Records Management Policy

Woosehill Medical Centre
01/05/2024

V1.2 November 2022

Contents

1. Introduction

This policy sets out how the Practice will approach the management of its records.

All NHS records (including email and electronic documents) are public records under the terms of the Public Records Act 1958 sections 3(1)-(2), and must be kept in accordance with the following statutory and NHS guidelines:

- The Public Records Act 1958 and 1967
- The UK General Data Protection Regulations 2016
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Records Management Code of Practice 2021
- The Common Law Duty of Confidentiality
- Confidentiality: NHS Code of Practice
- NHS Information Governance: Guidance on Legal and Professional Obligations

Guidance on the management of NHS records is provided by the Department of Health. The Records Management: NHS Code of Practice 2021 sets out a schedule of minimum retention periods for many types of records and is based on legal requirements and professional best practice.

2. Scope and Definitions

This policy covers all Practice business areas and all information, irrelevant of the media being used to store the information. This includes:

- Patient records in all formats (Lloyd George Records, electronic)
- Corporate records in all formats (paper and electronic), active and inactive, held for use in the organisation;
- Administrative (e.g. corporate, contracts, personnel, estates, finance and accounting, customer services and litigation);
- E-mails; other communication tools; text messages

Records management is the process by which an organisation manages all the aspects of records and information, from their creation through to their eventual disposal (Records Lifecycle). The aim of the policy is to ensure:

- **Accountability** – Records are adequate to account fully and transparently for all business actions and decisions, in particular to:
    - protect legal and other rights of staff or those affected by those actions;
    - facilitate audit or examination;
    - provide credible and authoritative evidence
- **Accessibility** – Records can be located when needed and only those with a legitimate right can access the records and the information within them. Records are displayed in a way that is consistent with their initial use, and the current version is identified where multiple versions exist.
- **Interpretation** –The context of the record can be interpreted through means such as: identification of who created or amended the record, when this was done, at what

stage of the process this was done, whether the amendments were appropriate, and how the record is related to other records.

- **Quality** – Records can be trusted and are complete and accurate; records reliably represent the information; records show who they were created by; records reflect the business process; the integrity and authenticity of the records can be demonstrated.
- **Maintenance through time** – In order for the quality, availability, accessibility, interpretation and trustworthiness of records to be maintained for as long as is needed, perhaps permanently, despite changes of format.
- **Security** – Records are secure from unauthorised or inadvertent alteration or erasure; access and disclosure are properly controlled; audit trails are followed to track all use and change in order to ensure that records are held in a robust format which remains readable for as long as records are required.
- **Retention and disposal** – Records are retained and disposed of appropriately, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value. The British Security Industry Association standard (BSIA) EN15713:2009 - Secure Destruction of Confidential Material must be adhered to when destroying confidential information.
- **Staff are trained** – All staff are made aware of their responsibilities regarding records management.

3. Processes/Requirements

The Practice's records provide evidence of actions and decisions, represent a vital asset to support daily functions or operations and are its corporate memory. Records support clinical care, policy formation and managerial decision-making to protect the interests of the Practice. They enable consistency, continuity, efficiency and productivity and help the Practice to deliver services in consistent and equitable ways.

The Practice operates within an Information Governance compliance environment. Failure to meet any relevant requirement could result in official sanction, reputation damage and even limits on what data and services could be provided as a business. The Practice must be compliant with the NHS Data Security and Protection Toolkit (DSPT) and Records Management Code of Practice 2021

The organisational benefits from good records management are:

- control and availability of valuable information assets to support clinical care and all operations
- efficient use of staff time
- compliance with legislation and standards
- good utilisation of storage and server space
- a reduction in costs
- supporting the day to day business that underpins the delivery of a high quality service to our customers

- maintaining the integrity of the records
- meeting legal requirements
- monitoring and audit cycles

The Practice will establish and maintain policies to ensure compliance with the Records Management Code of Practice 2021

Records Management – Components and Principles

The International Organisation for Standardisation (ISO) 15489-1:2016 Information and documentation – Records Management Lifecycle – defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of businesses.

Records Life Cycle	
Lifecycle Stage	**Description**
1. Planning	We will develop and implement policy, procedures and functionality to deliver compliant records management strategy. We will identify key records that must be captured and managed.
2. Creation & receipt	We shall ensure that our records are properly captured into approved filing systems, that they are protected from unauthorised access or change, are assigned the correct data classifications and are named following an agreed standard.
3. Retention	We shall retain non-current and superseded records in our filing system to support ongoing business needs and compliance requirements. Our disposal schedules shall govern how long records are retained. Retained records shall continue to be protected and accessible, with storage facilities meeting appropriate standards.
4. Disposal	Our records shall not be retained indefinitely. At the end of the agreed retention periods, records shall be disposed of and a destruction certificate will be issued. A small percentage of records may become be flagged for permanent retention and will be passed to the appropriate place of deposit (POD).

UK General Data Protection Regulations (UK GDPR)

Under the UK General Data Protection Regulations (UK GDPR) the definition of 'data concerning health' is 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status' (Article 4(15)

'Personal Data' is defined as: 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (Article 4(1))

There are various UK GDPR definitions relating to the management of information and records in a health environment. For example, also under Article 4;

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;
- **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

For information on categories of data and their assigned definition, please refer to Appendix C – Categories of data/information**.**

Business/Commercial information, including that subject to statutory or regulatory obligations, is information which may be damaging to the Practice or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

Information Quality

Records are evidence of Practice activities. They may be required for litigation, governance, external audits, statutory enquiries, patient care and as a basis for decision making. Records need to be:

- complete (in terms of having been captured in full)
- accurate (factually correct, legible and assured as to the integrity of the record)
- relevant (data meets current and potential user's needs)
- accessible (available when needed)
- timely (recorded and available as soon after the event as possible)

Alterations or annotations must be clearly identifiable, traceable to the author and authorised by an appropriate person.

Clinical records must be timely, accurate, concise and up to date accounts of the assessment and treatment of individual patients. Good clinical record keeping is an integral and vital part of professional practice and may come under scrutiny should any issues arise.

Practice Managers shall also be clear on what records are required to sufficiently document business activities, and ensure that staff capture them following policy and procedure.

Manual/Paper Records

In keeping with the wider NHS agenda (NHS England Five Year Forward Plan), the Practice shall endeavour to maintain records electronically where practicable. Original electronic records will

be considered the 'primary version'. Printed copies of electronic records should be maintained only by exception and shall be appropriately destroyed at the earliest convenience.

Where it is practical to do so, the Practice will scan new or legacy paper records following scanning guidance (this follows standard British Standard (BS) 10008 to protect legal admissibility of scanned paper records). In some cases it might be desirable to hold original ink signed records and guidance will be taken from NHS Digital on these requirements. This is permissible, although scanning such documents is preferable so long as the scanned version is legally admissible.

Paper copies of records must be kept secure and should be stored in an appropriate locked filing cabinet, office or designated records store on site, or in an approved off-site storage facility, so they are available and accessible to those who need them.

Records Inventory

Information Asset Registers are used to monitor and understand what collections of records and information are held and note each documents retention period. The Practice will organise records into a Records File Plan in a systematic and organised way.

Disposal Schedules and Legal Holds

The Practice will not retain records indefinitely. A disposal process leads to records being destroyed or transferred elsewhere and includes a record of what happened so that the Practice can clearly show that it does not have the information any longer.

The planned disposal of any records shall be *held* if they pertain to an existing/emerging legal matter or request for information – this is known as a Legal Hold. An inventory of the retained records and the reason for the extended period of retention must be maintained.

Records shall be retained and disposed of following agreed disposal schedules and procedures that are based on the Records Management Code of Practice 2021 and business needs. Disposal shall always be carried out following confidentiality and sensitivity requirements.

Unilateral disposal of records, particularly if done contrary to disposal schedules or legal holds, is a serious breach of this policy.

Accredited File Shares

Electronic records shall be saved to the approved and governed file share and shall include sub-folders that assist with disposal management.

It is a legal requirement to securely store records that contain person identifiable data and special categories of personal data that are considered as personal confidential data or hold commercially confidential information. The Practice will ensure such data is stored within the Secure drive and have the correct protective marker applied – please refer to the 'Security and Access' heading below.

As a general rule, original electronic records should not be saved to 'offline' storage such as non-networked computer hard drives, USBs or optical media. In some circumstances e.g. anticipated limited network connection, staff may need to save copies of records to **encrypted** devices such as a USB memory stick. This is permissible if the relevant Practice Policy is followed, and any new records/versions are saved to the approved storage location as soon as possible and subsequently deleted from the storage device.

Naming Electronic Documents

Record naming is an important process in records management and it is essential that a unified approach is undertaken within all areas of the Practice to aid in the management of records.

In constructing a title it is necessary to decide how best to describe the content of the file or the individual document. The most commonly used elements in the creation of a title are listed below. It will depend on the nature of the document or folder which elements will be the most suitable for use in the title.

Common elements of a title:

- Department
- Date (if applicable)
- Subject
- Document status
- Version number

Staff members should refrain from naming folders or files with their own name unless the folder or file contains records that are biographical in nature about that individual, for example, personnel records.

Security and Access

Classification of NHS Information - Marking Guidance from NHS England

ALL information the Practice collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

EVERYONE who works within the Practice (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any Practice information or data that they access, irrespective of whether it is marked or not.

Line of Business Systems/Databases

Many records are held within databases. These may be in the form of uploaded documents e.g. a PDF or email, or as data streams, e-transactions and system actions. This policy applies to these records. The Practice shall consider the requirements of this policy when implementing, procuring or using databases.

Electronic records that are uploaded to databases, e.g. an email into EMIS, should be deleted from local systems, e.g. Inbox or File Share. It is bad practice to duplicate information across systems.

Data Backups

All data including electronic records are 'backed-up' to offline storage in accordance with the relevant Practice Policy. It is vital that 'rescued' records are complete copies and are not changed in any way. This includes embedded metadata, e.g. date created, data last modified.

Backups are within scope of statutory access to information requests and legal disclosure. Records deleted from user front-end storage, e.g. file shares, should also be deleted from the back-up and shadow copies. Current back-up policy is that any iteration of electronic data is backed-up for one year before being overwritten or deleted. In short, records that have been deleted from front-end systems within the last year may still be available in the back-up.

New Technologies – Cloud and Collaboration/Sharing

The use of new technologies to improve working practices, process monitoring and collaboration is becoming increasingly popular. These are characterised by services such as cloud storage and collaboration spaces being held outside of traditional on-site technology infrastructure.

The requirements of this policy apply to such technology because they are handling Practice information and records. Assurances must be in place to ensure that data retention schedules are met and data is fully deleted to include back-up copies and 'other' structures that may refer to or directly reference the data, for example, a document index.

Email Records/Electronic Communication

Email is a key communication tool. The email service is designed as a communication tool and is not an appropriate solution for long term file storage. Therefore, all emails that are records of business activity and/or formal records of a transaction should be saved to an appropriately named folder on shared network drive. Keeping all emails will result in a significant storage burden and information may become difficult to locate due to the size of files and attachments being stored.

NHS Mailboxes and Mailbox Archives should not be used for the long term storage of email records.

Particular attention must be paid to ensuring that emails relating to patients (clinical records) are dealt with promptly and where appropriate, deleted once the pertinent information has been transferred to the relevant record.

Staff shall regularly housekeep their Mailboxes so that transitory and spam type emails are disposed of. Managers shall ensure all required email records are transferred from a staff leaver's Mailbox to the approved store. Other forms of electronic communication such as Instant Messaging, voice recording and video conferencing will likely become more commonplace. These 'recordings', if retained, shall be managed under this policy.

Long Term Access and Protection – Record Preservation

The Practice shall take steps to ensure that records remain accessible and are not damaged during their retention; for some records this could be many decades. Such lengths of time require preservation management.

Records shall be protected from unauthorised access and natural risks such as flooding and fire. A risk assessment of all storage solutions (on or off-site) must be undertaken to ensure the area meets the required structural and environmental standards. Electronic records are at a particular risk of digital obsolescence and degradation of media. The Practice will ensure the long term accessibility of electronic content including; regular refreshing and error-checking of storage media; maintaining all records on networked and backed-up drives rather than removable media storage e.g. CDs, USBs; and assessing the digital preservation risks of any new system.

4. Roles and Responsibilities

Practice Manager

The Practice Manager is the person responsible for the day-to-day operational management of the records management programme and framework. They will oversee what information is held, what is added, what is removed, and who has access and why. As a result they are able to understand and address risks to information assets and to provide assurance to the Practice on the security and use of the assets. They ensure that staff have attended required record keeping training and are also responsible for drafting policies and procedures, conducting audits and supporting Practice staff.

Caldicott Guardian

The Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. They will support work to enable information sharing where it is appropriate to share and advise on possible choices for meeting compliance when processing information.

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been assigned the responsibilities set out in the UK GDPR, such as monitoring and assuring practice compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the Practice and acting as the contact point with the ICO.

All Staff

All staff and those working on behalf of the Practice who create and use records as part of the delivery of Practice business are expected to follow this policy and its procedures. This covers records in all formats (paper and electronic) both active and inactive.

5. Training

All staff are required to comply with the Practice policies and procedures, which stress the importance of appropriate information handling, incorporate statutory, common law and best

practice requirements. The Practice will ensure that all staff receive annual Information Governance training appropriate to their role through approved an approved training method. Managers are responsible for monitoring staff compliance. New starters and any temporary, contract or agency staff must also complete the annual Information Governance training.

6. Monitoring Compliance and Effectiveness

This policy will be monitored by the Practice to ensure any legislative changes that occur before the review date are incorporated.

Records management compliance should be audited following a scheduled plan using a defined audit methodology. **Practice Manager** will have direct responsibility for ensuring their information practices are audited with support from the Practice Manager. Where non-compliance or improvements could be made, there shall be agreed upon procedures with process owners/managers that should subsequently be followed up.

Failure to comply with this policy may result in ineffective working and an inability to meet the requirements of the Freedom of Information and the General Data Protection Regulations 2016. Where the policy is breached, this must be reported via the local incident reporting process and the Data Protection Officer and Caldicott Guardian informed, if required.

7. Review

This policy will be reviewed annually or earlier should there be significant changes to the regulatory environment or Practice.

8. References and Associated Documents

- Information Commissioners Office (Data Protection Act 2018 and UK General Data Protection Regulation) –Guide to the UK General Data Protection Regulation (UK GDPR) | ICO
- National Archives (Public Records) – www.nationalarchives.gov.uk
- Data Security and Protection Toolkit – Data Security and Protection Toolkit (dsptoolkit.nhs.uk)
- NHS England (Document and Records Management Policy Final v3) – www.england.nhs.uk
- Records Management Code of Practice 2021 - Records Management Code of Practice - NHSX
- Government Security Classifications 2018 - Government Security Classifications - GOV.UK (www.gov.uk)

Appendix A: Key Records Management Requirements

Legislation/Standard	Compliance Requirement
Public Records Act 1958	All NHS records are Public Records. All NHS organisations must make arrangements for the safe keeping and disposal of their information and records. Recent changes have reduced the 30 year public records disposal rule to 20 years.
Freedom of Information Act 2000 including Section 46 Code of Practice for Records Management.	Provisions for disclosure of information held by public authorities. Includes a Records Management Code of Practice to support the Act which gives guidance on good practice in records management. It applies to all authorities subject to the Act, to the Public Records Act 1958 or to the Public Records Act (Northern Ireland) 1923.
UK General Data Protection Regulation	Regulates the processing of personal data relating to living persons. Article 5 of the UK GDPR requires that personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or

	historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
Data Protection Act 2018 (DPA 2018)	The Data Protection Act 2018 replaces the Data Protection Act 1998 and legislates to an equivalent to the UK GDPR but includes national derogations not covered by the UK GDPR. The DPA 2018 should be read in conjunction with the UK GDPR.
Access to Health Records Act 1990	Regulates access to the records of a deceased person.
Records Management Code of Practice 2021	The guidelines in this Code apply to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. The code includes records of staff, complaints, corporate records and any other records held in any format or media.

Appendix B: Clinical Records Guidance

UK GDPR Recital number 35 clarifies that Personal data concerning health should include all data pertaining to the health status of a data subject that reveals information relating to the past, current or future physical or mental health status of the data subject. This includes:

- information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person;
- a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;
- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;
- and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

Good clinical record keeping is an integral and vital part of professional practice which contributes to a high standard of:

- The delivery of clinical care
- Continuity of care
- The sharing of information and improving communication between parties
- Business and reporting purposes

Clinical records must be a timely, accurate, concise and up to date account of the assessment and treatment of individual patients.

Information held in clinical records will relate to any aspect of patient health, treatment and other care they receive and, by their nature, are considered as OFFICIAL-SENSITIVE: PERSONAL.

Only business areas that specifically require clinical records to carry out their work should have access to them, and they should only access them as required for job activities. If you receive clinical records and you are not sure why, report this to your **Manager and Dr Rishi Anand Information Governance Officer**

Individual employees are responsible for the safeguarding of confidential information held as paper records (in a structured filing system) and electronically (on computers and within an agreed filing procedure). Please ensure there are robust 'track and trace' mechanisms in place for all paper records, e.g. tracer cards. Access to electronic information must be appropriately restricted.

Unavailable, mislaid or lost clinical records are a serious risk and immediate action must be taken. The Practice must log this as an incident and carry out an investigation.
Any unauthorised use of clinical information, e.g. searching for information about a relative, or any use of information outside of a "legitimate professional relationship" may lead to immediate disciplinary action. This would be viewed as a breach of confidentiality.

Appendix C: Categories of Data / Information

Please note that the categories of data/information listed below will be used or referred to in all Practice polices. The purpose of this is to ensure that a consistent approach is adopted.	
Personal Data (derived from the UK GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the UK GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: • The racial or ethnic origin of the data subject • Their political opinions • Their religious beliefs or other beliefs of a similar nature • Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 • Genetic data • Biometric data for the purpose of uniquely identifying a natural person • Their physical or mental health or condition • Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data are owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: To Share or Not To Share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the Practice or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

Document Control

This document was created by NHS South Central and West Commissioning Support Unit (SCW) and as such the Intellectual Property Rights of this document belong to SCW.

Document Name	Version	Status	Author
Records Management Policy Primary Care template	1.2	Published	NHS SCW Information Governance Services
Document objectives	This document supports Practice staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience	All staff		
Monitoring arrangements and indicators	This document will be monitored by NHS SCW Information Governance Services to ensure any legislative changes that occur before the review date are incorporated.		
Review frequency	SCW reviews customer documents in line with our planned schedule		
SCW Planned Review date	01 November 2023		
Date uploaded to SCW Website	March 2023		
Approved & ratified by practice	Woosehill Medical Centre	01/05/2024	
Date issued by practice	01/05/2024		
GP Review date	01/05/2025		

Change record

Date	Author	Version	Page/s	Reason for Change
28.08.2020	SCW	1	All	Review for Website publication
26.10.2021	SCW	1.1	All	Update UK GDPR & RMCOP 21 in all sections & Removal of Appendix D Retention Schedule
25.11.2022	SCW	1.2	All	Links updated in line with relevant guidance