CATHAYS SURGERY

# RECORDS MANAGEMENT POLICY

Version: 1
Last Updated: August 2021

# Records Management Policy

CATHAYS SURGERY

## Contents

## 1.0 Definitions

The terms that appear throughout the policy are subject to the predefined definitions that appear below:

'The practice' or 'practice' refers to Cathays Surgery in its capacity as a health care provider, business and its facilities and premises.

'The DPA', 'DPA', 'DPA 2018' or 'The Act' refers to the Data Protection Act 2018.

'The GDPR' or 'GDPR' refers to the General Data Protection Regulation 2016.

'The FOI Act' refers to the Freedom of Information Act 2000.

'ICO' refers to the Information Commissioners Office.

## 2.0 Introduction

This template policy has been created for use by Cathays Surgery with assistance from the NHS Wales Informatics Services' (NWIS) DPO Support Service in line with the **Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016**, The National Archive's (TNA) Guidelines for Public Records and the current regulatory and legal framework. Compliance with this policy will help to ensure the Practice is complaint with, GDPR, Data Protection Act 2018 and the **Lord Chancellors Code of Practice** on the management of records issued under S46 of FOIA Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources of the practice.

It is of paramount importance to ensure that records are efficiently managed, and this policy sets out the way that the practice will retain, process and dispose of records.

The practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The practice fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The practice also recognises the need to share patient information with other health organisations in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest, all within compliance with the Data Protection Act 2018 and the GDPR.

The practice believes that accurate, timely and relevant record management is essential to deliver the highest quality health care. As such, it is the responsibility of practice staff members to ensure that record keeping, and the subsequent retention periods of records are adhered to.

The Practice acknowledges the current ongoing enquiries including the Independent Inquiry into Child Sexual Abuse (IICSA) and Infected Blood Inquiry (IBI) and the NHS Wales mandate not to destroy any records that are or may fall into the remit of such enquiries.

## 3.0 What is a record?

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

Examples of records that should be managed using the guidelines in this policy are listed below. This list gives examples of functional areas as well as the format of the records:

**Function:**

- Patient health records (electronic or paper based, including those concerning all specialties and GP records).
- Records of private patients seen on NHS premises.
- Accident & emergency, birth, and all other registers.
- Theatre registers and minor operations (and other related) registers.
- Administrative records (including, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling).
- X-ray and imaging reports, output and images.
- Integrated health and social care records.
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is not for direct care purposes. This can include data for service management, research or for supporting commissioning decisions.

**Format:**

- Photographs, slides, and other images.
- Microform (i.e. microfiche/microfilm).
- Audio and video tapes, cassettes, CD-ROM etc.
- E-mails.
- Computerised records.
- Scanned records.
- Text messages (SMS) and social media such as Twitter and Skype (both outgoing from the NHS and incoming responses from the patient).
- Websites and intranet sites that provide key information to patients and staff.

## 4.0 Scope

This policy applies to all records created, received, maintained and held, in all formats, by staff of the Practice in the course of carrying out their functions. Records are defined as documents, regardless of format, which facilitate the operations and business of the practice and which are thereafter retained for a set period to provide evidence of its activities and transactions, as detailed within the Retention Schedule.

This policy applies to all employees of the practice, including associates, contractors, temporary staff and any students who are carrying out work on behalf of the practice.

## 5.0 Legislative Compliance

The management of records held by the practice is regulated by the following regulatory frameworks:

- **Data Protection Act 2018** & **General Data Protection Regulation (GDPR)**
- **Freedom of Information Act 2000**
- **Limitation Act 1980**
- **Welsh Health Circular (WHC) (99)7**
- **Welsh Health Circular (WHC) (2000)71**
- **Public Records Act 1958**
- **Local Government (Wales) Act 1994**
- **Lord Chancellor's Code of Practice**

The DPA and FOI Act contain provisions relating to the destruction or alteration of information or records after a legal access request has been received. Such destruction or alteration will be considered a disciplinary offence. FOI Act also creates a criminal offence in relation to these actions.

This policy is designed to support disposal decisions made and the practice to defend legitimate records management activity

Section 46 of the Freedom of Information Act sets out the Lord Chancellor's Code of Practice on the Management of Records sets out measures and good practice that should be in place in relation to information management to ensure that requests made under the Freedom of Information Act can be answered in a timely manner, and also that information is not disposed of when it may still be required.

## 6.0 Responsibilities

The Practice Manager is responsible for ensuring the highest level of commitment to the policy and the availability of resources to support its implementation and associated legal requirements.

The Practice Manager is responsible for the implementation of this policy throughout the practice, and in addition, they must ensure that all staff are aware of this policy, understand their responsibilities in complying with the policy requirements and are up to date with mandatory information governance training.

The Practice's staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. Breaches of the policy must be reported in line with the practice's reporting processes and dealt with in line with the practice's disciplinary process where appropriate.

## 7.0 Standards

The following standards need to be maintained at all times:

- Records must be managed in a manner complying fully with legislative and regulatory requirements affecting their use and retention.
- Records must have relevant content, context and format, and must be accurate authentic, useable, reliable, timely and well managed.
- Records must directly relate to and support a service, function or actively delivered by the practice, ad be able to support decision making.
- Records must serve the interests of the practice, its staff, patients and other stakeholders by maintaining high quality documentation for appropriate lengths of time.
- Records must be managed via systems and processes ensuring efficiency and consistency throughout their lifecycle of creation, distribution, use, maintenance and disposition.
- Records must be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities.
- Records must be kept securely to ensure the confidentiality and importance of the content, being protected from unauthorised or unlawful disclosure.

- Records must be accessible and retrievable to support the continuity of practice business and the efficiency of the provided services.

- Records must be retained and disposed of in compliance with the Records Retention Schedule.

- Records must undergo a review at the end of their retention period and, if no longer required, be securely destroyed in an efficient, timely and confidential manner.

## 8.0 Creating records

The practice must have in place adequate systems for documenting its main activities and ensuring that any records created are maintained and serve the practice's functions in accordance to the standards detailed in section VII.

All records must be accurate and complete, so that it is possible to establish what has been done and why. The quality of all records must be sufficient to allow practice staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met.

Where appropriate, templates should be used so that documents are produced consistently, and can be stored in a cohesive manner. In addition to this, version control procedures should be used for drafting and revising documents, so that practice staff can easily differentiate between versions and readily identify the latest copy.

The practice must identify and take responsibility of records or record sets and appoint an individual to fulfil the role of an Information Asset Owner.

Any duplicate records that are retained increases the risk regarding the management use and alteration of the record. There may be need to keep a local version of a record centrally, however, it should be avoided where possible and a system enabling the use of a single central version implemented.

Where possible, to reduce the need for duplication of documents, records should be stored in central folders that are accessible to relevant practice staff. Digital records should be stored in a shared workspace whenever possible. Titles of these digital records should be easily identifiable.

Both paper and electronic records systems should contain metadata to enable the records to be understood and stored/accessed easier. This will make administration and retention periods easier to

## 9.0 Organising records

Records should be organised and described in a uniform, logical manner that facilitates fast, accurate and comprehensive retrieval so that they are easily accessible when they are required.

Classifying records and holding them in an appropriate filing structure will enable suitable retention periods to be assigned. Keeping diverse records together in a less structured format will make it difficult to identify and retrieve record when they are needed, and make it difficult to assign retention periods.

Digital storage of records enables records to be tagged and introduces a searching functionality which can be used to find records quickly.

## 10.0 Off-site storage

When storage or physical records is unavailable, the practice may use a contracted off-site storage provider, Shared Services. Records stored off-site need to be considered carefully as it will take longer to recall the records to the practice in the event that they are needed.

## 11.0 Security and access

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with practices Data Protection/Information Governance policy. Records must be stored in safe and secure physical and digital environments, taking account of the need to preserve important information in a useable format enabling ease of access in correlation to the frequency of use.

Records should not be only accessible by a single person but should be stored in centralised storage or filing systems or on a shared drive, so that departments can operate efficiently when individual members of staff are absent. Where appropriate, access to central records should be appropriately available across the practice in order to avoid recreating information that already exists and storing duplicate data unnecessarily.

Records that would be vital to the continued functioning of the practice in the event of a disaster must be identified and protected. These include records that would recreate the practice's legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders. All critical business data must be protected by appropriate preservation, backup and disaster recovery policies. Where vital records are only available in paper format it is best practice that they are duplicated, and the originals and copies stored in separate locations. If duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect vital documents.

## 12.0 Retention

Section 12.2 of the Lord Chancellor's Code of Practice on the Management of Records states:

***"As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used, and costs are not incurred in maintaining records that are no longer required."***

Records must only be kept for as long as is required to meet operational, business and legal needs. It is a legal requirement established by the DPA to only retain records containing personal data for as long as strictly necessary, and organisations can be subject to enforcement action by regulatory bodies, such as the ICO, for failing to comply. By having clearly defined procedures for the retention and disposal of records, the practice can demonstrate its responsibility in the management of information and records.

The practice's Records Retention Schedule is intended to provide guidance to all areas of the practice regarding appropriate retention periods for the different categories of records held by the practice. It applies to all formats of records and is intended to promote consistency and the retention of the minimum volume of records while accounting for requirements imposed by legislation and regulation.

Retention can be complicated if records of a dissimilar nature, with different retention requirements, are filed together. The practice should consider retention periods when designing their records storage systems and practices to avoid this issue. Files should be reviewed regularly to ensure records are not kept for too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

The Records Retention Schedule includes the following information:

- **Record type** – The type of record or information asset, applying to all formats of record.
- **Recommended retention period** – The recommended length of time for which the records should be kept by the practice.
- **Action at the end of retention period** – This is the action that should be taken once the retention period has reached its end.
- **Notes** – Any additional information unrelated to the three prior fields.

## 13.0 Disposal

When a record reaches the end of its retention period, a review must be taken on the documents future. The outcomes of this review can be any of the following:

- Reappraisal
- Permanent preservation
- Destruction

### 13.1 Reappraisal

Before action is taken to permanently preserve or destroy a record at the end of its retention period, a reappraisal of any need to retain it for present functions should be undertaken, but it should only be necessary to revise the retention period on rare occasions.

In some circumstances it may be necessary to retain a record for longer than its defined retention period. A new operational function requiring its retention may have arisen, or it may be required for investigation or litigation purposes, or because it is needed in order to respond to an access request received under data protection or freedom of information legislation. If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision while taking circumstances into account. A period of one year is recommended.

Examples of when information may be required to be held for longer periods are where:

- The information is subject to a request for information under access to information legislation such as a Subject Access Request under the Data Protection Act or a request under the Freedom of Information Act.
- The Practice is subject to ongoing legal action in which the information relates.
- The information is subject to an investigation e.g. an Independent Inquiry into Child Sexual Abuse or the Infected Blood Inquiry.
- There is a greater public interest in an issue requiring long term preservation of the information.

### 13.2 Permanent preservation

Some of the practice's records are retained permanently because they have long term evidential or historical value. The practice's Records Retention Schedule should help to identify records that have archival value. The following records are examples of items that may be worthy of permanent preservation:

- Records that document policy formation.
- Records that show the development of the practice and its infrastructure.
- Records that show evidence of important decisions or precedent.
- Records showing the development of the relationship between the practice staff and the practice's corporate functions.
- Records documenting the practice's relationship with external parties and stakeholders, and the practice's place in the local, national and international community.

Where records are considered to be of historical value the practice should contact is local place of deposit (add in national archives link) who will assess and transfer the appropriate records for preservation.

### 13.3 Destruction

The destruction of records is an irreversible act which must be clearly documented and carefully considered. All records identified for disposal will be destroyed under confidential conditions in accordance with the practice retention schedule – see DPO Retention Schedule Guidance sheet.

A decision for destruction must be made by the Practice Manager, disposal certificates and a destruction log should be maintained.

When disposing of digital records, the practice will ensure that all traces of the record are deleted securely, and are not duplicated on other systems, hard drives (HDDs), servers or removable storage devices.

## 14.0 Information not listed on the Records Retention Schedule

Occasionally documents and information held by the practice may not be specifically listed on the retention schedule. In such cases information should be held for the time of appropriate equivalent records, for example petty cash records should be retained in line with financial transaction records.

## 15.0 Review

This policy will be reviewed every two years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation;
- Practice change or change in system/technology;
- Change in Senior personnel e.g. Practice Manager or Senior Partner or;
- Changing methodology.

## 16.0 Equality Impact Assessment

This policy has been subject to an equality assessment.

Following assessment, this policy was not felt to be discriminatory or detrimental in any way with regard to the protected characteristics, the Welsh Language or carers.