 hours (with the exception of weekends) following discharge date.

Following completion of this checklist, the record will be destroyed after a time period of 1 month (from scanned date).

Ward Follow on instructions: _____
(Back to ward if no instructions)

Checklist:

	Print Name	Date
Ward Pack Completed by		
Scanned by		
Coded by		
Forwarded on by (as per ward instruction)		
Health Records File/destroy		

5.0 Document 4: Standard Order for Skinny Files

First document

Front control sheet

1.Discharge Summary
Discharge notification

2.ReSpect Forms
ReSpect Forms (will be at the front of the file whilst the patient is an in-patient; to be moved for scanning when the patient has been discharged) please note these have changed from the DNAR forms

3.Admission Record

- Patient co-morbidity record
- A&E clinical transfer form
- A&E CAS card
- GP Letters
- History and Continuation sheet
- Ambulance sheet
- Emergency admission checking proforma
- “About Me” document
- ITU Daily Assessment

4.Operation Note (scanned in colour)
Operation Note (if separate)

5.Anaesthetic Record

6.Consent Form

7.Integrated Care Pathway (scanned in colour)
Care Pathway Booklets

8. Other Procedure Documentation

- Operative Note
- Bronchoscopy report
- ERCP reports
- Pre procedure checklist
- Who Surgical checklist
- Booklets (gold)

9.Treatment Sheets

- Prescription Sheets
- Warfarin charts
- Chemo Charts

10 ECG

- ECG (colour)

11 Results & Reports (scanned in colour)

- ECG's
- EEG'S
- Miscellaneous
- Histology/cytology reports
- Endoscopy
- Cardiology
- Other investigations

12 Patient Risk Assessment

13.Nursing

Nursing Record:

- D&V form
- Urine charts
- Fluid and Food charts
- Intervention chart

Other nursing:

- Additional Manual Handling assessment
- Additional MUST chart
- Discharge Checklist
- Pressure sore booklet all HPU 1,2,3,5,6
- Falls prevention (pink)
- Weight Chart
- Urinary catheter tool

14.Care Plans (Nursing)

15 Social notes

- Safeguarding documentation
- MARF Booklets
- Any Social Services Documentation

16 Mental Health

- Any documentation regarding patient state of mind

17.Referrals

- Step Down Assessment form

- Specialist Assessment
- Continuing Health Care Assessment (CHC)
- Decision Support Tool (DST)
- Clinical Illustrations
- Section 2(social service notification)
- Section 5 (ready to discharge)
- Referral to diabetes outreach team
- Nutrition care plan

18.Therapy

All therapy docs i.e.; physiotherapy

19.All Other Hospitals

From Other hospitals except transfer and ambulance sheet

20.All Other Documentation

- Loss of property
- Temperature charts
- Transitory Forms
- Electrolyte Charts

6.0 Document 5: Ward Attender Documentation Control Sheet

Vol	Unit No
Surname	
Forename	
	NHS No
DOB	
Barcode	
(or affix patient ID label)	

This file contains ward attendance records following an inpatient admission:

Ward_____

Speciality_____

Episode Date: _____

After discharge the ward attendance record will be scanned as part of the electronic record on the Clinical Web Portal.

Following completion of this checklist, the record will be destroyed after a time period of 1 month (from scanned date).

Checklist:

	Print Name	Date
Ward Pack Complete by		
Scanned by		
Health Records File/destroy		

Attachment 7: Storage and Retrieval of a Health Record

Contents

1.0 Procedure Statement

The Trust is committed to protecting the information that it holds, and appropriate storage and security of information is the responsibility of every member of staff in the trust. The processes in this attachment must be used to facilitate this.

As the Trust moves towards electronic ways of working, the paper health record will over time become less frequently used for the care of our patients. However, in line with Records Management Code of Practice for Health & Social Care 2021, Data Protection Act 2018 (Principle 6) and GDPR, the Trust must ensure that there are both organisational and technical measures in place to keep data secure throughout the lifecycle of the health record through to destruction. This applies to both electronic and paper-based information.

Accurate recording and the knowledge of the whereabouts of all health records is essential if the information they contain is to be located quickly and efficiently. The tracking systems used provide an up to date and easily accessible movement history and audit trail. Records are often misplaced or lost because the next destination has not been recorded. It is vital that health records are appropriately retrieved and tracked to ensure they can be located as and when required to assist in the provision of quality care. There are audits in place on a monthly basis to access compliance refer to Attachment 5 Health Records Audit and monitoring.

2.0 Document 1: Health Records Storage & Security Process

Currently patient health records are stored in several formats including:

- Physical Paper Records
- Microfilmed Records
- Electronically Scanned Records (these are records which are held in paper and manually scanned in CWP)
- Electronically Sourced Records (these are records which are electronically created and retained within a system)
- Other locally held systems, both in paper and electronic formats

2.1 Standards for the storage and security of Paper and electronic health records

a) Should be stored throughout its existence in an environment suited to its format and security requirements, to ensure its preservation from physical harm or degradation and its security from loss or unauthorised access.

b) Whether original or duplicate record, it should never be kept outside corporate systems (e.g. on PC hard drives, on CDs or other removable media) except as a temporary off-line copy driven by a business need to work off-site or off-line, or for authorised transfer to other users or systems.

c) Records in all formats should be stored in conditions that protect them from threats to their physical integrity through unnecessary wear and tear; specific threats such as fire, flooding, and magnetic fields; and environmental extremes or fluctuations. Where appropriate, special storage equipment and environments should be sourced through procurement.

d) Records that are held in either electronic or paper format should be stored in systems that enable them to be readily identified and retrieved throughout their existence.

e) Records held in electronic formats should be managed and stored in such a way as to ensure usability and accessibility through time. This may involve migration of information between environments and systems, conversion to current software versions, or conversion from obsolete to current formats. Services will work with IT in such cases.

f) For paper health records protection from unauthorised access will require restricted access by being locked in a room and cabinets or storage area, ensuring that files are not left open for general or casual view. Any access to secure rooms must be via restricted ID badge access or a number lock facility.

g) For electronic records protection from unauthorised access will require mechanisms such as password protection or encryption of digital files and data. Computer monitors must not be left open for general view or casual view. Please see OP12 IT Security Policy (xrwh.nhs.uk) for more information.

h) Where records are stored on a mobile device (e.g. PDA, USB drive, laptop), special care must be taken to ensure that the device is physically protected from theft, loss, or

damage. Please refer to the removable media attachment of OP12 IT Security Policy (xrwh.nhs.uk) for more information.

i) Paper records must be transported around the site in secure envelopes or appropriately covered trolleys refer to attachment 4 - Management of a Health Record - Document 3: Transportation of Health Records

j) Where possible a clear desk policy should be adopted. Paper health records must not be left on desks but stored away securely when not in use.

k) Only access the health record for the purpose it was obtained, for further information on confidentiality (refer to OP97 Confidentiality Code of Conduct for Staff (xrwh.nhs.uk)attachment 12)

l) For more information about IT security (refer to OP12 IT Security Policy)

2.2 The Health Records Library

The Health Records Library is a 24 hour / 365 days per year, central designated safe storage area for patient 'paper' health records whilst not in use.

Access to the department is restricted to staff who have a legitimate reason for entry. Electronic swipe card access secures all doors to the department. Entry can only be gained by using the hospital ID card system upon the appropriate security being granted by the Head of Health Records Services (or designated deputy). Staff without access privileges must report to the reception area where hospital ID will be required prior to any records being released. Access to the Health Records Library will be monitored and a review will be carried out on an annual basis to ensure only staff with legitimate reasons have access.

Paper storage is currently divided into three basic elements which are 'Live Records', 'Deceased Records' and Community Archive Records.

Live Records: The main patient health record will be stored within the Health Records Library until in line with the NHS retention schedules they can be destroyed

Deceased Records: Health records for deceased patients will be retained in their original format within the Health Records Library for a period of 2 months post deceased date. After this time, they will be stored in their original format securely offsite until such time they are eligible for destruction (in line with the NHS retention schedules)

Adult Community Services Archive Storage: Local processes are in place within the Adult Community Services Group for archive records whereby they are transferred, stored and managed off site by an external company and are managed in accordance with the regulations for the storage and retention for health records refer to Document 3 Archiving, Storage and Retrieval Process for Community Records.

3.0 Document 2: Health Records Retrieval & Tracking

This protocol applies to all staff involved in the tracking and retrieval of health records from their current location to a new location whereby the last recorded person will be held responsible for the recovery of any missing records.

When tracking any 'paper' health records the following key standards MUST be applied as a minimum:

- They must be tracked immediately at the time they are created or forwarded to another location
- The tracking MUST include the date the records were forwarded
- It must include the full details of where the record will be forwarded to, i.e. name, designation/ department/ or clinic code
- The status of the record must also be updated where records have been scanned, disposed of, or sent to off-site storage
- It is desirable to include telephone extension numbers
- For outpatient clinics where noteless working has not yet been adopted, available notes will be retrieved and tracked to the clinic code from the Health Records Library. The cycle will begin whereby they will be forwarded to clinic preparation team, then to the clinic before being returned to the medical secretary.
- Staff must take responsibility for ensuring they receive any notes requested and tracked to the receiving department. If notes requested do not arrive, they must contact the original department storing the record.

For each service that handles patients paper health records, there is an expectation that local protocols are in place to ensure the above standards are applied as a minimum.

The following protocol applies to patient records stored at New Cross. In the event that records are forwarded to other sites, e.g. Cannock Chase Hospital, West Park, Gem Centre, local processes must be in place to ensure the receiving location track the records to ensure they can be located.

Health Records Library – New Cross Hospital Local Protocol (Paper Records)

The Health Records Library provides a 24 hour service for the retrieval of patient health records stored within the area. Notes can be requested via two methods:-

- **Telephone –** This method must be used to request either urgent or semi-urgent notes (required within 24hours). A maximum of 3 sets of records can be requested at any one time

- **Email –** All non-urgent requests must be requested via the Health Records email box rwh-tr.HealthRecordsLibrary@nhs.net
  When making a request you must provide the following information to ensure the tracking system is correctly updated. It can also be used to ensure that only those staff with authorised reasons may access an individual record:
  - Name and designation of the requestor
  - Extension number
  - Patient name and unit number

- Reason for request

Out of Hours Requests

For paper records required for emergencies out of hours, the Health Records Library staff must be bleeped via Switchboard who will retrieve records filed within the health records library.

Monitoring and assurance

Tracking and Tracing audits are carried out and are monitored via the Health

4.0 Document 3: Archiving, Storage & Retrieval Process for Community Records

The storage of archived patient records for Community Services is managed in joint partnership between the individual Community Service and the Health Records Service.

Patients who are currently attending a Community Service will have their paper health records stored and managed within the local service. For patients who have been discharged from the services or deceased the paper records will be stored off site with an external storage company until such time that they are eligible in line with the trust retention schedule to be destroyed (refer to attachment 8 - Retention /Appraisal/ Disposal and Destruction)

4.1 Process for Archiving from local services

Health Records will provide archiving boxes, labels and arrange ad hoc collections via emailing rwh-tr.CommunityRecordsArchiving@nhs.net or if urgent contact the Health Records team on extension 88100.

In order to achieve efficient storage, each box used to archive patient records must be filled as much as possible and not weigh more than 15kg for Health and Safety reasons.

A submission form (Document 4) must be completed for each box.

A detailed description must be included on the submission form detailing the patient records contained within the box and where possible a full inventory attached

Each box must be labelled with an ID box number label (provided by Health Records) and corresponding ID box number must be written on the 'submission form'

Once the box is filled, if a full inventory can be completed this must be attached to the submission form and placed within the top of the box

The eligible date for destruction must be clearly entered onto the box and the submission form. (Must not state as per policy)

A copy must be kept of the submission form and inventory for the local services record and retrieval process.

On a monthly basis (first Monday in month), boxes will be collected by internal transport and delivered to the offsite storage facility. Any services/location not on (Document 6) will require an ad hoc collection request.

4.1 Storage of the boxes within the offsite facility

- Following collection by the Trust's internal transport on either a monthly or ad-hoc collection, the boxes will be delivered directly to the offsite store. The collection log (Document 6) will be completed by the driver and a copy given to Health Records Services for recording
- On receipt of the boxes the offsite store will log each box number and record/index information taken from the content of the submission form the service has completed

4.2 Process for retrieving a record or box.

- The service must complete a retrieval form (Document 5) and email to rwh-tr.CommunityRecordsArchiving@nhs.net
- The requested box or individual patient record will then be requested from the offsite store, who will arrange direct delivery of the records to the service. The delivery service will return records every Friday, if requests are of an urgent nature, this must be recorded on the request form
- If a box is delivered to a service, this will be collected and re-archived on the monthly collection unless an ad hoc collection is arranged.
- If a box or an individual record is requested and will no longer be required to re-archive this must be made clear on the retrieval form

4.3 Process for re-archiving retrieved records

If you require a document or box to be returned, please return securely via internal post (for documents) or arrange internal transport to be returned to:

Community Records Archiving
c/o Health Records Library
McHale Building – Zone B, Location B19
New Cross Hospital

Please ensure that you include a copy of the original retrieval form (Document 5) with the returned document/box. If you are returning more than one document/box, please ensure that the appropriate form is securely attached to the correct document/box to allow us to re-archive correctly.

If a document has been permanently removed from a box, then re-archived it is essential that the local service records this for future reference by indicating on the original submission form in the box and a copy kept locally.

4.4 Destruction

At the start of each calendar year the records will be appraised by Health Records Services and those eligible will be destroyed in line with the retention and destruction schedule using confidential destruction within the offsite company. A destruction certificate is supplied and retained within the Health Records Services.

5.0 Document 4: Community Records Submission form

This form must be completed and placed inside the top of each storage box containing the patient files you wish to archive. Boxes will be returned to the service if not fully completed. Archive boxes are for the storage of patient records only

Specialty: _____

Location: _____

Contact number _____

Date sent _____

Date of destruction _____
(do not state as per policy)

AFFIX BOX LABEL OR WRITE BOX NUMBER HERE

Sent by (print name) _____

Sent by (signature) _____

Full description of Records contained in box (if not attaching an inventory)

Where possible a completed inventory must be attached to the submission form when forwarding records for archive storage. It is essential that a detailed description or inventory is logged and recorded within the service as it is the service responsibility to supply the appropriate box number when retrieving records.

Removed Records

Indicate full details of records permanently removed from this box after original archiving:

Patient Name:	Patient Name:
DOB	DOB
5MV/NHS Number:	5MV/NHS Number:
Date Removed:	Date Removed:
Name of staff removing:	Name of staff removing:
Reason for permanent removal:	Reason for permanent removal:
Where document now held:	Where document now held:

6.0 Document 5: Patient Record Request Form

This form must be completed to request the return of a patient record/archived box. The form must be emailed to **rwh-tr.CommunityRecordsArchiving@nhs.net**
The delivery service will return records each Friday, if requests are of an urgent nature, this must be recorded on the request form or contact the health records team on x8**8109**

Date requested	
Name & contact details of requester	
Location and speciality requested from	
Archiving box number	
Patients demographic details & any identification numbers	
Reason for requesting (please indicate if re-archiving is required or if this is a permanent retrieval	
Delivery scheduled for each Friday please state if urgent delivery required	

HEALTH RECORDS USE ONLY

DATE RECEIVED		**NAME COMPLETED**	
DATE COMPLETED		**RETRIEVAL DETAILS**	

7.0 Document 6: Community Records Collection Schedule

Monthly collections (1st Monday of each month)

Date of collection……..(to be completed by driver)

Base	Number of Boxes collected
Bilston HC (District Nurses and Community Matrons)	
Gem Centre	
Phoenix Health Centre	
Mayfields Health Centre (Foot Health)	
Pendeford HC(Anti – Coag)	
Primrose Lane HC (District Nurses)	
Science Park (District Nurses and Community Matrons)	
Warstones HC	
West Park Marson Wing Ground Floor (District Nurses, Community Matrons and Intermediate Care Team)	
West Park Marson Wing 1st Floor (Hosp @ Home, Admission Advoidance)	
West Park (Jessie Fowlke corridor)(Neuro Rehab,)	
West Park (Jessie Fowlke corridor)(Stroke Coordinators)	

Any services/locations not on the above table will require an ad hoc collection request through emailing rwh-tr.CommunityRecordsArchiving@nhs.net

Attachment 8: Retention, Appraisal, Disposal and Destruction of Health Records

Contents

1.0 Procedure Statement

This protocol details the appropriate standards regarding the retention, appraisal, disposal and destruction of health records.

Storage limitation is a key principle, which links closely with the right of access. This principle ensures that information is kept in a form that permits the identification of patients for no longer than is necessary and only for the purposes for which the personal information is processed. This applies to all records, including those which are kept electronically i.e. Clinical Web Portal.

Directorates will periodically review and appraise patient records in line with the retention schedule and anonymise or erase any data we no longer have a valid legal basis to process or retain. When using patient identifiable data for uses beyond direct care purposes (secondary purposes ie research etc) needs to be assessed in line with the De-Identification and Pseudonymisation Policy http://intranet.xrwh.nhs.uk/pdf/policies/OP_111_Policy.pdf this reduces the risk that the record becomes irrelevant, excessive, inaccurate or out of date. Apart from helping the Trust to comply with the data minimisation and accuracy principles of GDPR, this also reduces the risk that we will use such data in error. Personal data held for longer than retention guidance standards may also increase the level risk associated to that date, and result in additional resources used when not necessary.

Records, whether in paper or electronic format must not be kept longer than necessary. When records are at the end of their minimum retention period, refer to the Records Management Code of Practice for Health and Social Care 2021 Disposal will consist of the record being removed for permanent preservation or the record being deemed fit for permanent destruction.

If consent is used as the legal basis to process the patients data then the agreed retention period must be adhered to, and a patient may withdraw their consent and also apply the right to erasure at any time, at which point their identifiable data can no longer be used, and must be erased/anonymised (as per consent agreement). All electronic systems must be able to do this.

The fifth data protection principle states from the Data Protection Act 2018 (DPA):

(1) is that personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

(2) Appropriate time limits must be established for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

Remember that directorates must also respond to subject access requests for any personal data held. This may be more difficult if old data is held for longer than needed. Individuals have rights to the information that is held about them including rights of access, rectification, erasure, to restrict processing, so if data is kept for longer than the set retention periods this will need to be justified and an explanation why their personal data has been kept in a form that permits the identification of the individual. The patient could make a complaint and report this to the ICO for the Trust to be investigated.

2.0 Retention Schedule

Each record must be examined/appraised prior to destruction and the retention periods below applied. Examples of health records the Trust holds are in the below table. This list is not exhaustive and the Records Management Code of Practice should always be consulted prior to destruction.

Record Type	Local Procedures
General Adult Health Records	8 years from discharge or when patient last seen Please also see below 2.1
Adult Social Care Records	8 years from discharge or when patient last seen
Children's Records (including midwifery. Health visiting and school nursing)	25th Birthday or 26th if the patient was 17 at the conclusion of treatment. (check for any other involvement which will extend the retention period) Please also see below 2.1
Obstetric Records, Maternity Records, Antenatal and Post Natal records	25 years. Please also see below 2.1
Cancer/Oncology Records	30 years (or 8 in the event of patient death)
Contraception/Sexual Health	8 years after discharge unless implant or device inserted in which case 10 years
Electronic Patient Records	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the

	records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule. Please also see below 2.1
GP Patients Records	Sent to CAPITA PCS for records management
Litigation cases	10 years adults / 30 years children - post case closure, review and consider transfer to a place of deposit. At this point litigation cases will be referred to legal services for appraisal. Health Records to consider any further sanctions that may apply on a case by case basis.

- You need to think about and be able to justify how long you keep personal data. This will depend on your purposes for holding the data.
- You should periodically review the data you hold and erase or anonymise it when you no longer need it
- You must carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data
- You can keep personal data for longer if you are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.
- You must have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten' refer to Attachment 4 – Health Records Access and Subject Rights Requests Procedure.

3.0 Independent Inquiry's

At the time of writing there are two independent Inquiries which have requested that restrictions are in place on the destruction of patient records.

Children's records as part of the Independent Inquiry into Child Sexual Abuse (IICSA) also referred to as the Goddard Report, the conclusion of this inquiry is expected in 2022, no child records can be destroyed. This includes patients who are now adults who have a paediatric section in their health record i.e. they received care as a child. For further information see https://www.iicsa.org.uk/

- The Infected Blood Inquiry medical records are not destroyed for patients identified as having Haemophilia. To ensure as a Trust we compile to this we advise that records are retained in the electronic record on (CWP) if a transfusion has been given. Further information about the records required can be found on their website Homepage | Infected Blood Inquiry

4.0 Appraisal Process

The process of deciding what to do with records whether paper or electronic when their use has ceased is called appraisal.

Appraisal of records must be undertaken by the IAO or their nominated person with delegated authority and should be a planned schedule of work within the department and not just an ad hoc process.

The purpose of an appraisal process is to ensure that the heath records are examined at the appropriate time to determine whether they need to be retained for a longer period of time, or whether they should be destroyed.

5.0 Identification of Patient Records for Destruction

Inactive patient records are identified for destruction as per process below.

Inactive patients are defined as no activity on the Patient Administration System (PAS) or Clinical Web Portal (CWP) for the time periods given above (Section 2.0). GP initiated requests provided by Pathology and/or Radiology, which do not result in any activity i.e. a referral in to the Trust, are not included.

- Retention periods must be calculated from the end of the calendar year and from the date of the patient's last attendance or date of death in the case of deceased patients.
- Check the eligibility for destruction of the health record in line with the retention schedule/Records Management Code of Practice for Health and Social Care 2021. Ensure your decision to destroy has followed a checking process and validated by a colleague, IAO's to ensure there is a local process in place.
- If the health record is eligible, update the casenote status on PAS or any relevant system that holds the record to denote that the record has been destroyed and when.

6.0 Destruction of paper records

All patient records eligible for destruction must be disposed of confidentially and to an international standard (BSIA EN15713:2009 – Secure Destruction of Confidential Material) refer to the HS10 Waste Management Policy. Shredding must be completed by using a cross cut shredder under confidential conditions. Shredding bins are available from Waste Management in the Estates Department who will arrange for a confidential bin to be delivered and a collection service. The Trust has approved an external shredding company, who will destroy confidential waste onsite under these standards.

Information Asset Owners must provide copies of their destruction certificates to Head of Health Records Services on request.

7.0 Destruction of Electronic Records

Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub (document indexing) can remain demonstrating that a record has been destroyed, then the code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed.

If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the required retention period. This will be managed by the IAO or their nominated person with delegated authority

By hard delete we are referring to the complete destruction and unavailability of the electronic patient record and its dependencies.

By soft delete we are referring to the complete removal of access to an electronic patient record by end users. However, the record remains archived until such time as it can be hard deleted safely. Where possible, hard deletion of electronic records will proceed, however, where such an activity endangers the wider store of electronic patient records, a soft delete will be performed. In some circumstances, the health record cannot be permanently deleted (hard delete) without damaging the data store of the incumbent system. In such circumstances, the health records will be rendered neutralized by removing all ability to access it (soft delete), effectively deleting it in all but action.

With electronic records, the case may be that where information that has been 'deleted' may still exist, in some form or another, within a system. The word 'deletion' can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the health record. The key is to ensure data is put beyond use (soft deleted). If it is appropriate to delete the health record from a live system, any information held on a back-up system must also be deleted.

You must seek advice from ICT Services regarding whether an IT system is enabled to permanently delete the health record or data held.

IAO's must ensure local processes are in place for their information assets.

8.0 Electronic media

A wide range of electronic storage media may be used to store or process patient records including, but not necessarily limited to:

- Desktop computers
- Servers
- Multifunction devices (e.g. printers)
- Photocopiers
- Laptops, tablet computers and electronic notebooks
- Mobile telephones
- Digital recorders
- Cameras
- iPads/hand held devices
- USB devices
- DVDs, CDs and other portable devices and removable media.

Please refer to OP12 attachment 19 – Sanitisation, Reuse, Disposal and Destruction Protocol for further advice.

Records Management Code of Practice 2021

A guide to the management of health and care records

AUGUST 2021

CONTENTS

Introduction

The Records Management Code of Practice for Health and Social Care 2021 (from this point onwards referred to as the Code) is a guide for you to use in relation to the practice of managing records. It is relevant to organisations working within, or under contract to, the NHS in England. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities.

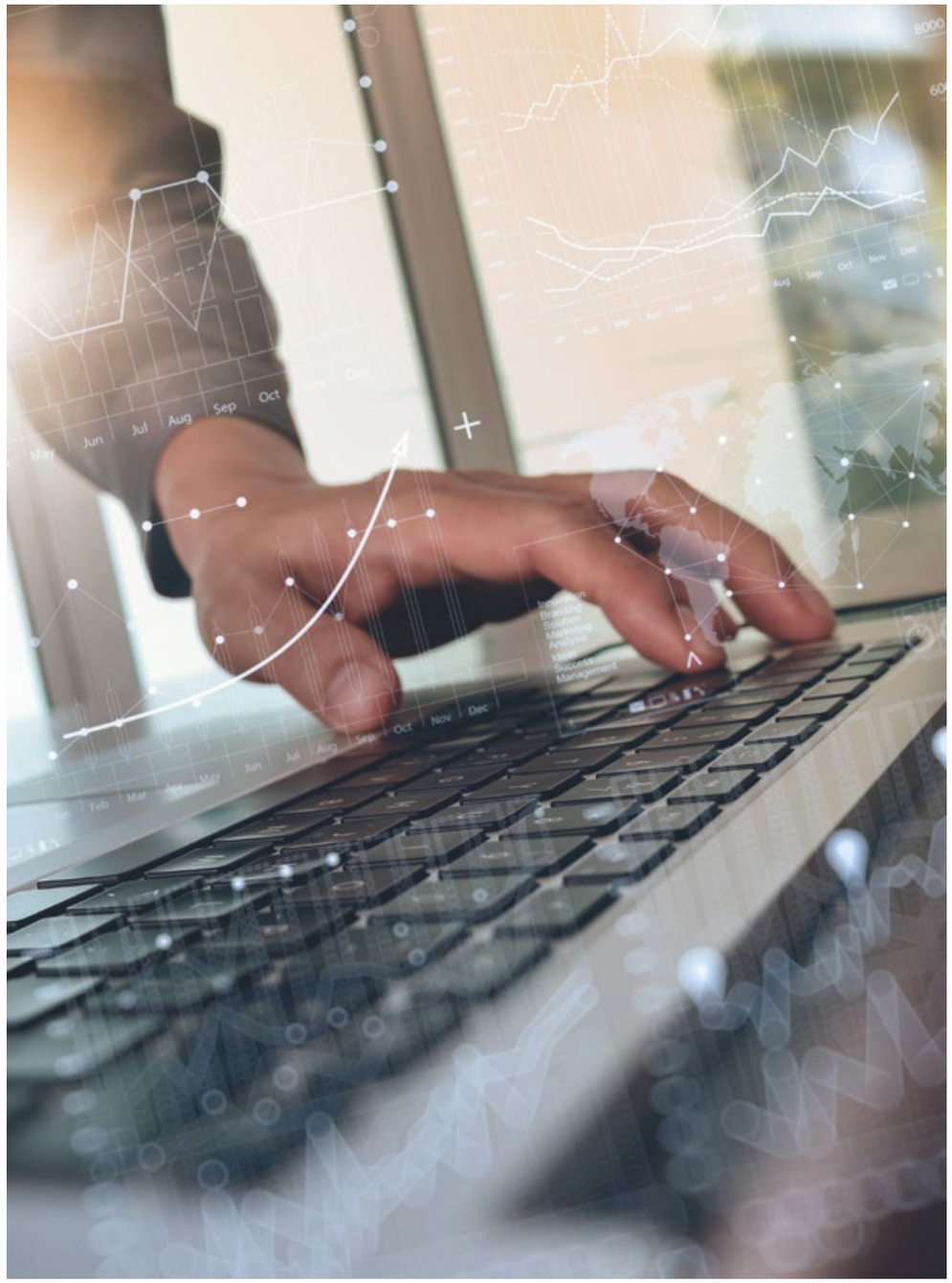
The Code provides a framework for consistent and effective records management based on established standards. It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records. It also advises on how to design and implement a records management system including advice on organising, storing, retaining and deleting records. It applies to all records regardless of the media they are held on. Wherever possible organisations should be moving away from paper towards digital records.

The Code is accompanied by a number of important appendices:

- **Appendix I**: information on public inquiries
- **Appendix II**: a retention schedule for different types of records
- **Appendix III**: detailed advice on managing different types and formats of records such as integrated care records and staff records.

All organisations and managers need to enable staff to conform to the standards in this Code. This includes identifying organisational changes or other requirements needed to meet the standards, for example, the people, money and correct tools required. Information Governance performance assessments, such as the Data Security and Protection Toolkit hosted by NHS Digital, and your own organisation management arrangements will help you identify any necessary changes to your current records management practices. Those who have responsibilities for monitoring overall performance, like NHS England and Improvement and the Care Quality Commission (CQC), help ensure effective management systems are in place. An example is by inspecting sites as part of their key lines of enquiry and statutory powers.

The guidelines in this Code draw on published guidance from The National Archives and best practice in the public and private sectors. It is informed by lessons learnt and it will help organisations to implement the recommendations of the Mid Staffordshire NHS Foundation Trust Public Inquiry relating to records management and transparency.



This Code must also be read in conjunction with the following:

- Professional Records Standards Body (PRSB) structure and content of health and care records standards
- Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (FOIA) - The National Archives has commenced work on revising this code and will issue an update in due course.

This 2021 revision was conducted by NHSX. It reflects feedback following a consultation which 50 organisations responded to including national stakeholders and local organisations. It is intended to be a light-touch review. The Code replaces previous guidance listed below:

- Records Management: NHS Code of Practice: Parts 1 and 2: 2006, revised 2009 and 2016
- HSC 1999/053: For the Record - managing records in NHS Trusts and health authorities
- HSC 1998/217: Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients (Replacement for FHSL (94) (30))
- HSC 1998/153: Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice

Standards and practice covered by the Code will change over time so this document will be reviewed and updated as necessary. In particular, it should be noted that at the time of writing there are a number of on-going public inquiries including the Independent Inquiry into Historic Child Sex Abuse (IICSA) and Infected Blood Public Inquiry (IBI). This means that records must not be destroyed until guidance is issued by the inquiry. Future public inquiries may lead to specific records management requirements. Where that happens, the Inquiry will publish additional guidance on its website. NHS England and Improvement may also issue guidance to the health and care system relating to the inquiry.

It should also be noted that we are proposing to undertake a review into the retention time for de-registered GP records. De-registered refers to when a patient is no longer on the GP practice system. It does not refer to patients who are still registered at a GP practice but have not needed to receive care. If a patient has moved to another practice, the record would be sent to the new provider. However, if the reason for de-registration is unknown, the digital record is printed off and sent in paper form to NHS England and Improvement. We are proposing to review the retention time for de-registered GP records to ensure that the significant costs of retaining the records for 100 years are justified by the benefits they bring. We will look for example at how many records are recalled and what the reasons are.

Scope of the Code

1.1 OVERVIEW

This section explains the legal definition of a record and the types of records in scope of the Code.

1.2 WHAT IS A RECORD?

There are a couple of definitions of a record, which are useful to highlight. The ISO standard ISO 15489-1:2016 defines a record as:

> *'Information created, received, and maintained as evidence and as an asset 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.

1.3 SCOPE OF RECORDS COVERED BY THE CODE

The guidelines in this Code apply to NHS and adult social care records. This includes:

- records of patients treated by NHS organisations
- records of patients treated on behalf of the NHS in the private healthcare sector
- records of private patients treated on NHS premises
- records created by providers contracted to deliver NHS services (for example, GP services)
- adult service user records who receive social care support
- jointly held records
- records held as part of a Shared Care Records programme
- records held by local authorities such as public health records, contraceptive and sexual health service records
- staff records
- complaints records
- corporate records – administrative records relating to all functions of the organisation

The Code does not cover children's social care records. These are within the remit of the Department for Education.

Whilst not strictly covered by this guide, private providers can also use this Code for guidance in relation to their records management. The Private and Voluntary Health Care (England) Regulations 2001 provide a legal framework for private providers to manage their records.

There are a number of smaller health and care providers that this Code will apply to, for example, dental practices or independent care providers providing an element of NHS or nursing care. For some aspects of this Code, these small organisations should take a pragmatic approach to, for example, the application of security classifications.

1.4 TYPE OF RECORDS COVERED BY THE CODE

The guidelines apply regardless of the media on which the records are held. Usually these records will be on paper or digital. However, some specialties will include physical records, such as physical moulds made from plaster of Paris (refer to Appendix III).

Examples of records that should be managed using the guidelines in this Code include:

- health and care records
- registers - for example, birth, death, Accident and Emergency, theatre, minor operations
- administrative records, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling
- x-ray and imaging reports, output and images
- secondary uses records (such as records that relate to uses beyond individual care), for example, records used for service management, planning, research

Examples of record formats that should be managed using the guidelines from this code:

- digital
- paper
- photographs, slides, and other images
- microform (microfiche or microfilm)
- physical records (records made of physical material such as plaster, gypsum and alginate moulds)
- audio and video tapes, cassettes, CD-ROM etc
- e-mails
- computerised records
- scanned records
- text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient or service user) such as Twitter and Skype
- metadata added to, or automatically created by, digital systems when in use. Content can sometimes be of little value if it is not accompanied by relevant metadata
- websites and intranet sites that provide key information to patients or service users and staff

Appendix III provides further details about managing specific types of records, for example, complaints records.

Records management obligations

2.1 OVERVIEW

All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law. Health and care professionals also have professional responsibilities, for example, complying with the Caldicott Principles and records keeping standards set out by registrant bodies. Whilst every employee has individual responsibilities, each organisation should have a designated member of staff who leads on records management. Each organisation should also have a policy statement on records management which is made available to staff through induction and training. Organisations may be asked for evidence to demonstrate they operate a satisfactory records management regime.

2.2 LEGAL OBLIGATIONS

Public Records Act 1958 and Local Government Act 1972

The Public Records Act 1958 is the principal legislation relating to public records. Records of NHS organisations are public records in accordance with Schedule 1 of the Act. This means that employees are responsible for any records that they create or use in the course of their duties. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. The Act applies regardless of the format of the records. The Secretary of State for Health and Social Care and all NHS organisations have a duty under the Act to make arrangements for the safekeeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public Records who reports annually on this to the Secretary of State for Culture, Media and Sport who is accountable to parliament.

Public health and social care records, where a local authority is the provider (or the provider is contracted to provide services to a local authority), must be managed in accordance with the requirement to make proper arrangements under Section 224 of the Local Government Act 1972. This states that proper arrangements must be in place with respect to any documents that belong to or are in the custody of the council or any of their officers.

Where health and social care records are created as a joint record or part of a system where local health and care organisations can see the records of other local health and care organisations, then these records would be managed in line with the requirements of the Public Records Act 1958 where one or more of the bodies that created the joint record is a public record body.

The NHS Standard Contract notes a contractual requirement on organisations which are not bound by either the Public Records Act 1958 or the Local Government Act 1972 to manage the records they create. There are also statutory requirements affecting both private and voluntary care providers as set out in the Private and Voluntary Health Care Regulations 2001.

Freedom of Information Act 2000

The Freedom of Information Act (FOIA) governs access to and management of non-personal public records. The FOIA was designed to create transparency in government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of those organisations to supply information through good records management programmes. Records managers should adhere to the code of practice on record keeping issued by the Secretary of State for Culture, Media and Sport, under section 46 of the FOIA. The section 46 Code of Practice is used as a statutory statement of good practice by the regulator and the courts.

UK GDPR and Data Protection Act 2018

The UK GDPR is the principal legislation governing how records, information and personal data are managed. It sets in law how personal and special categories of information may be processed. The Data Protection Act 2018 principles are also relevant to the management of records. Under the UK GDPR, organisations may be required to undertake Data Protection Impact Assessments (DPIA) as set out in Section 3 of this Records Management Code.

The UK GDPR also introduces a principle of accountability. The Information Commissioner's Office (ICO) Accountability Framework can support organisations with their obligations. Good records management will help organisations to demonstrate compliance with this principle.

Health and Social Care Act 2008

Regulation 17 under the Health and Social Care Act 2008 requires that health and care providers must securely maintain accurate, complete and detailed records for patients or service users, employment of staff and overall management. The CQC are responsible for regulating this and have issued guidance on regulation 17. The CQC may have regard to the Code when assessing providers' compliance with this regulation.

Other relevant legislation

Other legislation requires information to be held as proof of an activity against the eventuality of a claim. Examples of legislation include the Limitation Act 1980 or the Consumer Protection Act 1987. The Limitation Act sets out the length of time you can bring a legal case after an event and sets it at six years. This forms the basis for some of the retention periods set out in Appendix II.

2.3 PROFESSIONAL OBLIGATIONS

Staff who are registered to a Professional body, such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC) or Social Work England will be required to adhere 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.

The Academy of Medical Royal Colleges (AoMRC) generic medical record keeping standards were prepared for use in the NHS, primarily in acute settings but the standards are useful for all health and care settings. The AoMRC notes that a medical record, whether paper or digital, must adhere to certain record keeping standards. The Royal College of Nursing has produced guidance on abbreviations and other short forms in patient or client records.

Further information about professional standards for records can be obtained from your relevant professional body. The main standard setting bodies in health and social care in England are:

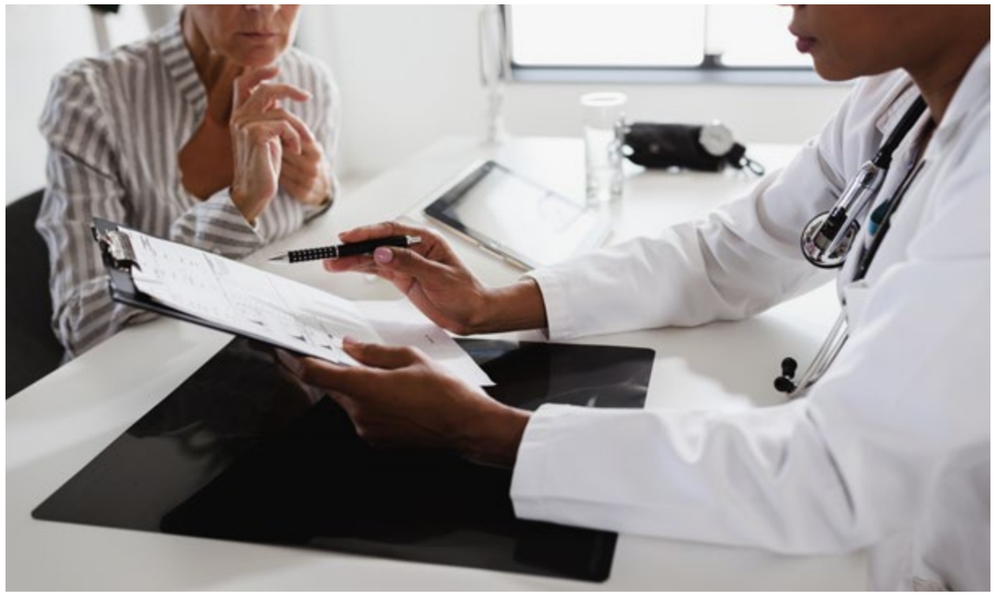
- Academy of Medical Royal Colleges
- British Medical Association
- General Medical Council
- Health and Care Professions Council
- Royal College of Midwives
- Royal College of General Practitioners
- Royal College of Nursing
- Royal College of Obstetricians & Gynaecologists
- Royal College of Pathologists
- Faculty of General Dental Practice
- Pharmaceutical Services Negotiating Committee
- Royal College of Physicians
- Social Work England

There are also organisations that provide advice specifically to records managers and archivists. These are:

- The Federation for Informatics Professionals
- The National Archives
- The Archives and Records Association
- The Institute of Health Records and Information Management
- Information and Records Management Society

Caldicott principles

The Caldicott principles outline eight areas that all health and social care staff are expected to adhere to in addition to the UK GDPR.



2.4 MANAGEMENT RESPONSIBILITIES

Records management should be recognised as a specific corporate responsibility within every organisation. It should provide a managerial focus for records of all types, in all formats throughout their lifecycle, from creation through to ultimate disposal. The records management function should have clear responsibilities and objectives and be adequately resourced to achieve them.

A designated member of staff of appropriate seniority, ideally with suitable records management qualifications, should have lead responsibility for records management within the organisation. This could be a care home manager or practice manager or in a larger organisation, a staff member reporting directly to a board member. This lead role should be formally acknowledged, included in relevant job descriptions and communicated throughout the organisation. It is essential that the manager(s) responsible for the records management function is directly accountable to or works in close association with the manager(s) responsible for other information governance work areas. When new IT projects or upgrades are introduced, the person responsible for Records Management should be closely involved.

As records management activities are undertaken throughout the organisation, mechanisms must be in place to enable the designated corporate lead to exercise an appropriate level of management of this activity, even where there is no direct reporting line. This might include cross-departmental records and information working groups or individual information and records champions or coordinators who may also be information asset owners.

All staff, whether working with clinical or administrative records, must be appropriately trained so that they are competent to carry out their designated duties and fully aware of their personal responsibilities in respect of record keeping and records management. No patient or service users' records or systems should be handled or used until training has been completed. Training must include the use of electronic records systems. It should be done through generic and organisation-wide training programmes which can be department or context specific. Training should be complemented by organisational policies, procedures and guidance documentation.

2.5 ORGANISATIONAL POLICY

Each organisation must have an overall policy statement on how it manages all of its records. This may be a standalone policy or part of the overall suite of IG policies. The policy should include details of how the organisation will use the records it creates. For example, as well as records being used to plan and deliver care, they will also be used for service improvement and research.

This statement must be endorsed by the Operational Management Team, board (or equivalent) and made available to all staff at induction and through regular updates and training.

The policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an organisational commitment to create, keep, manage, and dispose of records and document its principal activities in this respect. The policy should also:

- outline the role of records management within the organisation and its relationship to the organisation's overall strategy
- define roles and responsibilities within the organisation in relation to records, including the responsibility of individuals to document their actions and decisions. An example is, who is responsible for the disposal of records
- assign responsibility for the arrangements for records appraisal, selection and transfer for the permanent preservation of records (as required by section 3 (1) of the Public Records Act 1958)
- provide a framework for supporting standards, procedures and guidelines and regulatory requirements (such as CQC and the NHS Digital hosted Data Security and Protection Toolkit)
- indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored and maintained
- provide the mandate for final disposal of all information by naming the committee or group that oversees the processes and procedures
- provide instruction on meeting the records management requirements of the FOIA and the UK GDPR

The policy statement should be reviewed at regular intervals (at least once every two years) and if appropriate should be amended to maintain its relevance. The policy is also an important component of the organisation's information governance arrangements and should be referenced in the organisation's IG policies or framework.

Organisations must also conduct an annual survey to understand the extent of their records management responsibilities and to help inform future work-plans. It will aid organisations to know:

- what series of records it holds (and potential quantities)
- the format of its records
- the business area that created the record (and potential Information Asset Owner)
- disposal potential for the coming year

Information Asset Management systems may support this process. They can help identify where records are held and whether they are being held under the correct security conditions, and in the case of health and care records, remain confidential. The process can also be used as an opportunity for asset owners to identify how long their records need to be held. The process will identify business critical assets and ensure that there are adequate business continuity measures in place to assure access.

2.6 MONITORING RECORDS MANAGEMENT PERFORMANCE

Organisations may be asked for evidence to demonstrate they operate a satisfactory records management regime. There is a range of sanctions available if satisfactory arrangements are not in place. Sanctions vary in their severity for both organisations and the individual. They may include:

- formal warning
- professional de-registration – temporary suspension or permanent
- regulatory intervention – leading to conditions being imposed upon an organisation, or monetary penalty issued by the ICO

Organising records

3.1 OVERVIEW

As set out in section two, each organisation must have a policy for managing records. This section describes how to design and implement a records management scheme, decide what a record is and arrange records. It includes information about the importance of metadata and security classifications.

3.2 DESIGNING A RECORDS KEEPING SYSTEM

A record keeping system should be implemented at organisational level and within departmental standard operating procedures as appropriate. 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.

A records management system should cover each stage of the lifecycle:

- creation: create and log quality information
- using: use or handle
- retention: keep or maintain in line with NHS recommended retention schedule
- appraisal: determine whether records are worthy of archival preservation
- disposal: dispose appropriately according to policy

Designing and Implementing Record Keeping Systems (DIRKS) is a manual which led to the creation of ISO 15489-1:2016 Information and documentation - Records Management**.** This standard, published by the International Organization for Standardization (ISO), focuses on the business principles behind records management and how organisations can establish a framework to enable a comprehensive records management programme. The standard is an eight-stage process and can be summarised as:

1. conduct preliminary investigation
2. analyse business activity
3. identify requirements for records
4. assess existing systems
5. identify strategies to satisfy requirement
6. design records system
7. implement records systems
8. conduct post implementation review

The standard also describes the characteristics of a record.

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 To have been created or sent at the time purported
Reliable	Full and accurate record of the transaction or activity or fact Created close to the time of transaction or activity Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction or activity
Integrity	Complete and unaltered Protected against unauthorised alteration Alterations after creation can be identified as can the person making the changes
Useable	Located, retrieved, presented and interpreted Context can be established through links to other records in the transaction or activity

These characteristics allow strategies, policies and procedures to be established that will enable records to be authentic, reliable, integral and usable throughout their lifecycle.

In terms of ensuring a record is reliable, where an organisation realises that inaccurate information is being held about its patient or service users, then it should take steps to rectify the situation and make records as accurate as they can. An example of what action might be taken can be found in the Institute of Health Records and Information Management (IHRIM) - Good Practice Guidance 2020.

There are a series of other British and international standards that are used to produce record keeping systems. These all interrelate and work within the same guiding principles and where possible use the same terminology. They all rely upon defining roles and responsibilities, processes, measurement, evaluation, review and improvement.

3.3 CONDUCTING A DATA PROTECTION IMPACT ASSESSMENT

Under UK GDPR, organisations are required to conduct Data Protection Impact Assessments (DPIAs) where there is a new or change in use of personal data and a potentially high risk to privacy. A DPIA template can be found on the ICO website). Some uses require a mandatory DPIA (where processing is large scale or introduces new technologies. If you are looking to establish a new records management function, then it will be vitally important to complete a DPIA. This will highlight potential risks to privacy and data protection, allowing you to action, mitigate or eliminate that risk. This must be conducted prior to any processing being carried out.

When you are looking to amend a record's function, you should check with the person responsible for records management first, for example, your record manager or your data protection officer. DPIA completion in this circumstance will depend on the amendments you are looking to make. For example, if you intend to add three racking shelves for paper HR files to the existing twenty shelves you would probably not complete a DPIA. If you were looking to send your records offsite for scanning or destruction you must complete a DPIA, as this is a new process and the risk is greater.

3.4 DECLARING A RECORD

Within the record keeping system, there must be a method of deciding:

- what is a record
- what needs to be kept

This process is described as 'declaring a record'. A record can be declared at the point it is created or it can be declared 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 retention policy that has been adopted. Some activities will be pre-defined as creating a record that needs to be kept, such as health and care records or the minutes and papers of board meetings. Other records will need to fulfil the criteria as being worth keeping, such as unique instances of a business document or email. Datasets may also be declared as records and managed accordingly.

Declared records can be held in the 'business as usual' systems or they can be moved into a protected area such as an Electronic Document and Records Management System (EDRMS) depending on the record keeping system in use. Organisations' teams should only hold the records they need to conduct business, locally.

Records and information relating to closed cases may be kept locally for a short period of time (such as a year). This is in case a patient or service user re-presents or is re-referred. After that time, they should be moved to long-term storage for the rest of their retention period. 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 or sensitive data. Your organisation's records management policy should cover what you need to do locally in this circumstance.

Key legislation, such as the UK GDPR or FOIA, applies to all recorded information of the types covered by these Acts, whether declared as a formal record or not. However, declaration makes it easier to manage information in accordance with the legislation and business needs. Requests for information made under this legislation are easier to find in a logical filing system. Accumulations of informally recorded information, which can be difficult to find, should therefore be minimised.

3.5 ORGANISING RECORDS

Record keeping systems 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, however, it is often linked to an organisation's hierarchical structure.

Records should be arranged into a classification scheme, as required by ISO 15489 and the Section 46 Code of Practice. At the simplest level, the business classification scheme can be anything from an arrangement of files and folders on a network to an EDRMS. The important element is that there is an organised naming convention, which is logical, and can be followed by all staff. The scheme can be designed in different ways. Classification schemes should try to classify by function first. Once a recommended 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 2018-March 2019

The transaction can then be assigned a rule (such as retention period), a security status or other action based on the organisational policy. The scheme will enable appropriate management controls to be applied and support more accurate retrieval of information from record systems.

3.6 USING METADATA TO ORGANISE AND FIND RECORDS

Metadata is 'data about data' or structured information about a resource. The Cabinet Office e-Government Metadata Standard states that:

> *'metadata makes it easier to manage or find information, be it in the form of webpages, electronic documents, paper files or databases and for metadata to be effective, it needs to be structured and consistent across organisations'*

The standard sets out 25 metadata elements, which are designed to form the basis for the description of all information. The standard lists four mandatory elements of metadata that must be present for any piece of information. A further three elements are mandatory if applicable and two more are recommended.

Mandatory elements	Mandatory if applicable	Recommended
Creator	Accessibility	Coverage
Date	Identifier	Language
Subject	Publisher	
Title		

The following provides a practical example of the metadata standard being used to produce a label to be placed on the side of a box of paper records, which are ready to archive:

Box label	Local interpretation	Metadata standard
Tiverton Community NHS Trust	Organisation name	Creator
Midwifery	Service name	Creator
Patient case records surname A-F	Description of record	Subject or title
2000	Date/year of discharge	Date
2025	Date/year of destruction	Date

Where there is sufficient metadata it can be possible to arrange records by their metadata alone, however, a business classification scheme would always be recommended. Records arranged by their metadata rather than into a classification scheme often lack 'context'. This reduces the ability to produce an authentic record. Finding records arranged in this way is often reliant on a powerful search tool used to 'mine' the data or use a process called 'digital archaeology'. This is not recommended because it is so time-consuming to determine authenticity, but it has been included in this Code as legacy record keeping systems may not have been organised logically.

3.7 APPLYING SECURITY CLASSIFICATIONS

The NHS has developed a protective marking scheme for the 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 data is classed as 'NHS Confidential'.

There is no expectation that a security classification must be applied or used by all health and care organisations. For example, it would be disproportionate for a small care home or dental practice to apply NHS or Government security classifications to a small cohort of records. Whereas a large NHS Trust may want to use the NHS classification scheme.

Records storage for operational use

4.1 OVERVIEW

This section covers how to store records for operational use. It includes considerations relating to both paper and digital records including the challenge of ensuring digital records remain authentic and usable over time and the management of off-site storage. Further information about the management of specific formats of records (for example, cloud-based records and records created on personally owned computers and equipment) are in Appendix III.

4.2 MANAGEMENT AND STORAGE OF PAPER RECORDS

Wherever possible, organisations should be moving to digital records. The original paper record guarantees the authenticity of the record. However, it can make it hard to audit access to the record, depending on where this is stored, because paper records do not have automatic audit logs. Storage of paper records also will incur costs, whether in-house or offsite. This cost will only increase as the size of the holding or length of time they are stored, increases.

Where possible, paper records management processes should be as environmentally friendly as possible. This will help contribute towards the NHS target to reduce its carbon footprint and environmental impact. Examples include the shredding of paper records and the end product used for recycling purposes instead of burning records in industrial furnaces.

4.3 MANAGEMENT AND STORAGE OF DIGITAL RECORDS

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, for example, through the use of search functions and digital tools.

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

The European Commission has produced an overarching standard in this area. (Further information is available on the DLM forum foundation). The authenticity of a record is dependent on a number of factors:

- sufficient metadata to allow it to remain reliable, integral and usable (refer to section 3)
- the structure of the record
- the business context
- links between other documents that form part of the transaction the record relates to

The management of digital records requires constant, continual effort, and should not be underestimated. Failure to properly maintain digital records can result in doubt being raised over the authenticity of the digital image. Examples include:

- a record with web links that do not work once they are converted to another format, loses integrity
- a record with attachments, such as hyperlinks or embedded documents that do not migrate to newer media, are not complete or integral
- an email message that is not stored with the other records related to the transaction, is not integral as there are no supporting records to give it context

Digital information presents a unique set of issues which must be considered and overcome to ensure that records remain:

- authentic
- reliable
- retain their integrity
- retain 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 and the advent of newer digital platforms. Digital preservation ensures that digital information of continuing value remains accessible and usable.

The amount of work required to maintain digital information as an authentic record must not be underestimated. For example, the information recorded on an electronic health record system may need to be accessible for decades (including an audit trail to show lawful access and maintain authenticity) to support continuity of care. Digital information must not be left unmanaged in the hope a file can be used in the future. The National Archives has produced a variety of technical and role-based guidance and useful checklists to support this management process.

As there are no digital records in existence today that are of such an age, it is difficult to even plan continued access in an authentic form over such a timeframe. For example:

- paper records can deteriorate over time - so can digital media as the magnetic binary code can de-magnetise in a process called 'bit rot' leading to unreadable or altered information, thus reducing its authenticity
- software upgrades can leave other applications unusable as they may no longer run on updated operating systems
- media used for storage may become obsolete or degrade, and the technology required to read them may not be commercially available
- file formats become obsolete over time as more efficient and advanced ones are developed

There are several strategies that can be adopted to ensure that digital information can be kept in an accessible form over time. Among the most common strategies adopted are:

- migration to the new systems (retaining existing formats - this is the preferred method)
- emulation (using software to simulate the original application)
- preservation of host system
- conversion to a standard file format (or a limited number of formats)

The Digital Preservation Coalition has produced a handbook that will help organisations understand some of the issues associated with retaining digital records for long periods of time.

The UK Government National Cyber Security Centre (NCSC) provides good practice guidelines on forensic readiness and defines it as:

> *'the achievement of an appropriate level of capability by an organisation in order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in security investigations, in disciplinary matters, in an employment tribunal or in a court of law'.*

The NCSC notes that

> *'it is important for each organisation to develop a forensic readiness of sufficient capability and that it is matched to its business need'.*

Forensic readiness involves:

- specification of a policy that lays down a consistent approach to digital records
- detailed planning against typical (and actual) case scenarios
- identification of (internal or external) resources that can be deployed as part of those plans
- identification of where and how the associated digital evidence can be gathered that will support case investigation
- a process of continuous improvement that learns from experience

In many organisations, forensic readiness is managed by information security or informatics staff, but records managers need to ensure that they input to policy development and feed in case scenarios as necessary.

Where possible, electronic records management processes should be as environmentally friendly as possible to help contribute towards the NHS target to reduce its carbon footprint and environmental impact. An example would be to replace outdated IT servers with up to date energy efficient systems, reducing the amount of energy required for the solution.

4.4 MANAGING OFFSITE RECORDS

It is vital to highlight the importance of actively managing records stored offsite. This applies to both paper records and records stored in cloud-based solutions (refer to Appendix III for further information about cloud-based records). Managing off-site records effectively will ensure that:

- there is a full inventory of what is held offsite
- retention periods are applied to each record
- a disposal log is kept
- there is evidence of secure disposal of records and information

The National Archives has produced guidance to identify and support the requirements for selecting and transferring paper records and further guidance on identifying and specifying requirements for offsite storage of physical records. It is a best practice benchmark for all organisations creating or holding public records and provides advice and guidance on the tracking of records at all stages of the information lifecycle up to disposal. The National Archives does not provide guidance on onsite storage of operational and live records. This should be determined by the local organisation in line with this Code.

When considering using offsite storage, organisations should consider the following:

- **Instruction**: The controller must provide clear instructions relating to all processing of offsite records including destruction of the records.
- **Access to site**: Access to the storage site should be possible to be able to exercise due diligence, and conduct site visits if necessary.
- **Retrieval**: Organisations will need to agree how their records will be retrieved and what timeframe they will be returned. An example would be to ensure that you can respond to subject access and FOI requests or retrieve them to dispose of when the minimum retention period has been reached.

You must conduct a DPIA if you are looking to start storing records offsite. This is because it will be a new process for handling potentially high volumes of personal data with increased risk. A DPIA must be completed:

- at the outset of entering an offsite storage contract
- if you have not completed one before on the service (even if it has been established for a number of years)
- if you change service provider
- if you change how you manage your contract or elements of it (for example, change from destruction by pulping to destruction by shredding)
- if you end the service by bringing it in-house

If offsite storage is currently operated by your organisation it may be worth conducting a DPIA to ensure current measures guard against risks to privacy. A DPIA is also evidence of due diligence, providing the outcomes are actioned.

Management of records when the minimum retention period is reached

5.1 OVERVIEW

This section covers the management of records once their business need has ceased and the minimum retention period has been reached. A detailed retention schedule is set out in Appendix II. This section includes information on the destruction and deletion of records, reviewing records for continued retention once their minimum period for retention has expired, and the selection of records for permanent preservation. It also includes information and advice about the transfer of records to Place of Deposits (PoD). Appendix I relating to public Inquiries should also be considered before destroying any records.

5.2 APPRAISAL

Appraisal is the process of deciding what to do with records once their business need has ceased and the minimum retention period has been reached. This can also be known as the disposition of records. The National Archives has produced guidance on appraisal.

Appraisal must be defined in a policy and any decisions must be documented and linked to a mandate to act (derived from the board). Any changes to the status of records must also be reflected in your organisation's Record of Processing Activity. In no circumstances should a record or series be automatically destroyed or deleted.

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

- **Ongoing use:** You might need to keep the record for longer than the minimum period for care, legal or audit reasons. In these cases, you can set an extension to the minimum period, provided it is justified and approved.
- **Classification of diseases (based on ICD10 code):** Some health conditions may lend themselves towards a longer, or extended, retention period.
- **Operational delivery:** The way a service was delivered may have been pioneering or innovative at the time, which may justify an extended retention period 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 the records are part of a series that will be added to (type of record rather than additional content into existing records), you need to consider space issues in your local records store or organisation archive. For example, continued expansion of a series that is hardly recalled would not justify an extension to the retention period.
- **Recall rates:** If a series of records is routinely accessed to retrieve records, then there may be justification for extending the retention period due to ongoing use. Whereas, for a series of records that has a very low recall rate, continued retention may 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 consider retaining for longer. It would also be helpful to have early discussions with your local PoD about potential accession, even if the record has ceased to be of operational value or use. PoDs will not normally accession records before 20 years retention has passed, unless there are exceptional circumstances for early transfer. The PoD must agree to the transfer PRIOR to it occurring. If early discussion with the PoD indicates the record (or series) will not be accessioned, and you have no ongoing operational use for the record or series, then you must securely destroy the record, and obtain evidence of destruction (for example, destruction certificate).
- **Previous deposits:** The records you hold may be a continuation of a series that has historically been accessioned by a local PoD. It is important to find out what has historically been accessioned from your organisation to the PoD, 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.

This list is not exhaustive, and organisations may have bespoke issues to consider as well.

Digital records can be appraised if they are:

- arranged in an organised filing system
- differentiated by the year of creation
- organised by year of closure
- clear about the subject of the record

If digital records have been organised in an effective file plan or an electronic record keeping system, this process will be made much 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 or delete
- continued retention – this will require justification and documented reasons
- permanent preservation

All appraisal decisions need to be justified, follow policy or guidance, and be documented and approved by the relevant board, committee or group of the organisation.

5.3 DESTROYING AND DELETING RECORDS

If as a result of appraisal, a decision is made to destroy or delete a record, there must be evidence of the decision. It is good practice to get authorisation for destruction or deletion from an appointed committee or group with a designated function to appraise records, working to a policy or guidelines. Where the destruction or deletion process is new, or there is a change in the destruction process (such as a change of provider, or the method used), a DPIA must be completed and signed off by the organisation.

Destruction of paper records

Paper records selected for destruction can be destroyed, subject to following ISO 15489-1:2016. Destruction can be conducted in-house or under contract with an approved offsite company. If an offsite company is used, the health or care organisation, as the controller, is responsible for ensuring the provider chosen to carry out offsite destruction meets the necessary requirements and can evidence this. This evidence should be checked as part of due diligence (for example, if the provider says they have the ISO accreditation, then check with the ISO). Other diligence activities, such as a site visit to the contractor, should also be carried out. Destruction provider companies must provide a certification of destruction for the bulk destruction of records. This certification must be linked to a list of records, so organisations have clear evidence that particular records have been destroyed.

Records that do not contain personal data or confidential material can be destroyed in a less secure manner (such as confidential waste bins that do not provide certificates of destruction). If in doubt, material should be treated as confidential and evidentially destroyed. Do not use the domestic waste or put records on a rubbish tip to destroy identifiable, confidential material, because they remain accessible to anyone who finds them. The British Security Industry Association (BSIA) has provided a guide on information destruction.

Destruction of digital records

Destruction implies a permanent action. For digital records ‘deletion’ may not meet the ISO 27001 standard as the information can or may be able to be recovered or reversed. Destruction of digital information is therefore more challenging. If an offsite company is used, the health and care organisation as the controller should check with the ISO whether the provider meets the necessary requirements, similar to the process for the destruction of paper records.

One element of records management is accounting for information, so any destruction of hardware, hard drives or storage media 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 ICO guidance Deleting personal data sets out that if information is deleted from a live environment and cannot be readily accessed, then this will suffice to remove information for the purposes of UK GDPR. Their advice is to only procure systems that will allow permanent deletion of records to allow compliance with the law.

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

If a system doesn't 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 it as a dormant or archived record. All activity in electronic systems must be auditable, and (where appropriate) local policies and procedures should cover archived digital records.

In relation to FOIA, the ICO guidance Determining whether information is held advises that once the appropriate limit for costs incurred for that FOI has been reached, there are no more requirements to recover information held. The only exemption to this would be where the organisation is instructed by a court order.

The following are examples of when information cannot be destroyed or disposed of:

- if it is subject to a form of access request, for example, Subject Access Request (SAR), FOIA request
- if it is required for notified legal proceedings, for example, a court order, or where there is reasonable prospect of legal proceedings commencing (an impending court case). This information will possibly be required for the exercising or defending of a legal right or claim
- if it is required for a coroner's inquest
- if it is of interest to a public inquiry, for example, who will issue guidance to organisations on what kind of records they may require as part of the inquiry. Once notified, organisations can re-commence disposal, taking into account what records are required by the inquiry. If in doubt, check with the Inquiry Team.

5.4 CONTINUED RETENTION

The retention periods given in Appendix II are the minimum periods for which records must be retained for health and care purposes. In most cases, it will be appropriate to dispose of records once this period has expired, unless the records have been selected for permanent preservation.

Organisations must have procedures and policies for any instances where it is necessary to maintain specifically identified individual records, or group of records (clinical or otherwise) for longer than the stated minimum, including:

- temporary retention
- public inquiries
- ongoing access request, for example, where the ongoing processing of an access request cuts over the minimum retention period. It would not be acceptable to dispose of a record that is part way through being processed for an access request because the minimum retention period has been reached.
- where there is a continued business need beyond the minimum retention period, and this is documented in local policy

There will be occasions where care specialties will create digital records that have different retention periods. For example, a radiology scan might need to be kept for the minimum of 8 years, and then destroyed as the record is no longer required. Yet a different image for a similar case may need to be kept for longer due to the nature of that particular case. In these situations, organisations can apply different retention times and this should be picked up at the review stage once the 8 years has expired.

Where records contain personal data, the decision to retain must comply with UK GDPR. Decisions for continued retention beyond the periods laid out in this Code must be recorded, made in accordance with formal policies and procedures by authorised staff and set a specific period for further review.

Generally, where there is justification, records may be retained locally from the minimum period set in this Code, for up to 20 years from the last date at which content was added.

NHS individual staff and patient records

For NHS individual staff and patient records that have a recommended retention period beyond 20 years (for example, maternity records), these can be retained for longer as specified in Appendix II, in this case for 25 years. The Secretary of State for Digital, Culture, Media and Sport has approved the retention of NHS individual staff and patient records up to 20 years where this is necessary for continued NHS operational use. This may be reflected in an extended retention period beyond 20 years being mandated by the Code (such as with the maternity records). Where organisations use this provision locally to retain records for longer than 20 years, this must be documented in published policies.

It must be remembered that in some cases of health and social care, there may be gaps between episodes of care. If a patient or service user begins a new episode of care whilst their previous record is still within agreed retention periods, then these episodes of care will link, and the retention period will begin again at the end of the current episode. This may mean that some or all of the information from the previous episode will go over a 20-year retention mark, but this is acceptable as it links to a more recent care episode.

Other types of records

For records that are not staff or patient records, for example, board minutes or records relating to buildings, a different arrangement is in place. Where an organisation needs to keep any other type of record beyond 20 years, then approval must be sought separately from the Secretary of State for Digital, Culture, Media and Sport.

This is the case even where the recommended retention period is longer in the Code. The Code does not recommend a minimum retention period beyond 20 years for the majority of these types of records. However asbestos, radiation and some building records have longer retention periods due to current legislation at the time of writing. We are progressing an application to the Advisory Council for these three types of records. Organisations should retain them for the retention period set out in the Code at this time. We will update the Code with the outcome of that application in autumn 2021.

Organisations should always check current legislation. Any applications for approval should be made to The National Archives in the first instance (asd@nationalarchives.gov.uk).

Examples of the application of Secretary of State (SoS) retention approval

1. A trust wishes to check the retention period for cancer/oncology records. The Code states 30 years so the records are retained for 20 years without the need to apply the SoS approval. The last 10 years would be covered by SoS approval as they relate to individual patients, providing the trust has an ongoing need and justification for continued storage.
2. A trust wishes to retain patient records for 16 years due to developments in the treatment of infectious diseases (where a patient is cared for in an isolation ward). The Code recommends eight years before disposal. The trust can make a local decision to retain the records for 16 years. This does not need SoS approval because the period is under 20 years. The decision is documented in the trust's published policy. The trust notes that retention beyond 20 years for these records would utilise the SoS retention approval, subject to ongoing business need and justification of the proposed extended retention period.

5.5 RECORDS FOR PERMANENT PRESERVATION

The Public Records Act 1958 requires organisations to select records for permanent preservation. Selection for transfer under this Act is separate to the operational review of records to support current service provision. It is designed to ensure the permanent preservation of a small core (typically 2-5%) of key records, which will:

- enable the public to understand the working of the organisation and its impact on the population it serves
- preserve information and evidence likely to have long-term research or archival value

Records for preservation must be selected in accordance with the guidance contained in this Code. Any supplementary guidance issued by The National Archives and local guidance from the relevant PoD should always be consulted in advance of any possible accession. This is to ensure it is appropriate to transfer the records selected. As a rule, national organisations, such as NHS England, will accession their records to The National Archives, and local NHS and social care

organisations will accession their records to the local PoD, as appointed by the Secretary of State for Culture, Media and Sport.

Selection may take place at any time in advance of transfer. However, the selection and transfer must take place at or before records are 20 years old. Records may be selected as a class (for example, all board minutes) or at lower levels down to individual files or items.

Records can be categorised as follows:

- transfer to PoD - this class of records should normally transfer in its entirety to the PoD – trivial or duplicate items can be removed prior to transfer
- consider transfer to PoD - all, some or none of this class may be selected (as agreed with the PoD)
- no PoD interest

Other records should not normally be selected for transfer. Whilst there may be occasions where records to support research are transferred (for example, to support research into rare conditions), records should not be transferred just because they relate to research or with the sole purpose of preservation in case they could be used for future research. The Public Records Act 1958 is not designed to support the routine archival of research records. Records should not be transferred unless they specifically meet the criteria below. If in doubt, it is recommended to check with the local PoD.

Where it is known that particular records will be transferred to PoDs routinely, this should be noted in the records management policy (or equivalent) alongside the reason for the routine transfer. Likewise, one-off transfers should also be noted for reference. It is not practical to update local policies each time a transfer is made. If a particular type becomes a regular transfer, this could be added to the next update of the records management policy. It may be sufficient to publish a link to the PoD's public catalogue or The National Archives Discovery Catalogue to which data for transferred records is added annually. Where it is known a record will form part of the public record at creation, it must be preserved locally until such time it can be transferred. PoDs will know which types of records they will always take (such as board minutes). The National Archives is working on providing guidance on which record will always be transferred and those that might be of local interest.

The Tavistock and Portman NHS Foundation Trust has a policy for the selection of material for permanent preservation: a method for selecting the works of eminent clinicians' work and a panel for selecting historical records. Where a clinician has amassed a lifetime of research or important cases these may be identified and retained.

Patient or service user records for permanent preservation

Records of individual persons may also be selected and transferred to the PoD provided this is necessary and proportionate in relation to the broadly historical purposes of the Public Records Act 1958 and PoD agreement. For example, individual patient files relating to a hospital that is now closed and the files are coming to the end of their retention. In West Yorkshire, a hospital, which opened in 1919, closed in 1995 and in 2011 patient files were still being transferred to the local PoD to finish the series. All patient records for the hospital are now at the PoD.

Patient or service user confidentiality will normally prevent use for many decades after transfer and the physical resource will be substantial (for example, x number of archive boxes) therefore the transfer of patient or service users records should only be considered where one or more of the factors listed below apply:

- the organisation has an unusually long or complete run of records of a given type
- the records relate to population or environmental factors peculiar to the locality
- the records are likely to support research into rare or long-term conditions
- the records relate to an event or issue of significant local or national importance
- the records relate to the development of new or unusual treatments or approaches to care, or the organisation is recognised as a national or international leader in the field of medicine or care concerned
- the records throw particular light on the functioning, or failure, of the organisation, or the NHS or social care in general
- the records relate to a significant piece of published research

Any policy to select patient or service user records should only be agreed after consultation with appropriate clinicians, the group or committee responsible for records management and (if necessary), the Caldicott Guardian. This decision, and the reasoning behind the decision, should be published in the minutes

of the meeting at which this decision is taken. Routine transfers of patient or service user records to a PoD can be included in the records management policy of the organisation or its equivalent.

Any records selected should normally be retained within the NHS or social care (under the terms of Retention Instrument 122) until the patient or service user is deceased, or reasonably assumed to be so and then can subsequently be transferred. Records no longer required for current service provision may be temporarily retained pending transfer to a PoD. Records containing sensitive or confidential information should not normally be transferred early, unless in agreement with the PoD. If a patient or service user expresses a wish that they do not want their health or care record transferred to a PoD, this must be respected unless the transfer is required by law.

Transfers of records to the Place of Deposit

Records selected for permanent preservation should be transferred to the relevant PoD appointed by the Secretary of State for Digital, Culture, Media and Sport. PoDs are usually public archive services provided by the relevant local authority. Current contact details of PoDs and the organisations which should transfer to them can be found on The National Archives website. As a general rule, national public sector organisations will deposit with The National Archives, while local organisations will deposit with a local PoD. For example, NHS England will deposit with The National Archives, whereas a local NHS body or local authority will deposit with the local PoD. This could be the county record office, or a specialised facility run by local authorities for the county.

There will be a mandatory requirement to transfer some types of records whereas others will be subject to local agreement. The retention schedule included with this Code identifies records which should be transferred to the locally approved PoD when business use has ceased. There may also be records of local interest which need to be accessioned to the PoD (such as a continuation of a series already accessioned). Prior to any transfer being made, a discussion must be had with the local PoD to enable agreement on which records will be transferred and the process for doing so. (Also refer to Appendix I, which provides information about public inquiries that may impact upon the selection of records for transfer).

Transferred records should be in good condition and appropriately packed, listed and reviewed for any FOIA exemptions. Records selected for transfer to a PoD (after appraisal) may continue to be exempt from public access for a specified period after transfer in accordance with Section 66 of FOIA. For more detail on the transfer process and sensitivity review refer to The National Archives guidance.

Requests to access records held in the Place of Deposit (PoD)

Once transferred to the PoD, records will still be owned by the organisation transferring them and all relevant laws will apply. Individual records deposited with PoDs are still protected by the UK GDPR, FOIA and duty of confidentiality. Where records are kept for permanent preservation for reasons other than care, consideration should be given to preserving the records in an anonymised way to protect confidentiality. Where this is not possible, then consider removing as many identifiers as possible. If you are looking to preserve a record because the treatment provided was innovative or highlights new ways of working, then the identity of the patient is not required. For individual care, it would be required, as the record may need to be retrieved.

Where a local PoD holds records and access is requested, the PoD will liaise with the depositing organisation before releasing any information (including any checks for SARs required by UK GDPR and any exemptions under FOIA). This allows for a check for any harmful information that may be in the record or if there are other grounds on which to withhold the record. Where a public interest test is required, the transferring organisation must carry this out and inform the PoD of the result. The depositing organisation must make a decision on what information to release and where information is withheld, explain the reason why (except in exceptional circumstances, for example, a court order to the PoD).

Unless there are exceptional circumstances, PoDs will not normally continue to apply FOI exemptions to records more than 100 years old.

Where a patient or service user has died the UK GDPR no longer applies but FOIA applies regardless as to whether the individual is alive or not. The Section 41 (confidence) exemption of FOIA and the duty of confidence remain relevant so records cannot be accessed by anyone who does not have a lawful basis to view a record. FOIA decisions indicate that, in general, health and social care information will remain confidential after death.

The duty of confidence does diminish over time, but it is recommended that at least 10 years should have passed after a person's death before reviewing the consequences of relaxing disclosure controls on information about a person previously regarded as confidential. This review should consider the potential harm or distress to surviving family members of disclosing information that might be regarded as particularly sensitive or likely to attract publicity, and the risks that the disclosure might undermine public trust in the health and care system. When a person is deceased, the Access to Health Records Act 1990 may enable access to the health record for a limited purpose by specified individuals (such as those with a claim arising out of the death of the person).

Appendix I: Public and Statutory Inquiries

Records form an important part of the evidence in inquiries. Inquiries take into account a huge range of records and what is required can vary by inquiry. When an inquiry is conducted, the Inquiry Team will issue detailed guidance setting out what types of records they are interested in. If you have any records that an inquiry requests, you must produce them or explain why you cannot produce them.

Before any records relating to inquiries are destroyed, you must check with the Inquiries Team that they are no longer required. If you are in doubt regarding records that may or may not be of use for an inquiry, you must retain them until there is clear instruction from the inquiry.

Before considering the selection of records for permanent preservation under the Public Records Act 1958 (refer to section 5), you should discuss any inquiries with the relevant PoD to take account of exceptional local circumstances and defunct record types not listed here.

At the time of writing there are two independent Inquiries which have requested that large parts of the health and social care sector do not destroy any records that are, or may fall into the remit of the Inquiry:

- The Independent Inquiry into Child Sexual Abuse (IICSA) - this is due to finish in 2022. Records that should not be destroyed include children's records and any instances of allegations or investigations or any records of an institution where abuse has or may have occurred
- The Infected Blood Inquiry - further information about the records required can be found on their website

The Government has also committed to holding a public inquiry into its response to the coronavirus pandemic that began in March 2020. No details of what records will be required are known at this stage, but it is likely to require records relating to policy and decision making as a minimum.

Appendix II: Retention schedule

This Appendix sets out the retention period for different types of records relating to health and care. Where indicated, Appendix III should also be referred to. This sets out further detail relating to the management of specific types and formats of records.

The following information is important to ensure the retention schedule is used correctly.

The retention periods listed in this retention schedule must always be considered the **minimum period.** With justification, a retention period can be extended for the majority of cases, up to 20 years (refer to section five of the Code). For more information, refer to R v Northumberland County Council and the Information Commissioner (23 July 2015). This provides assurance that it is legitimate to vary common practice or guidance where a well-reasoned case for doing so is made.

Retention periods begin when the record ceases to be operational. This is usually at the point of discharge from care when the record is no longer required for current on-going business, or the patient or service user has died. There are some exceptions to this rule, whereby the retention begins from the date the record is created (for corporate records, such as policies, the retention may start from the date of publication). These are marked with an asterisk (*) in the schedule and may also contain further information in the notes for that entry.

If a record comes back into use during its retention period, then the retention period will reset and begin again from the end of the second period of use. This may mean that records will look as if they are being kept for longer than the retention times stated here, or even maximum periods as suggested by law, but this is acceptable where retention periods reset due to use (refer to section five of the Code).

The actions following review as set out in the schedule are as follows:

- **Review and destroy if no longer required:** Destroy refers to the confidential and secure destruction of the record with proof of destruction. These will be records with no archival value and there is no longer an ongoing business need to retain them for longer.
- **Review and dispose of if no longer required:** 'Dispose of' refers to the secure destruction of a record OR the transferral to the appointed PoD for permanent preservation. A certificate of transfer will be provided as proof of transfer (and can act as evidence of disposal). Refer to section five of the Code for further information about permanent preservation.

- **Review and consider transfer to PoD:** This refers to records that are more likely to be transferred to the PoD, subject to their discussion and agreement about potential accession. Not all records considered for accession will be taken by the PoD. If the record has been offered and declined to be taken, and it has no further retention value, then it must be securely destroyed. Where you have potentially a new series of records for the PoD, you must discuss accessioning them before any action is taken.
- **Review and transfer to PoD:** This refers to records that should be transferred to the PoD such as trust board minutes and final annual financial report - local agreement will already be in place to accession these.

It is very important that any health and care records are reviewed before they are destroyed. This review should take into account:

- serious incidents which will require records to be retained for up to 20 years as set out in the schedule
- use of the record during the retention period which could extend its retention
- potential for long-term archival preservation - this may particularly be the case where the records relate to rare conditions such as Creutzfeldt-Jakob Disease records or innovative treatments, for example, new cancer treatments

If setting a retention period not covered by this Code, there are a number of factors to consider including:

- **Legal or regulatory obligations:** There may be a specific legal or regulatory reason to keep a record, which may also provide guidance on how long that record needs to be kept to meet that obligation.
- **Purpose of the record:** The reasons you have created the record may also help define how long you need to keep them for. A record created for medico-legal reasons may need to be for a long period of time, whereas a record created for a specific event that has no post-event actions will attract a short retention period.
- **Number of records:** The number of records in a series can help you set a retention period. It is worth noting that the number of records is not directly proportionate to a longer retention period (for example, the more records created, then the longer they must be kept). It should also be noted that the number of records is also not indicative of historical value. Due to its type, one record may have historical value, where a series of 200+ records might not.
- **Service delivery:** The uniqueness or niche way a service is delivered may lend itself to a longer retention period. PoDs can be interested in taking records relating to services that were delivered in a unique way.
- **Call or recall of records:** If a record or series has a low recall rate, it could be indicative of a shorter retention period. Likewise records that are continually in use may require a longer retention period.

The above list is not exhaustive.

CARE RECORDS

Record Type	Retention Period	Disposal Action	Notes
Adult health records not covered by any other section in this schedule (includes medical illustration records such as x-rays and scans as well as video and other formats. Also includes care plans)	8 years	Review and consider transfer to PoD	Records involving pioneering or innovative treatment may have archival value, and their long term preservation should be discussed with the local PoD or The National Archives. Also refer to Appendix III: ambulance service records.
Adult social care records (including care plans)	8 years	Review and destroy if no longer required	

Record Type	Retention Period	Disposal Action	Notes
Children's records (including midwifery, health visiting and school nursing) - can include medical illustrations, as well as video and audio formats	Up to 25th or 26th birthday	Review and destroy if no longer required	Retain until 25th birthday, or 26th if the patient was 17 when treatment ended.
Clinical records that pre-date the NHS (July 1948)		Review and transfer to PoD	Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed.
Dental records - clinical care records	15 years	Review, and destroy if no longer required	Based on Limitations Act 1980. This applies to all dental care settings and the BSA. This also includes FP17 or FP17O forms.
Dental records - finance related	2 years	Review, and destroy if no longer required	These include PR forms. NHS BSA may retain financial records for a minimum of 6 years.

Record Type	Retention Period	Disposal Action	Notes
Electronic Patient Record Systems (EPR)	Refer to notes	Review and destroy if no longer required	Where the system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain, demonstrating the destruction, then the Code should be followed in the same way for digital as well as paper records with a log kept of destruction. If the EPR does not have this capacity, then once records reach the end of their retention period, they should be made inaccessible to system users upon decommissioning. The system (along with the audit trails) should be retained for the retention period of the last entry related to the schedule.
GP patient records - deceased patients	10 years	Review and destroy if no longer required	Confidentiality generally continues after death and records should be retained for medico-legal and possible public interest (for example, research) reasons. Review retention after 10 years when possible medico-legal reasons will lapse under requirements of the Limitation Act 1980. Destroy if the record holds no value for researchers. Also refer to Appendix III: GP records.

Record Type	Retention Period	Disposal Action	Notes
GP patient records – living patients	Continual retention		If the patient has not been seen for 10 years, or a request for transfer to a new GP has not been received, the GP practice should check the Personal Demographics Service (PDS) for indication of death or other reason for no contact. If there is no reason to suggest no contact, then the record must be kept by the GP practice. If they have died, or transferred to a new practice, transfer the record to NHSE or the new provider respectively. These records cannot be disposed of as they may require further services as they get older. Also refer to Appendix III: GP records

Record Type	Retention Period	Disposal Action	Notes
GP patient records – de-registered cases where the reason is unknown	100 years	Review and dispose of if no longer required	These are cases where the patient has de-registered from the practice, but the reason is unknown. It would be good practice for GPs to check if there is a reason for de-registration (death, missed registration at another practice, emigration etc.). It is not suggested that a retrospective check be carried out, but it would be good practice going forward to conduct a check for these cases. Once checked under General Medical Services (GMS) regulations, records should be sent to NHSE via Primary Care Support England (PCSE) operational processes. Also refer to Appendix III: GP records

Record Type	Retention Period	Disposal Action	Notes
GP patient registrations form	6 years after the year of registration	Review and dispose of if no longer required	These need to be kept for 6 years as GP per capita payments are made based on registered patient numbers. Most GP practices scan the form into the patient's electronic record once it is created. The paper form can be destroyed securely once the minimum retention period has been reached, unless there is another reason to keep the form longer (this would be identified at the review stage).
Integrated records – all organisations contribute to the same single instance of the record	Retain for period of longest specialty	Review and consider transfer to PoD	The retention time will vary depending upon which type of health and care settings have contributed to the record. Areas that use this model must have a way of identifying the longest retention period applicable to the record.
Integrated records – all organisations contribute to the same record, but keep a level of separation (refer to notes)	Retain for relevant specialty period	Review and consider transfer to PoD	This is where all organisations contribute into the same record system but have their own area to contribute to and the system still shows a contemporaneous view of the patient record.
Integrated records – all organisations keep their own records, but enable them to be viewed by other organisations	Retain for relevant specialty period	Review and consider transfer to PoD	This is the most likely model currently in use. Organisations keep their own records on their patients or service users but can grant 'view only' access to other organisations, to help them provide health and care to patients or service users.
Mental health records including psychology records	20 years, or 10 years after death	Review and consider transfer to PoD	Covers records made under the Mental Health Act (MHA) 1983 (and 2007 amendments). Records retained solely for any person who has been sectioned under MHA1983 must be considered for longer than 20 years where the case is ongoing, or the potential for recurrence is high (based on local clinical judgment). This applies to records of patients or service users, regardless of whether they have capacity or not.
Obstetrics, maternity, antenatal and postnatal records	25 years	Review and destroy if no longer required	For record keeping purposes, these are considered to be as much the child's record as the parent, so the longer retention period should be considered.

Record Type	Retention Period	Disposal Action	Notes
Prison health records	10 years	Review and destroy if no longer required	A summary of their prison healthcare is sent to the person's new GP upon release and the record should be considered closed at the point of release. These records are unlikely to have long term archival value and should be retained by the organisations providing care in the prison, or successor organisations if the running of the service changes hands.
Cancer/oncology records – any patient*	30 years, or 8 years after death	Review and consider transfer to PoD	Retention for these records begins at diagnosis rather than the end of operational use. For clinical care reasons, these records must be retained longer in case of re-occurrence. Where the oncology record is part of the main records, then the entire record must be retained.
Contraception, sexual health, family planning, Genito-Urinary Medicine (GUM)	8 or 10 years	Review and destroy if no longer required	8 years for the basic retention requirement but this is increased to 10 in cases of implants or medical devices. If the record relates to a child, then retain in line with children's records. (Also refer to Appendix III: records dealt with under the NHS Trusts and Primary Care Trusts (Sexually transmitted disease) directions 2000).
Creutzfeldt-Jakob Disease – patient records	30 years or 10 years after death	Review and consider transfer to PoD	Diagnosis records must be retained for clinical care purposes.
Human Fertility and Embryology Authority (HFEA) records – treatment provided in licenced centres	3,10, 30 or 50 years	Review and destroy if no longer required	These retention periods are set out in HFEA guidance.
Long-term illness, or illness that may reoccur – patient records	20 years, or 10 years after death	Review and destroy if no longer required	Necessary for continuation of clinical care. The primary record of the illness and course of treatment must be kept where the illness may reoccur or it is a life-long condition such as diabetes, arthritis or Chronic Obstructive Pulmonary Disease.

Record Type	Retention Period	Disposal Action	Notes
Sexual Assault Referral Centres (SARC)	30 years, or 10 years after death (if known)	Review, and destroy if no longer required	These records need to be kept for medico-legal reasons because an individual may not be in a position to bring a case against the alleged perpetrator for a long time after the event. Once the retention period is reached, a decision needs to be made about continued retention. Records cannot be kept indefinitely just in case an individual might bring a case. Some individuals may never bring a case and indefinite retention may be seen as a breach of UK GDPR (keeping information longer than necessary). Consideration also needs to be given to the Police and Criminal Evidence Act 1984, Human Tissue Act 2004, and Criminal Procedure and Investigations Act 1996 legal requirements (other laws and regulations may also need to be taken into account).

PHARMACY

Record Type	Retention Period	Disposal Action	Notes
Controlled drugs - registers	2 years, (refer to notes)	Review and destroy if no longer required	Misuse of Drugs Act 2001. NHS England has issued guidance in relation to controlled drugs. Also refer to Appendix III: controlled drugs
Controlled drugs - order books, requisitions etc	2 years	Review, and destroy if no longer required	Misuse of Drugs Act 2001.
Pharmacy prescription records	2 years	Review and destroy if no longer required	A record of the prescription will also be held by NHS BSA and there will be an entry on the patient record. Further advice and guidance on pharmacy records can be found on the Specialist Pharmacy Service website.

PATHOLOGY

Record Type	Retention Period	Disposal Action	Notes
Pathology reports, information about samples	Refer to notes	Review and consider transfer to PoD	This Code is concerned with the information about a specimen or sample. The length of time clinical material (for example, a specimen) is stored will drive how long the information relating to it is retained. Sample retention can be for as long as there is a clinical need to hold it. Reports should be stored on the patient file. It is common for pathologists to hold duplicate records. For clinical purposes, these should be retained for eight years after discharge or until a child's 25th birthday. If information is retained for 20 years, it must be appraised for historical value, and a decision made about its disposal. Also refer to Appendix III: specimens and samples

EVENT AND TRANSACTION RECORDS

Record Type	Retention Period	Disposal Action	Notes
Blood bank register*	30 years minimum	Review and consider transfer to PoD	Need to be disposed of if there is no on-going need to retain them (such as the currently ongoing Infected Blood Inquiry), subject to any transfer to the PoD.
Clinical audit*	5 years	Review and destroy if no longer required	Five years from the year in which the audit was conducted. This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period, for example, data from adult health records would be kept for 8 years.
Chaplaincy records*	2 years	Review and consider transfer to PoD	Also refer to corporate governance records.
Clinical diaries	2 years	Review and destroy if no longer required	Two years after the year to which they relate. Diaries of clinical activity and visits must be written up and transferred to the main patient record. If the information is not transferred from the diary (so the only record of the event is in the diary), then this must be retained for eight years and reviewed. Some staff keep hardback diaries of their appointments or business meetings. If these contain no personal data, they can be disposed of after two years.

Record Type	Retention Period	Disposal Action	Notes
Clinical protocols*	20 years	Review and consider transfer to PoD	Clinical protocols may have preservational value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (refer to corporate governance records).
Datasets released by NHS Digital and its predecessors	Delete with immediate effect	Delete in line with NHS Digital instructions	NHS Digital issue guidance through the Data Access Request Service (DARS) process on the retention and disposal of data released by them.
Destruction certificates, or electronic metadata destruction stub, or record of clinical information held on physical media	20 years	Review and consider transfer to PoD	Destruction certificates created by public bodies are not covered by a retention instrument (if they do not relate to patient care and if a PoD or The National Archives do not accession them). They need to be destroyed after 20 years.
Equipment maintenance logs	11 years	Review and destroy and no longer required	
General ophthalmic services – patient records related to NHS financial transactions	6 years	Review and destroy if no longer required	
GP temporary resident forms	2 years	Review and destroy if no longer required	This assumes a copy has been sent to the responsible GP for inclusion in the GP patient record.
Inspection of equipment records	11 years	Review and destroy if no longer required	
Notifiable diseases book*	6 years	Review and destroy if no longer required	
Operating theatre records	10 years	Review and consider transfer to PoD	10 years from the end of the year to which they relate.
Patient property books	2 years	Review and destroy if no longer required	Two years from the end of the year to which they relate.
Referrals – NOT ACCEPTED	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record.

Record Type	Retention Period	Disposal Action	Notes
Requests for care funding – NOT ACCEPTED	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record. NB: These may have potential PoD interest as what the NHS or social care can or cannot fund can sometimes be an issue of local or national significance and public debate. Refer to Appendix III: individual funding requests
Screening* – including cervical screening – where no cancer or illness detected is returned	10 years	Review and destroy if no longer required	Where cancer is detected, refer to the cancer/oncology schedule.
Screening – children	10 years or 25th birthday	Review and destroy if no longer required	Treat as a child health record and retain for either 10 years or up to 25th birthday, whichever is the LONGER.
Smoking cessation	2 years	Review and destroy if no longer required	Retention begins at the end of the 12-week quit period.
Transplantation records*	30 years	Review and consider transfer to PoD	Refer to guidance issued by the Human Tissue Authority.
Ward handover sheets*	2 years	Review and destroy if no longer required	This information relates to the ward. Any individual sheets held by staff may be destroyed confidentially at the end of the shift.

TELEPHONY SYSTEMS AND SERVICES

This is related to 111 or 999 phone calls or services, Ambulance, out of hours, and single point of contact call centres.

Record Type	Retention Period	Disposal Action	Notes
Recorded conversations – which may be needed later for clinical negligence or other legal purposes*	6 years	Review and destroy if no longer required	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980. Further guidance is issued by NHS Resolution.
Recorded conversations – which form part of the health record*	Treat as a health record	Review and destroy if no longer required	It is advisable to transfer any relevant information into the main record, through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record, the recording must be considered as part of the record and be retained accordingly.
Telephony systems record*	1 year	Review and destroy if no longer required	This is the minimum specified to meet NHS contractual requirements.

BIRTHS, DEATHS AND ADOPTION RECORDS

Record Type	Retention Period	Disposal Action	Notes
Birth notification to child health	25 years	Review and destroy if no longer required	Retention begins when the notification is received by the child health department. Treat as part of the child's health record if not already stored within the health record.
Birth registers*	2 years	Review and consider transfer to PoD	Where registers of all births that have taken place in a particular hospital or birth centre exist, these will have archival value and should be retained for 25 years and offered to the local PoD at the end of the retention period. Information is also held by the NHS Birth Notification Service electronic system, and by ONS. Other information about a birth must be recorded in the care record.
Body release forms*	2 years	Review and destroy if no longer required	

Record Type	Retention Period	Disposal Action	Notes
Death – cause of death certificate counterfoil*	2 years	Review and destroy if no longer required	These detail the name of the deceased and suspected cause of death (which initially may be different to the final cause of death as stated on the official death certificate). A death notification certificate is issued if a doctor is satisfied there is no suspicious or unexpected circumstances surrounding the death, and the counterfoil retained by the setting that issued the initial cause of death certificate (which is used to obtain the full death certificate from a registrar of births, death and marriages). Cases referred to the coroner would not be able to issue a certificate as the cause would be unknown. These are unlikely to have archival value.
Death - register information sent to the general registry office on a monthly basis*	2 years	Review and consider transfer to PoD	A full dataset is available from ONS.
Local authority adoption record (usually held by the LA)*	100 years	Review and consider transfer to PoD	The local authority Children's Social Care Team hold the primary record of the adoption process. Consider transferring to PoD only if there are known gaps in the primary local authority record, or the records pre-date 1976. Also refer to Appendix III: adoption records
Mortuary records of deceased persons	10 years	Review and consider transfer to PoD	Retention begins at the end of the year to which they relate.
Mortuary register*	10 years	Review and consider transfer to PoD	
NHS medicals for adoption records*	8 years or 25th birthday	Review and consider transfer to PoD	The health reports will feed into the primary record held by the local authority. This means that adoption records held in the NHS relate to reports that are already kept in another file, which is kept for 100 years by the relevant agency or local authority. Consider transferring to PoD only if there are known gaps in the primary local authority record or the records pre-date 1976. Also refer to Appendix III: adopted persons health records
Post-mortem records*	10 years	Review and destroy if no longer required	The coroner will maintain and retain the primary post-mortem file including the report. Hospital post-mortem records will not need to be kept for the same extended time period as (subject to local policy) these reports may also be kept in the medical file.

CLINICAL TRIALS AND RESEARCH

Record Type	Retention Period	Disposal Action	Notes
Advanced medical therapy research - master file	20 years	Review and consider transfer to PoD	
Clinical trials – applications for ethical approval	5 years	Review and consider transfer to PoD	Master file of a trial authorised under the European portal, under Regulation 536/2014. For clinical trials records retention refer to the MHRA guidance. The sponsor of the study will be the primary holder of the study file and associated data. This is based on the Medicines for Human Use (Clinical Trials) Amendment Regulations 2006 (specifically Regulations 18 and 28).
European Commission Authorisation (certificate or letter) to enable marketing and sale within EU member state's area	15 years	Review and consider transfer to PoD	
Research - datasets	No longer than 20 years	Review and consider transfer to PoD	
Research – ethics committee's and HRA approval documentation for research proposal and records to process patient information without consent	5 years	Review and consider transfer to PoD	This applies to trials where opinions are given to proceed with the trial, or not to proceed. These may also have archival value.
Research – ethics committee's minutes (including records to process patient information without consent)	20 years	Review and consider transfer to PoD	Retention period begins from the year to which they relate and can be as long as 20 years. Committee minutes must be transferred to PoD.

CORPORATE GOVERNANCE

Record Type	Retention Period	Disposal Action	Notes
Board meetings*	Up to 20 years	Review and transfer to PoD	A local decision can be made on how long to retain the minutes of board meetings (and associated papers linked to the board meeting), but this must not exceed 20 years, and will be required to be transferred to the local PoD or The National Archives (for National Bodies).
Board meetings (closed boards)*	Up to 20 years	Review and transfer to PoD	Although these may still contain confidential or sensitive material, they are still a public record and must be transferred at 20 years, and any FOI exemptions noted, or indications that the duty of confidentiality applies.
Chief Executive records*	Up to 20 years	Review and transfer to PoD	This may include emails and correspondence where they are not already included in board papers.
Committees (major) – listed in Scheme of delegation or report direct into the board (including major projects)*	Up to 20 years	Review and transfer to PoD	
Committees (minor) – not listed in scheme of delegation*	6 years	Review and consider transfer to PoD	Includes minor meetings, projects, and departmental business meetings. These may have local historical value and require transfer consideration.
Corporate records of health and care organisations and providers that pre-date the NHS (July 1948)		Review, and transfer to PoD	Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed. An example might be the minutes of the hospital board from 1932, or midwifery diaries dated Dec 1922.
Data Protection Impact Assessments (DPIAs)	6 years	Review and destroy if no longer required	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one -off, then 6 years from completion.
Destruction certificates or record of information held on destroyed physical media	20 years	Review and dispose of if no longer required	Where a record is listed for potential transfer to PoD have been destroyed without adequate appraisal, consideration should be given to a selection of these as an indicator of what has not been preserved.
Electronic metadata destruction stubs			Refer to destruction certificates.
Incidents – serious	20 years	Review and consider transfer to PoD	Retention begins from the date of the Incident – not when the incident was reported.

Record Type	Retention Period	Disposal Action	Notes
Incidents – not serious	10 years	Review and destroy if no longer required	Retention begins from the date of the incident – not when the incident was reported.
Incidents – serious incidents requiring investigation	20 years	Review and consider transfer to PoD	These include independent investigations into incidents. These may have permanent retention value so consult with the local PoD. If they are not required, then destroy.
Non-clinical QA records	12 years	Review and destroy if no longer required	Retention begins from the end of the year to which the assurance relates.
Patient advice and liaison service (PALS) records	10 years	Review and destroy if no longer required	Retention begins from the close of the financial year to which the record relates.
Patient surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	May be required again if analysis is reviewed.
Patient surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.

Record Type	Retention Period	Disposal Action	Notes
Policies, strategies and operating procedures – including business plans*	Life of organisation plus 6 years	Review and consider transfer to PoD	Retention begins from when the document is approved, until superseded. If the retention period reaches 20 years from the date of approval, then consider transfer to PoD.
Quarterly reviews from NHS trusts	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.
Risk registers	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act and corporate awareness of risks.
Staff surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	Forms are anonymous so do not contain PID unless provided in free text boxes. May be required again if analysis is reviewed.
Staff surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
Trust submission forms	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.

COMMUNICATIONS

Record Type	Retention Period	Disposal Action	Notes
Intranet site*	6 years	Review and consider transfer to PoD	
Patient information leaflets	6 years	Review and consider transfer to PoD	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.
Press releases and important internal communications	6 years	Review and consider transfer to PoD	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.
Public consultations	5 years	Review and consider transfer to PoD	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation (particularly where this resulted in changes to the services provided) and so may have historical value.
Website*	6 years	Review and consider transfer to PoD	The PoD may be able to receive these by a regular crawl. Consult with the PoD on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken.

STAFF RECORDS AND OCCUPATIONAL HEALTH

Record Type	Retention Period	Disposal Action	Notes
Duty roster	6 years	Review and if no longer needed destroy	Retention begins from the close of the financial year.
Exposure monitoring information	40 years or 5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Occupational health reports	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	
Occupational health report of staff member under health surveillance	Keep until 75th birthday	Review and if no longer needed destroy	
Occupational health report of staff member under health surveillance where they have been subject to radiation doses	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	

Record Type	Retention Period	Disposal Action	Notes
Staff record	Keep until 75th birthday (see notes)	Review, and consider transfer to PoD	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. Some PoDs accession NHS staff records for social history purposes. Check with your local PoD about possible accession. If the PoD does not accession them, then the records can be securely destroyed once the retention period has been reached.
Staff record - summary	75th Birthday	Review, and consider transfer to PoD	Please see the good practice box staff record summary used by an organisation. Some organisations create summaries after a period of time since the staff member left (usually 6 years). This practice is ok to continue if this is what currently occurs. The summary, however, needs to be kept until the staff member's 75th birthday, and then consider transferring to PoD. If the PoD does not require them, then they can be securely destroyed at this point.
Timesheets (original record)	2 years	Review and if no longer needed destroy	Retention begins from creation.
Staff training records	See notes	Review and consider transfer to a PoD	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The following is recommended: **clinical training records** - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer **statutory and mandatory training records** - to be kept for ten years after training completed **other training records** - keep for six years after training completed
Disciplinary records	Retain for 6 years	Review and destroy if no longer required	Retention begins once the case is heard and any appeal process completed. The record may be retained for longer, but this will be a local decision based on the facts of the case. The more serious the case, the more likely it will attract a longer retention period. Likewise, a one-off incident may need to only be kept for the minimum time stated. This applies to all cases, regardless of format.

PROCUREMENT

Record Type	Retention Period	Disposal Action	Notes
Contracts sealed or unsealed	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
Contracts - financial approval files	Retain for 15 years after the end of the contract	Review and if no longer needed destroy	
Contracts - financial approved suppliers documentation	Retain for 11 years after the end of the contract	Review and if no longer needed destroy	
Tenders (successful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
Tenders (unsuccessful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	

ESTATES

Record Type	Retention Period	Disposal Action	Notes
Building plans, including records of major building works	Lifetime (or disposal) of building plus 6 years	Review and consider transfer to PoD	Building plans and records of works are potentially of historical interest and where possible, should be kept and transferred to the local PoD.
Closed circuit television (CCTV)	Refer to ICO Code of Practice	Review and destroy if no longer required	The length of retention must be determined by the purpose for which the CCTV has been used. CCTV footage must remain viewable for the length of time it is retained, and where possible, systems should have redaction or censoring functionality to be able to blank out the faces of people who are captured by the CCTV, but not subject to the access request, for example, police reviewing CCTV as part of an investigation.
Equipment monitoring, and testing and maintenance work where ASBESTOS is a factor	40 years	Review and destroy if no longer required	Retention begins from the completion of the monitoring or testing. This includes records of air monitoring and health records relating to asbestos exposure, as required by the Control of Asbestos Regulations 2012.
Equipment monitoring – general testing and maintenance work	Lifetime of installation	Review and destroy if no longer required	Retention begins from the completion of the testing and maintenance.
Inspection reports	Lifetime of installation	Review and dispose of if no longer required	Retention begins at the END of the installation period. Building inspection records need to comply with the Construction (Design and Management) Regulations 2015.

Record Type	Retention Period	Disposal Action	Notes
Leases	12 years	Review and destroy if no longer required	Retention begins at point of lease termination.
Minor building works	6 years	Review and destroy if no longer required	Retention begins at the point of WORKS COMPLETION.
Photographic collections – service locations, events and activities	Up to 20 years	Review and consider transfer to PoD	These provide a visual historical legacy of the running and operation of an organisation. They may also provide secondary uses, such as use in public inquiries.
Radioactive records	30 years	Review and destroy if no longer required	Retention begins at the CREATION of the waste. If a person handling radioactive waste is exposed to radiation (accidental or otherwise), then the records relating to that person must be kept until they reach 75 years of age or would have attained that age. In any event, records must be kept for at least 30 years from the date of dosing or accident. This also includes patients or service users who require medical exposure to radiation, as required by the Ionising Radiation Regulations 2017.
Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhyndrin Test	11 years	Review and destroy if no longer required	Retention begins from the DATE OF TEST.
Surveys – building or installation (not patient surveys)	Lifetime of installation or building	Review and consider transfer to PoD	Retention period begins at the END of INSTALLATION period. (See Inspection reports for legal basis for these records)

FINANCE

Record Type	Retention Period	Disposal Action	Notes
Accounts	3 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate. Includes all associated documentation and records for the purpose of audit.
Benefactions	8 years	Review and consider transfer to PoD	These may already be in the financial accounts and may be captured in other reports, records or committee papers. Benefactions, endowments, trust fund or legacies should be offered to the local PoD.
Debtors' records – CLEARED	2 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Debtors' records – NOT CLEARED	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Donations	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.

Record Type	Retention Period	Disposal Action	Notes
Expenses	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Final annual accounts report*	Up to 20 years	Review and transfer to PoD	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with board papers for that year to keep a complete set of governance papers.
Financial transaction records	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Invoices	6 years from end of the financial year they relate to	Review and destroy if no longer required	
Petty cash	2 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Private Finance Initiatives (PFI) files	Lifetime of PFI	Review and consider transfer to PoD	Retention begins at the END of the PFI agreement. This applies to the key papers only in the PFI.

Record Type	Retention Period	Disposal Action	Notes
Staff salary information or files	10 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Superannuation records	10 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.

LEGAL, COMPLAINTS AND INFORMATION RIGHTS

Record Type	Retention Period	Disposal Action	Notes
Complaints – case files	10 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the complaint. The complaint is not closed until all processes (including potential and actual litigation) have ended. The detailed complaint file must be kept separately from the patient file (if the complaint is raised by a patient or in relation to). Complaints files must always be separate. (Also refer to Appendix III: complaints records)
Fraud – case files	6 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the case. This also includes cases that are both proven and unproven.
Freedom of Information (FOI) requests, responses to the request and associated correspondence	3 years	Review and destroy if no longer required	Retention begins from the CLOSURE of the FOI request. Where redactions have been made, it is important to keep a copy of the response and send to the requestor. In all cases, a log must be kept of requests and the response sent.
FOI requests – where there has been an appeal	6 years	Review and destroy if no longer required	Retention begins from the CLOSURE of the appeal process.
Industrial relations – including tribunal case records	10 years	Review and consider transfer to PoD	Retention begins at the CLOSE of the financial year to which it relates. Some organisations may record these as part of the staff record, but in most cases, they should form a distinctive separate record (like complaints files).
Litigation records	10 years	Review and consider transfer to PoD	Retention begins at the CLOSURE of the case. Litigation cases of significant or major issues (or with significant, major outcomes) should be considered for transfer. Minor cases should not be considered for transfer. If in doubt, consult with the PoD.
Intel patents, trademarks, copyright, IP	Lifetime of patent, or 6 years from end of licence or action	Review and consider transfer to PoD	Retention begins at the END of lifetime or patent, or TERMINATION of licence or action.
Software licences	Lifetime of software	Review and destroy if no longer required	Retention begins at the END of lifetime of software.
Subject Access Requests (SAR), response, and subsequent correspondence	3 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the SAR.
SAR – where there has been an appeal	6 years	Review and destroy if no longer required	Retention begins at CLOSURE of appeal.

Appendix III: How to deal with specific types of records

This Appendix provides detailed advice on records management relating to specific types of records for example, transgender records, witness protection records and adopted persons records. These are presented in alphabetical order. It also provides advice on managing certain formats of records, for example, emails, cloud-based records and scanned records.

TYPE OF RECORD

Adopted persons health records

Notwithstanding any other centrally issued guidance by the Department of Health and Social Care or Department for Education, the records of adopted persons can only be placed under the new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used but more commonly the birth names are used.

Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure.

It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it were considered appropriate to do so following the adoption.

Ambulance service records

Ambulance service records will contain evidence of clinical interventions delivered and are therefore clinical records. This means that they must be retained for the same time as other acute or mental health clinical records depending on where the person is taken to for treatment. Where ambulance service records are not clinical in nature, they must be kept as administrative records. There is a distinction between records of patient transport and records of clinical intervention. If the ambulance clinical record is handed over to another service or NHS trust, there must be a means by which the ambulance trust can obtain them again if necessary. Alternatively, they can be copied and only the copy transferred, providing this is legible.

Asylum seeker records

Records for asylum seekers must be treated in exactly the same way as other care records, allowing for clinical continuity and evidence of professional conduct. Organisations may decide to give asylum seekers patient or service user held records (section below) or hold them themselves. Patient or service user held records should be subject to a risk assessment because the record legally belongs to the organisation, and if required, they must be able to get it back. There is a risk that patient or service user held records could be tampered with or altered in an unauthorised way so careful consideration needs to be given to this decision.

Audio and visual records

Audio and visual records can take many forms such as using a dictaphone (digital or analogue) to record a session or conducting a health or care interaction using videoconferencing technologies.

The following needs considering when patient or service user interactions are captured in this way:

- **Clinical appropriateness:** Organisations should decide when it is appropriate to use audio or visual methods for the provision of health or care. This should be documented in organisational policies and understood by the relevant health and care professionals.
- **Retention:** If the recording is going to be kept elsewhere (for example, as part of the health and care record) then there is no reason to keep the original recording provided the version in the main record is the same as the original or there is a summary into words which is accurate and adequate for its purpose. If the recording is the only version or instance of the interaction, then it must be kept for the relevant retention period outlined in this Code (for example, adult, child health or mental health retention periods). Some recordings may have archival value (although this is unlikely), and this should be considered on a case-by-case basis.
- **Digital continuity:** You must consider the medium on which the recording is made and ensure that it is available throughout its retention period (for example, if the system or file format is becoming obsolete, then you will need to migrate it to a newer platform or format to ensure availability). If it is a digital recording and you are looking to store it in the health and care record, ensure the transfer process captures the authenticity of the recording kept.

- **Storage:** Ensure your recordings are stored on systems you control or are provided to you under contract. If stored with the product provider, you must give them (as controller) clear instructions on the storage and retention of those images (for example, delete one month after the date of the recording because it has been summarised into the main health and care record, or retain for 8 years from consultation with the patient or service user, then destroy). Providers acting under contract to a controller are obliged to carry out their written instruction.
- **Transparency:** You must be transparent with patients and service users regarding the use of audio and visual technology, and associated records, so that they have a reasonable understanding of how they will be used, why, and what will happen with the recording after the interaction. For example, it would be unfair to tell participants that the recordings are deleted if they are not.

Child school health records

Similar to family records (refer to page 94), each child should have their own school health record rather than a record for the school (with consecutive entries) or per year intake. If a child transfers to a school under a different local authority, then the record will also need to be transferred to the new school health service provider. This must only be done once it is confirmed the child is now resident in the new location. The record must be transferred securely. The recipient of the record should contact the sender to confirm receiving the record (if appropriate). If the records are kept on school premises, then access must be restricted to health staff delivering care or other staff who have a legitimate reason to access them.

Local organisations may operate a paper or digital system. Records from other Child Health Teams, following a referral, must be accepted by the receiving organisation regardless of format. This is due to safeguarding risks.

Complaints records

Where a patient or service user complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Detailed complaint information should never be recorded in the health and care record. A complaint may be unfounded or involve third parties and the inclusion of that information in the health or care record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient or service user and the Health and Care Team. In some cases, it may be appropriate to share details of the complaint with the health and care professional involved in providing individual care in order to make improvements in care delivery. However, there may also be times where the complaint is about an individual but not care related and it might not be appropriate to share details of the complaint with that person, in case further action is required. The Complaints Team should review each complaint on a case-by-case basis.

Where multiple teams are involved in the complaint handling, all the associated records must be brought together to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. A complaint cannot be fully investigated if the investigation is based on incomplete information. It is common for the patient or service user to ask to see a copy of their complaint file and it will be easier to deal with if all the relevant material is in one file. Where complaints are referred to the Ombudsman Service, a single file will be easier to refer to.

Health and care organisations should have a local policy to follow with regards to complaints, covering how information will be used once any complaint is raised, and after the complaint has been investigated, regardless of outcome. The ICO has also issued guidance on complaints files and who can have access to them, which will drive what must be stored in them.

Contract change records

Once a contract ends, any service provider still has a liability for the work they have done and, as a general rule, at any change of contract the records must be retained until the time period for liability has expired.

In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision (for current cases) upon termination of the contract. It is also the case that after the contract period has ended, the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

When a service is taken over by a new provider, the records of the service (current and discharged cases) all transfer to the new provider (unless directed otherwise by the commissioner of the service). This is to ensure that the records for the service remain complete and enable patients or service users to obtain their record if they so request it. It also makes the records easier to locate if they

are required for other purposes. This will also stop the fragmentation of the archive records for the service and make it much easier to retrieve records.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also include consideration of the identity of the legal entity, which must manage the records.

In some cases, records may end up orphaned. This may happen where the organisation that created them is being disbanded and there is no successor organisation to take over the service or provision. In these cases, orphaned records need to be retained by the highest level commissioner of that service or provision. For example, if a GP practice closes, patients will be offered the choice to register with another nearby practice. When they register with the new practice, the record will follow the patient to that new practice. However, if a practice closes, and the patient does not re-register elsewhere, the record will transfer to NHS England and Improvement, who commission primary care services in England for ongoing management.

Where the content of records is confidential, for example, health and care records, it will be necessary to inform the individuals concerned about the change. Where there is little impact upon those receiving care, it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes will require individual communications. Although the conditions of UK GDPR may be satisfied, in many cases there is still a duty of confidentiality which may require a patient or service user (in some cases) to agree to the transfer, dependent upon the legal basis and the implications of their choice discussed with them. If the new provider has a statutory duty to provide the service, then consent does not need to be sought. If there is no statutory duty, then consent would need to be sought to satisfy the common law duty of confidentiality.

It is vital to highlight the importance of actively managing records, which are stored in offsite storage (refer to section three of the Code for further information on offsite storage including the importance of completing a DPIA).

These principles and guidance can also apply to non-clinical situations as well, such as when CCGs merge or a trust takes over the running of another one.

Annex 1 of this Appendix summarises the considerations and actions required relating to various contract change situations.

Continuing healthcare (CHC) records

Continuing healthcare records can be split into two parts:

- **Care record:** The care record is the information relating to a patient or service user's care that enables the CHC panel to determine eligibility for CHC based on an assessment of needs. This can be provided directly by the patient or service user or obtained from health and care providers as part of the eligibility process. Consent to obtain this information would be required to satisfy the duty of confidence. The initial checklist completed by the referrer may also contain some level of confidential information and this may also be used to determine eligibility.
- **Administrative record:** The administrative record is the information used by the CCG to ensure the CHC process runs effectively - an example being appointment letters asking the patient or service user to attend a panel. CCGs require access to health and care information to determine a patient or service user's entitlement (once the CCG has been notified).

CHC activity is covered in law by the 2012 Commissioning Board and NHS CCG Regulations. This means consent is not required to process personal data in relation to CHC but consent will be required to satisfy the duty of confidence. CCGs will need to have systems in place to allow for the safe and secure sharing of patient or service user information with relevant partners as necessary, and to inform patient or service users of how their data will be used as part of this process. Digital viewing and sharing of records may be preferable to paper copies being printed and used for CHC, due to the risk of accidental loss or disclosure.

CHC records should be kept for the same period of time as adult and child health records, from the date the case is decided by the CHC panel. Where CHC cases relate to mental health, these should be kept for the same period of time as mental health records.

Controlled drugs regime

NHS England, in conjunction with the NHS Business Services Authority, has established procedures for handling information relating to controlled drugs. This guidance includes conditions for storage, retention and destruction of information. Where information about controlled drugs is held please refer to NHS England guidance.

Duplicate records

The person or team to which the record relates will normally hold the original record however occasionally duplicates may be created for legitimate business purposes. It is not necessary to keep duplicates of the same record unless it is used in another process and is then a part of a new record. Where this is not required, the original should be kept, and the duplicate destroyed. For example, incident forms, once the data is entered into the risk information system, the paper is now a duplicate, and so can be destroyed. Some clinical systems allow printouts of digital records. Where printouts are used, these must be marked as duplicates or copies to help prevent them from being used as the primary record.

Evidence required for courts

In UK Law, the civil procedure rules allow evidence to be prepared for court and, as part of this, the parties in litigation can agree what documents they will disclose to the other party and, if required, dispute authenticity. The disclosure of digital records is referred to as E-Disclosure or E-Discovery. The relevant part for disclosure and admissibility of evidence is given in the Ministry of Justice's Civil Procedure Rules - Part 3. If records are arranged in an organised filing system, such as a business classification scheme, or all the relevant information is placed on the patient or client file, providing records as evidence will be much easier. Further advice on electronic records and evidential weighting can be found in BIP10008: Evidential Weight and Admissibility of Electronic Information.

Family records

Family records used to be common within health visiting teams, amongst others, where a whole family view was needed to deliver care. Whilst these records should no longer be created, they are included here for legacy reasons.

Due to changes in the law and best practice, it is not advisable to create a single paper or digital record that contains the care given to all family members. Each person is entitled to privacy and confidentiality, and having all a person's records in one place could result in a health professional or family member accessing confidential information of another family member accidentally or otherwise.

Good practice would be to create an individual file for each person but with cross references to other family members. This means that each individual has their own record, but health and care professionals can see who else is related to that person, and so can check these records where necessary. Single records also help to protect privacy and confidentiality and (if digital) keep an audit trail of access.

General Practitioner records

It is important to note that the General Practitioner (GP) record, usually held by the General Practice, is the primary record of care and the majority of other services must inform the GP through a discharge note or a clinical correspondence that the patient has received care. This record is to be retained for the life of the patient plus at least ten years after death. The GP record transfers with the individual as they change GP throughout their lifetime. Where the patient has de-registered, records should be kept for 100 years since de-registration. A review is taking place to ascertain how long this period should be in the going forwards.

Current guidance advises that the content of paper Lloyd George records should only be destroyed once they have been scanned to the required standard and quality assurance of the scanned images has been completed, confirming that they are a like for like copy of the original paper records. The Lloyd George envelope itself should not be destroyed at the current time and must be kept to meet with the requirements for patient record movement. NHS England undertook a project to cease the creation of Lloyd George envelopes for all new entrants to the NHS, which was implemented in January 2021 (except in limited circumstances). They are also looking at ways to enable destruction of existing Lloyd George envelopes, though this aspect may have a longer implementation timeframe. This Code will be updated as the programme develops.

Individual funding requests (IFRs)

Similar to CHC, IFR cases are mainly administrative records, but also contain large amounts of personal/confidential patient information and as such, should be treated in the same way as CHC records.

As IFRs are unique to an individual, it may be that the care package given to the patient or service user is unique and bespoke to that person. This could mean that the record may have long-term archival value, due to the uniqueness of the care given in this way, and so potentially may be of interest to The National Archives. Local discussions should be held with the PoD to determine the level of local interest, although they would not normally get involved at this level of discussion. It would be a joint discussion on the principle and agreement to archive this type of record and then the responsibility of the health and care organisation to choose individual records that meet this criteria.

Integrated records

Since 2013, there has been an increase in the number of initiatives promoted and launched that involve integrated records. There has also been recognition nationally that joined up delivery of health and care services can increase the quality of care delivered, and also deliver those services more efficiently. Examples include:

- NHS England Vanguard Programme
- Sustainability and Transformation Plans (STPs)
- Integrated Care Services (ICS)
- Local Health and Care Records (LHCR)

Depending on the agreements under which integrated records are established these may be subject to the Public Records Act. Generally, if an NHS body is at least partly responsible for the creation and control of the record, it will normally be considered a public record to be managed in accordance with the Act. The relevant PoD should be notified that this is the case. If in doubt, consult with The National Archives.

The options for organisations will depend on what local architecture and systems are already in use. There are three types of retention for integrated records, and suggested retention periods for each.

1. All organisations contribute to a single record, creating the only record for that patient or service user. Consideration must be given to how this is managed in practice (for example, some records will be retained for 8 years and some for 20 years but they will look the same at face value) (**retain for the longest specialty period involved**).
2. All organisations pool their records into a single place but keep a level of separation between each type of record (**retain for each specialty as applicable – because they are not merged**)
3. All organisations keep their own records, but allow others to view their records, but not amend or add to (**retain for each specialty as applicable – because they are not merged**)

Where organisations are looking to create integrated records, they must enter into a joint controller arrangement, which detail the purpose and method of integrated records. It should also set out how disputes between controllers may be resolved. Information materials for patient or service users must also reflect how their records are used.

Increasingly, where organisations are using this type of system, the information contained within has the potential to be used for purposes other than individual care, such as Population Health Management (PHM). PHM is a tool that is increasingly being used to help plan and prepare care provision in a particular geographical area or specialty. See also the section on Integrated viewing technology and record keeping in the format section below.

NHSX has published an Information Governance Framework for Shared Care Records, which provides further guidance.

Occupational health (OH) records

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. It is permitted for reports or summaries to be held in the main staff record where these have been requested by the employer and agreed by the staff member. When occupational health records are outsourced, the organisation must ensure that:

- staff are aware of the outsourcing and how their information may be used for OH purposes
- the contractor can comply as necessary with data protection and confidentiality requirements
- there is a contract in place with the outsourced provider that has legally binding clauses in relation to data protection and confidentiality
- the contractor can retain records for the necessary period after the termination of contract for purposes of adequately recording any work-based health issues and is able to present them to the organisation if required

Pandemic records

Health and care organisations will create records as part of a response to a global pandemic. Pandemic events are rare but will nevertheless create records that need to be managed.

Both patient and service user records will be created that detail the care given to people affected by the pandemic. Corporate records will also be created which record business decisions, policies and processes that were taken in response to a pandemic.

These records should be managed in accordance with the retention schedules set out in this Code. Organisations should be mindful that a public inquiry (or inquiries) is likely to take place after a pandemic so the pandemic related records could be used or requested as part of that Inquiry. The Government has already agreed to hold a public inquiry into the coronavirus pandemic that began in 2020.

If organisations have created records specifically in response to a pandemic, these should not be destroyed when they have reached their minimum retention period, unless the public inquiry has ended, or the Inquiry has provided guidance on what type of records it will be interested in. These specific records may have historical value, so discussions should take place with your local PoD. A policy on how to manage a new admission to a care home of an individual with a coronavirus diagnosis may be of interest to the PoD, whereas the care record might not have the same value and should be managed as a health and care record. Any guidance or advice issued by The National Archives or your local PoD in relation to the preservation of pandemic records should be followed.

Patient or service user held records

Some clinical or care services may benefit from the patient or service user holding their own record, for example, maternity services. Where this is considered to be the case a risk assessment should be carried out by the organisation. Where it is decided to leave records with the individual who is the subject of care, it must be indicated on the records that they remain the property of the issuing organisation and include a return address if they are lost. Upon the discharge of the patient or service user, the record must be returned to the health or care organisation involved in the person's care.

Organisations must be able to produce a record of their work, which includes services delivered in the home where the individual holds the record. Upon the termination of treatment, where the records are the sole evidence of the course of treatment or care, they must be recovered and given back to the issuing organisation.

A copy can be provided if the individual wishes to retain a copy of the records through the SAR process. In cases where the individual retains the actual record after care, the organisation must be satisfied it has a record of the contents.

Patient or service user portals

Organisations may implement products that provide patients and service users with access to their records. Access may be either online or via an app or portal. There are increasing numbers of commercial organisations that are providing these products.

The provision of these products must comply with data protection legislation. Health and care organisations must conduct a DPIA if they are considering using such a product. Health and care organisations must remain controller for the patient or service user's information. In most cases, the supplier of the product or system will be a processor as the product facilitates access to the information held by health and care organisations.

Controllers must consider what is relevant and proportionate to include in this type of record. Some information may not be appropriate to add to the portal, for example, harmful information a patient does not know yet because the intention is to let them know in person during a consultation.

Information about the patient or service user must not be uploaded into the product until there is a clear legal basis for doing so, for example, patient consent. Individuals must be provided with information materials so that they can make an informed choice as to whether or not to sign up. The materials should also make it clear what information patients and service users can upload themselves directly to the portal if this is an option. It should also be clear to the patient or service user who controls the information.

Information stored in a product like this should be retained in line with the retention schedules outlined in this Code (for example, adult health records for 8 years after last seen).

Pharmacy held patient records

These are the records of patients that the pharmacy has dispensed medications to or had some other form of clinical interaction with (for example, given a flu jab) - similar to a hospital or care home patient record.

Records of prescriptions dispensed will be kept by NHS BSA so there is no need to keep a copy of the prescription locally except for audit purposes.

Other elements of the pharmacy record, for example, vaccinations provided, should be viewed in the same way as a patient record, and should be destroyed 8 years after the last interaction with the patient. However, if there is a need to keep the record for longer, then this can be extended up to 20 years, provided there is a justified, documented and approved reasons for doing so. Information materials for patients should also be reflective of the organisation's retention period.

Prison health records

In 2013 responsibility for offender health in HM Prison Service transferred from the Ministry of Justice to NHS England. A national computer-based record was created to facilitate the provision of care and the transfer of care records associated with inmate transfers throughout imprisonment.

A significant number of paper records remain, and some offender health services operate a mix of paper and digital records. Prison records should be treated as hospital episodes and may be disposed of after the appropriate retention has been applied. The assumption is that a discharge note has been sent to the GP.

Where a patient or service user is sent to prison the GP record (or social care record) must not be destroyed but held until the patient is released or normal retention periods of records have been met.

Prison health records may have archival value, but this is the exception rather than rule. Records should be kept in line with the same period as for de-registered GP records, with a view to further retention (with justification) and a potential transfer to a PoD, subject to their approval.

Private patients treated on NHS premises

Where records of individuals who are not NHS or social care funded are held in the record keeping systems of NHS or social care organisations, they must be kept for the same minimum retention periods as other records outlined in this Code. The same levels of security and confidentiality will also apply.

Public health records

A local authority normally hosts public health functions, but the functions still involve the handling of health and care information. For this reason, public health functions are in the scope of this Code. Where clinical information is being processed by the public health function it is expected to comply with the NHS Digital Code of Practice for Confidential Information.

Records relating to sexually transmitted diseases

Organisations that provide care and support under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000 must be aware of the additional obligations to confidentiality these impose on employees and trustees of organisations. These organisations include NHS Trusts, CCGs, local authority public health teams and those providing services under NHS contracts.

This obligation differs from the duty of confidentiality generally because it prohibits some types of sharing but enables sharing where this supports treatment of patient or service users. For this reason, it is common for services dealing with sexually transmitted diseases to partition their record keeping systems to comply with the directions and more generally to meet patient or service users' expectations that such records should be treated as particularly sensitive.

Secure units for patients detained under the Mental Health Act 1983

Mental health units operate on a low, medium and high-risk category basis. Not all patients on these units will have been referred via the criminal justice system. Some patients may be deemed a risk under the Mental Health Act and will need to be accommodated accordingly. Some patients may be high-risk due to the nature of a crime they have committed because of their mental health and therefore will need to be treated in a high secure hospital, such as Broadmoor. As such, their records should be treated in the same way as other mental health records including retention periods (20 years, and longer if justified and permitted) and final disposal. A long retention time may also help staff at these units deal with subsequent long-term enquiries from care providers.

Sexual assault referral centres

Sexual assault referral centres (SARCs) are highly specialised forensic and health services co-commissioned by Police and Crime Commissioners and NHS England and Improvement. SARCs support the physical, mental health and wellbeing of service users and collect forensic evidence pertaining to alleged sexual offences. Records generated may include forensic medical examination notes, body maps, photographic records, and DNA intelligence. Reports or statements on these records may be required as evidence in a court of law, and the records management process must facilitate this. Based on relevant guidance, legal and regulatory obligations, a minimum retention period of 30 years for SARC records has been applied by NHS England and NHS Improvement. This retention period reflects the severity of the alleged offence; the length of time for the potential bringing of criminal justice proceedings and right to appeal; and the potential for cold case review. Retaining records beyond 30 years is acceptable provided there is ongoing justification and the decision is documented and approved by the relevant committees responsible for the SARCs operational delivery.

Specimens and samples

The retention of human material is covered by this Code because some specialities will include physical human material as part of the patient or service user record (or linked to it). The record may have to be retained longer than the sample because the sample may deteriorate over time. Relevant professional bodies such as the Human Tissue Authority or the Royal College of Pathologists have issued guidance on how long to keep human material. Physical specimens or samples are unlikely to have historical value, and so are highly unlikely to be selected for permanent preservation.

The human material may not be kept for long periods, but that does not mean that the information or metadata about the specimen or sample must be destroyed at the same time. The information about any process involving human material must be kept for continuity of care and legal obligations. The correct place to keep information about the patient is the clinical record and although the individual pathology departments may retain pathology reports, a copy must always be included on the patient record. Physical specimens or samples do not have to be stored within the clinical record (unless designed to do so) but can be stored where clinically appropriate to keep the material, with a clear reference or link in the clinical file, so both the material and the clinical record can be joined together if necessary.

Staff records

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the information collected through the recruitment process and this will include the job advert, application form, evidence of the right to work in the UK, identity checks and any correspondence relating to acceptance of the contract. The central HR file must be the repository for this information, regardless of the media of the record.

It is common practice in some health and care organisations for the line manager to hold a truncated record, which contains portions of an employee's employment history. This can introduce risk to personal information (as it is duplicated), but also potentially expedient to do so. Organisations considering whether to use, or discontinue using, local HR files, should complete a risk assessment.

Information kept in truncated staff files should be duplicates of the original held in the central HR file. If local managers are given originals as evidence (such as a staff member bringing in a certificate of competence) they should take a copy for local use and the original should be kept with the main HR file. It is important that there is a single, complete employment record held centrally for reference and probity.

Upon termination of contract (for whatever reason), records must be held up to and beyond the statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS or organisational business purposes, in accordance with Retention Instrument 122. Usually this relates to inpatient ward areas, where the ward manager will keep a small file relating to the training and clinical competencies of ward staff. Where there is justification for long retention periods or protection is provided by the Code, this will not be in breach of GDPR Principle 5. (Refer to section 5 of the Code for further information about retention of records).

Some organisations operate a weeding system, whereby staff files are culled of individual record types that are now time expired (such as timesheets). Others have just kept the whole file as is and archived it away until 75th birthday. It is not recommended to change your system from one to the other because:

- the effort involved would be disproportionate to the end result
- if you begin to weed files, you would need to do this retrospectively to all files, to avoid having two types of central HR file
- you cannot reverse the weeding process – if you decide to keep full records, it is impossible to remake historically weeded files complete again

Both systems are acceptable, regardless of media. It is noted that organisations may have a hybrid system of paper historical staff files and digital current staff files. If possible, organisations should consider moving all their files into one format to create consistency.

Where an organisation decides to use a summary, it must contain as a minimum:

- a summary of the employment history with dates
- pension information including eligibility
- any work-related injury
- any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- professional training history and professional qualifications related to the delivery of care
- list of buildings where the member of staff worked, and the dates worked in each location

Good practice for a staff record summary:

Barts Health NHS Trust staff record summary contains the following fields:

- name
- previous names
- assignment number
- pay bands
- date of birth
- addresses
- positions held
- start and end dates
- reasons for leaving
- building or sites worked at

Disciplinary case files should be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record, as it may be pertinent to have an indication to the disciplinary case, but the full details and file must be kept separately from the main file.

With regards to staff training records, it can be difficult to categorise them to determine retention requirements but keeping all the records for the same length of time is also hard to justify. It is recommended that:

- clinical training records are retained until 75th birthday or six years after the staff member leaves, whichever is the longer
- statutory and mandatory training records are kept for ten years after training is completed
- other training records are kept for six years after the training is completed

The Chartered Institute for Personnel and Development, and the ICO have provided further information and advice on the retention of HR records.

Transgender patient's records

Sometimes patients change their gender and part of this may include medical care. Records relating to these patients or service users are often seen as more sensitive than other types of medical records. While all health and care records are subject to confidentiality restrictions, there are specific controls for information relating to patients or service users with a Gender Recognition Certificate. The use and disclosure of the information contained in these records is subject to the Gender Recognition Act 2004, (GRA) which details specific restrictions and controls for these records. The GRA is clear that it is not an offence to disclose protected information relating to a person if that person has agreed to the disclosure. The GRA is designed to protect trans patient and service user data and should not be considered a barrier to maintaining historic medical records where this is consented to by the user.

There are established processes in place with NHS Digital for patients undergoing transgender care in relation to the NHS number and the closing and opening of new Spine records. In practice, nearly all actions relating to transgender records will be based on explicit consent. Discussions will take place between the GP and the patient regarding clinical care, what information in their current record can be moved to their new record and any implications this decision may have (for example, they may not be called for a gender specific screening programme). Patients should be offered ways to maintain their historical records. This could include editing previous entries and removing references containing previous names and gendered language. Any decisions made regarding their record must be respected and the records actioned accordingly.

Any patient or service user can request that their gender be changed in a record by a statutory declaration, but the Gender Recognition Act 2004 provides additional rights for those with a GRC. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Panel issues a Gender Reassignment Certificate. At this time a new NHS number can be issued, and a new record can be created, if it is the wish of the patient or service user. It is important to discuss with the patient or service user what records are moved into the new record and to discuss how to link any records held in any other health or care settings with the new record, including editing previous records to remove names, gender references or details. The content of the new record will be based on explicit consent under common law.

However, it is not essential for a transgender person to have a GRC in order to change their name and gender in their patient record and receive a new NHS number. They do not need to have been to a Gender Identity Clinic, taken any hormones, undergone any surgery, or have a Gender Recognition Certificate.

Under the Equality Act (2010), Transgender people share the protected characteristic of 'gender reassignment'. To be protected from gender reassignment discrimination, an individual does not need to have undergone any specific treatment or surgery to change from their birth sex to their preferred gender. This is because changing physiological or other gender attributes is a personal process rather than a medical one. An individual can be at any stage in the transition process – from proposing to reassign their gender, to undergoing a process to reassign their gender, or having completed it.

Protected persons health records

Where a record is that of someone known to be under a protected person scheme, the record must be subject to greater security and confidentiality. It may become apparent (via accidental disclosure) that the records are those of a person under the protection of the courts for the purposes of identity. The right to anonymity extends to health and care records. For people under certain types of protection, the individual will be given a new name and NHS Number, so the records may appear to be that of a different person.

Youth offending service records

Due to the nature of youth offending, it is common for very short retention periods to be imposed on the general youth offending record. For purposes of clinical liability and for continuity of care the health or social care portion of the record must be retained as specified in this Code, which will generally be until the 25th birthday of the individual concerned.

FORMAT OF RECORD

Bring your own device (BYOD) created records

Any record that is created in the context of health and care business is the intellectual property of the employing organisation and this extends to information created on personally owned computers and equipment. This in turn extends to emails and text messages sent in the course of business on personally owned devices from personal accounts. They must be captured in the record keeping system if they are considered to fall within the definition of a record.

When an individual staff member no longer works for the employing organisation, any information that staff take away could be a risk to the organisation. If this includes personal data or confidential patient information, it is reportable to the ICO and may be a breach of confidentiality. For this reason, personal/confidential patient information should not be stored on the device unless absolutely necessary and appropriate security is in place. Local health and care organisations should have a policy on the use of BYOD by staff. Also refer to guidance on BYOD.

Cloud-based records

Use of cloud-based solutions for health and care is increasingly being considered and used as an alternative to manage large networks and infrastructure. NHS and care services have been given approval to use cloud-based solution, provided they follow published guidance from NHS Digital and information on GOV.UK.

Before any cloud-based solution is implemented there are a number of records considerations that must be addressed as set out by The National Archives. The ICO has issued guidance on cloud storage. Organisations must complete a DPIA when considering using cloud solutions.

Another important consideration is that at some point the service provider or solution will change and it will be necessary to migrate all of the records, including all the formats, onto another solution. Whilst this may be technically challenging, it must be done, and contract provisions should be in place to do this.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever-increasing storage instead of good records management will not meet the records management recommendations of this Code. For example, if digital health and care records are uploaded to cloud storage for the duration of their retention period, then they must contain enough metadata to be able to be retrieved and a retention date applied so it can be reviewed and actioned in good time.

Personal data that is stored in the cloud, and then left, risks breaching UK GDPR by being kept longer than necessary. This information would also be subject to Subject Access process, and if not found or left unfound, would be a breach of the patient or service user's rights.

Email and record keeping implications

Email is widely accepted as the primary communication tool used every day by all levels of staff in organisations. They often contain business (or in some cases clinical) information that is not captured elsewhere and so need to be managed just like other records. The National Archives has produced guidance on managing emails.

Email has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record. However, a common problem with email is that it is rarely saved in the business context.

The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Solutions such as email archiving and ever-larger mailbox quotas do not encourage staff to meet the standard of storing email in the correct business context and to declare the email as a record.

Where email archiving solutions are of benefit is as a backup, or to identify key individuals where their entire email correspondence can be preserved as a public record.

Where email is declared as a record or as a component of a record, the entire email must be kept, including attachments so the record remains integral - for example, an email approving a business case must be saved with the business case file. All staff need to be adequately trained in required email storage and organisations need to:

- undertake periodic audits of working practice to identify poor practice
- have a policy in place that covers email management - including the appraisal, archiving and disposal of emails
- take remedial action where poor practice or compliance is found

Automatic deletion of email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information, even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation. Legal holds can take many forms and records cannot be destroyed if there is a known process or a reasonable expectation that records will be needed for a future legal process such as:

- local inquiries into health or care issues
- national inquiries
- public inquiries
- criminal or civil investigations
- cases where litigation may be reasonably expected, for example, a patient has indicated they will take the organisation to court
- a SAR (known or reasonably expected)
- a FOI request (submitted or reasonably expected)

This means that no record can be destroyed by a purely automated process without some form of review whether at aggregated or individual level for continued retention or transfer to a PoD.

The NHSmail system allows a single email account for every staff member that can follow the individual through the course of their career. When staff transfer from one NHS organisation to another NHS organisation, they must ensure that no sensitive data relating to the former organisation is transferred. It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of classified information. This is facilitated by staff storing only emails that need to be retained on an ongoing basis.

Emails that are the sole record of an event or issue, for example, an exchange between a clinician and a patient, should be copied into the relevant health and care record rather than being kept on the email system or deleted.

Instant messaging records

Health and care services are increasingly using instant messaging apps or platforms to share patient and service user information between health and care professionals or to contact patients or services users in a transactional way, such as appointment reminders. NHSX has published guidance on this issue.

Instant messaging apps or platforms should not be used as the main, or primary, record for a person. Where possible, information shared in this way also needs to have a place in the health or care record of that person. This could be a printout of the exchange; contents transcribed into the record; or a progress note accurately covering the exchange entered into the record. If the app or platform is the only place that information is stored, then it must be managed in line with this Code.

Transactional messages, such as GP appointment reminders or pharmacy notifications that your prescription is ready for collection, have a short shelf-life and will no longer be needed once the appointment is attended or prescriptions collected. Organisations that use these systems should keep a record of messages sent to a person, in case they are needed later (such as proof that the patient was reminded of their appointment), but once it is clear that the purpose of the message has been fulfilled, there is no requirement to keep these messages.

Integrated viewing technology and record keeping

Many record keeping systems pool records to create a view or portal of information, which can then be used to inform decisions. This in effect creates a single digital instance of a record, which is only correct at the time of viewing. This may lead to legacy issues, especially in determining the authenticity of a record at any given point in the past. When deciding to use systems that pool records from different sources, organisations must be assured that the system can recreate a record at a given point in time, and not just be able to provide a view at the time of access. This will enable a health or care provider to show what information was available at the time a decision was made.

Consideration should also be given to the authenticity and veracity of the record, particularly if there is conflicting information presented by two or more contributors to the record. Some conflicts may be easier to resolve than others (for example, a person has a different address with two systems), however more complex conflicts would require organisations to have a process or procedure to agree how to resolve these.

Scanned records

This section applies to health and care records as much as it does to corporate records. When looking to scan records, organisations need to consider the following:

- the scanned image can perform equally as well as the original paper
- scanned images can be challenged in court (just as paper can)
- ability to demonstrate authenticity of the scanned image
- ensure technical and organisational measures are in place to protect the integrity, usability and authenticity of the record, over its period of use and retention
- discussions need to take place with the local PoD over records that may be permanently accessioned - they will need input into the format of the transferring record
- where the hard copy is retained, this will be legally preferable to the scanned image

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or digital, can be admissible as evidence.

The Archives and Records Association has produced a flow chart to support scanning processes. The British Standards Institution has published a standard that specifies the method of ensuring that electronic information remains authentic. The standard deals with both 'born digital' and scanned records. The best way to ensure that records are scanned in accordance with the standard is to use a supplier or service that meets the standard following a comprehensive procurement exercise, which complies with NHS due diligence. Using an BSI10008 accredited supplier, or an in-house accredited service would be seen as best practice.

For local scanning requirements or for those records where there is a low risk of being required to prove their authenticity, organisations may decide to do their own scanning following due diligence and internal compliance processes. This may require a business case to be drawn up and approved, and procurement rules followed to purchase the necessary equipment.

Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original, unless the format of the original has historical value, in which case consideration should be given to keeping it with a view to permanent transfer. Where paper is disposed of post-scanning, this decision must be made by the appropriate group or committee. A scan of not less than 300 dots per inch (or 118 dots per centimetre) as a minimum is recommended for most records although this may drop if clear printed text is being scanned. Methods used to ensure that scanned records can be considered authentic are:

- board or committee level approval to scan records
- a written procedure outlining the process to scan, quality check and any destruction process for the paper record
- evidence that the process has been followed
- technical evidence to show the scanning system used was operating correctly at the time of scanning
- an audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- fix the scan into a file format that cannot be edited

Some common mistakes occur in scanning by:

- only scanning one side and not both sides, including blank pages - to preserve authenticity, both sides of the paper record, even if they are both blank, must be scanned (this ensures the scanned record is an exact replica of the paper original)
- scanning a copy of a copy - leading to a degraded image
- not using a method that can show that the scanned record has not been altered after it has been scanned – questions could be raised regarding process and authenticity
- no long-term plan to enable the digitised records to be stored or accessed over the period of their retention

Once you have identified digital records that are suitable for accessioning to your local PoD or The National Archives (for national bodies, it is recommended to follow published The National Archives guidance on the accessioning of digital records.

Social media

Organisations must have approved policies and guidance when using social media platforms. It is acknowledged that social media will mainly be used for promoting activities of the organisation, rather than as a way of communicating care issues or interventions with patients or service users. Information posted on social media may also be classed as a corporate record and appropriate retention periods set where applicable.

Information posted on social media (such as details of upcoming meetings, or published policies) will usually be captured elsewhere in an organisation's corporate records' function, and where this is the case, there is no value in retaining the information held in the social media platform, as it will be a duplication of the corporate records management function.

The National Archives have begun to capture social media content of NHS bodies that have a national focus, such as NHS England and Improvement. Where requested, this can also be extended to local NHS bodies, but this would be the exception not the rule.

Website as a business record

As people interact with their public services, more commonly it is the internet and websites in particular that provide information, just as posters, publications and leaflets once did exclusively. A person's behaviour may be a result of interaction with a website and it is considered part of the record of the activity.

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate or there must be some other method to recreate what the website or intranet visitor viewed. It may be possible to arrange regular crawls of the site with the relevant PoD but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record. The UK Government Web Archive (part of The National Archives) undertook two central crawls of all NHS sites in 2011 and 2012 and may have captured some from 2004 onwards but the information captured will not include all levels of the sites or some dynamic content.

National NHS organisations have their websites regularly captured by The National Archives and can (upon request) capture local organisation's websites, where regional information would be captured that would not necessarily go to the local PoD (such as a CCG closing down). Local Authorities' websites are not routinely captured by the WebArchive Team at The National Archives but they can do so in exceptional circumstances and if requested by the Authority.

Annex 1: Records at contract change

Characteristic of new service provider	Fair processing required	What to transfer?	Sensitive records
NHS Provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light - notice on appointment letter explaining that there is a new provider. Local publicity campaigns such as signage or posters located on premises.	Entire record or summary of entire caseload.	N/A
Non-NHS Provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	N/A
NHS Provider from different premises but with the same staff.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	N/A
NHS Provider from different premises and different staff.	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. All records must be transferred by the former provider to the new provider.	Individual communications may not be possible so obtaining consent, from the holder of the current caseload, may need to be sought by the old provider before transfer. It may not be possible to transfer the record without consent (to satisfy confidentiality) so in some cases no records will be transferred.
Non-NHS provider from different premises but with same staff.	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload.	
Non-NHS from different premises and with different staff.	High – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload.