Llywodraeth Cymru
Welsh Government

RECORDS MANAGEMENT CODE OF PRACTICE FOR HEALTH AND SOCIAL CARE 2022

A GUIDE TO THE MANAGEMENT OF HEALTH AND CARE RECORDS

PUBLISHED FEBRUARY 2022

gov.wales

Contents

1	Introduction
3	Section 1: Scope of the code
5	Section 2: Records management obligations
10	Section 3: Organising records
15	Section 4: Records storage for operational use
19	Section 5: Management of records when the minimum retention period is reached
28	Appendix I: Public and statutory inquiries
29	Appendix II: Retention schedule
60	Appendix III: How to deal with specific types of records
77	Appendix IV: Records at contract change

Mae'r ddogfen yma hefyd ar gael yn Gymraeg.
This document is also available in Welsh.

OGL © Crown copyright 2022 WG44221 Digital ISBN 978-1-80391-679-8

Introduction

The Records Management Code of Practice for Health and Social Care 2022 (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 Wales. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities.

The Code is based on the Records Management Code of Practice for Health and Social Care 2021 developed by NHSX in England, and provides a framework for consistent and effective records management based on established standards and current legislation. 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 refers to information on public inquiries.
- Appendix II is a retention schedule for different types of records.
- Appendix III is 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 Wales Information Governance Toolkit hosted by Digital Health and Care Wales (DHCW), 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 organisations in Wales, Healthcare Inspectorate Wales (HIW), Audit Wales and the Information Commissioner's Office (ICO) 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 published by NHSX in England drew on published guidance from The National Archives (TNA) and best practice and lessons learnt in the public and private sectors.

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.
- Academy of Medical Royal Colleges' standards for the clinical structure and content of patient records.
- Code of Practice on the management of records issued under Section 46 of the Freedom of Information Act 2000 (FOIA) 2000.

This 2022 revision was conducted by Health and Social Services' Digital Policy Team, based on NHSX guidance, reflecting consultations in which 50 organisations responded, including national stakeholders and local organisations. This Code replaces the previous guidance:

- WHC 2000 (71): For the record – Managing Records in NHS Trusts and Health Authorities.

Equality

This Code of Practice 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.

Review

The Code of Practice will be in place for 1 year before a review, unless legislation changes in which case it will be updated as appropriate. Following this, it is recommended that the code is reviewed every 5 years.

Standards and practice covered by the Code will change over time so this document will be 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 inquiries may lead to further specific records management requirements being set. Where that happens, the Inquiry will publish additional guidance on its website.

It should also be noted a review into the retention time for de-registered GP records is being conducted. 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, a copy is sent to Primary Care Services in NHS Wales Shared Service Partnership. 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.

Section 1:

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 in Wales.

This includes:

- records of Welsh patients treated by NHS organisations in England or Wales;
- records of patients treated on behalf of NHS Wales in the private healthcare sector;
- records of private patients treated on NHS Wales premises;
- records created by providers contracted to deliver NHS services in Wales (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 Local Authorities.

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 (Wales) Regulations 2002 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;
- emails;
- 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.

Section 2:

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, following the Caldicott Principles records keeping standards such as UK GDPR and associated legislation, the Common Law Duty of Confidentiality and other 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 Minister for Health and Social Services and all NHS organisations in Wales have a duty under the Act to make arrangements for the safekeeping and eventual disposal of all types of records. This includes a list of some of the bodies deemed to be public records bodies.

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. Further guidance on the definition of Welsh public records bodies can be found in the Government of Wales Act 2006, Section 148.

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 Wales Standard Contract 2006 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 (Wales) Regulations 2002.

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. The Information Commissioner regulates compliance with FOIA, and provides detailed guidance on the ICO's website.

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. The Information Commissioner regulates compliance with UK GDPR and related legislation. Detailed guidance on all aspects of data protection is available at www.ico.org.uk.

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. HIW are responsible for regulating this and HIW may have regard to the Code when assessing providers' compliance with this regulation.

The Welsh Language (Wales) Measure 2011

Legislation and policy in Wales support the Welsh language recording on patient and clinical records. The Welsh Language Measure gives the Welsh language official status in Wales and the requirement to actively offer services in Welsh is a key principle of the *More than just words* framework.

Further details on the protocol of which language to record a consultation between a practitioner and a service user can be found in Appendix III under 'Welsh and English language record guidance'.

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 Care Wales 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 across the UK, 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 Wales 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;
- Nursing and Midwifery Council;
- Social Care Wales.

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 health and social care staff should aim to follow 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 managers responsible for the records management function is directly accountable to or works in close association with the managers 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.

Training

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/service users' records or systems should be handled or used until training has been completed.

Training must include the use of electronic records systems and it must be undertaken through the generic and/or Health Board-wide training programmes, which can be department or context specific.

Health Boards with Information Governance training should also include Records Management in this training. Training should be complemented by appropriate organisation policies, procedures and guidance documentation.

All staff employed by the NHS in Wales will receive information on their personal responsibilities for record keeping in contracts of employment. This includes the creation, use, storage, security and confidentiality of health records. Appropriate training will be given to all health records staff on the systems used to maintain records and these will meet local and national standards. All new employees to NHS organisations in Wales will be given basic records practice training as part of the induction process.

Training to help identify records for permanent preservation that should be send to the Place of Deposit can be provided by The National Archives.

Professional standards of record keeping are governed by the associated Royal colleges. These standards should form part of the professional practice review.

2.5 Organisational policy

Each board, trust or 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 Section3 (1) of the Public Records Act 1958);
- provide a framework for supporting standards, procedures and guidelines and regulatory requirements (such as HIW and DHCW's IG 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.

Section 3:

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 Wales' 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.

If your DPIA identifies high risk that you cannot mitigate, you must consult the ICO before starting the processing.

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 Section 46 Code of Practice of the Freedom of Information Act 2000. 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 to 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	

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
Aneurin Bevan University Health Board	Organisation name	Creator
Midwifery	Service name	Creator
Patient case records surname A-F	Description of record	Subject or title
2000	Date or year of discharge	Date
2025	Date or 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

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 government security classifications to a small cohort of records. Whereas a large NHS Trust may want to use a security classification scheme.

Section 4:

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 NHS Wales's 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 Digital Preservation 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 NHS Wales's 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 offsite storage of physical 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.

Section 5:

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. All organisations have a responsibility to dispose of records at the end of their lifecycle (usually the end of the retention period).

Welsh public records bodies as defined GOWA 2006, Section 148 have a statutory duty under PRA 1958 to ensure that records of permanent or historic value are transferred to a Place of Deposit (PoD). Information and advice on transfer to a Place of Deposit is included in this section.

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

Under the PRA, public bodies are required to identify records of historical value and transfer them to a PoD by the time they are 20 years old. In most cases Welsh bodies will transfer their records to a PoD such as the local archive or the National Library of Wales. 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 than the original retention period. 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 Wales' individual staff and patient records

For NHS Wales's 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, if there is an ongoing operational need to retain. 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 a public body needs to keep any other type of record beyond 20 years, then approval must be sought separately from the Archives Advisory Council.

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. NHS England are progressing a UK-wide 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 the next edition of the code.

Organisations should always check current legislation. Any applications for approval should be made to The National Archives in the first instance by email to asd@nationalarchives.gov.uk.

Information:

Examples of the application of Archives Advisory Council retention approval

1. A trust wishes to check the retention period for cancer or oncology records. The Code states 30 years so the records are retained for 20 years without the need to apply the approval. The last 10 years would be covered by Archives Advisory Council 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 require Archives Advisory Council 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. Further guidance on selecting relevant records for permanent preservation can be found in Welsh Health Circular WHC (2000) 71 and in the Brief Guide to Transferring Records of Local Interest to a Place of Deposit.

As a rule, national organisations, will accession their records to The National Archives, and local Health boards, trusts and social care organisations will accession their records to the local PoD within Wales, as appointed by the Secretary of State for Culture, Media and Sport. If you are unsure where you should accession records, contact the Archives Sector Development Team at TNA. There is also an app to help bodies identify their PoD: Where do I deposit my records?

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 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.

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 can be offered.

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 NHS Wales 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 NHS Wales 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. Further guidance for transferring records to a PoD can also 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. This could be the county record office, or a specialised facility run by local authorities for the county. For example, Swansea Bay University Health Board deposits its records to the West Glamorgan Archive Service.

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 UK 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. An easily searchable version of this table can also be found online here.

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). 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.	
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 NHS 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 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. When considering new systems, data controllers should consider that commissioning systems with limited storage breaches UK GDPR, and new systems should have capacity to comply with UK GDPR.
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 Wales Demographics Service (WDS) 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. These records cannot be disposed of as they may require further services as they get older. If they have died, or transferred to a new practice, transfer the record to Primary Care Services in NHS Wales Shared Services Partnership (NWSSP) or the new provider respectively. Also refer to Appendix III: GP records.
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 NHS Wales' Primary Care Services in NWSSP. (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.

Record type	Retention period	Disposal action	Notes
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.
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.

Record type	Retention period	Disposal action	Notes
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.
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. The Controlled Drugs (Supervision of Management and Use) (Wales) Regulations 2008. 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. The Controlled Drugs (Supervision of Management and Use) (Wales) Regulations 2008.
Pharmacy prescription records.	2 years.	Review and destroy if no longer required.	A record of the prescription will also be held by NWSSP and their Primary Care Services 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 8 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.
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.
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 DHCW and its predecessors.	Delete with immediate effect.	Delete in line with DHCW instructions.	

Record type	Retention period	Disposal action	Notes
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. Please note: These may have potential PoD interest as what NHS Wales 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 or 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.
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 Welsh 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.	
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.

Record type	Retention period	Disposal action	Notes
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 NHS Wales 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 required 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 December 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.

Record type	Retention period	Disposal action	Notes
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.
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 health boards and 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.

Record type	Retention period	Disposal action	Notes
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.
Leases.	12 years.	Review and destroy if no longer required.	Retention begins at point of lease termination.

Record type	Retention period	Disposal action	Notes
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.
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.	

Record type	Retention period	Disposal action	Notes
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.
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.

Record type	Retention period	Disposal action	Notes
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.

Adopted persons health records

Notwithstanding any other centrally issued guidance by the Department of Health, the Welsh Government and Social Care Wales, 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-hold 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, 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 Standard contract (Wales) 2006 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 Primary Care Services within NHS Wales Shared Services Partnership.

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 Local Health Boards (LHBs) 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 LHB to ensure the CHC process runs effectively – an example being appointment letters asking the patient or service user to attend a panel. LHBs require access to health and care information to determine a patient or service user's entitlement (once the LHB has been notified).

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 Wales, in conjunction with the NWSSP and their PCS, 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 The Controlled Drugs (Supervision of Management and Use) (Wales) Regulations 2008.

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 31. 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. Further Advice from PCS can be found in the Practice Guidance Notes for Registration Links.

Individual funding requests (IFRs)

Similar to CHC, IFR cases are mainly administrative records, but also contain large amounts of personal or 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. The vision and strategy in the following documents shows the vision for integrated care records in Wales:

- A Healthier Wales;
- Well-being of Future Generations Act.

Depending on the agreements under which integrated records are established these may be subject to the Public Records Act. Generally, if an NHS Wales 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 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. Where this is proposed, controllers must assure themselves of the lawfulness of any proposed new usage under UK GDPR and Duty of Confidence. See also the section on integrated viewing technology and record keeping in the format section below.

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 UK 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 National Archives Wales 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, and other relevant laws such as the Common Law Duty of Confidentiality. 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 NWSSP and their PCS 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

Responsibility for offender health in HM Prison Services in Wales is held by local Health Boards. A national computer-based record created by the Ministry of Justice was created to facilitate the provision of care and the transfer of care records associated with inmate transfers throughout imprisonment. Digital Health and Care Wales (DHCW) have been helping Health Boards to facilitate the use of this system in Wales.

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 Wales premises

Where records of individuals who are not NHS Wales or social care funded are held in the record keeping systems of NHS Wales 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 Code of Confidentiality for Health and Social Care in Wales (2005).

Records relating to sexually transmitted diseases

Organisations that provide care and support under The National Health Service (Venereal Diseases) Regulations 1974 must be aware of the additional obligations to confidentiality these impose on employees and trustees of organisations. These organisations include NHS Trusts, LHBs, local authority public health teams and those providing services under NHS contracts in Wales.

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 accommodated accordingly. 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 Local Health Boards. 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 Wales 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 Wales 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.

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 patients' 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 transgender 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.

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.

Welsh and English language records guidance

Legislation and policy in Wales support the Welsh language recording on patient and clinical records. In terms of recording on patient and care clinical records, the following protocol is advocated as best practice:

English records:

- When a service user language is English all the records will be written in English by both English and Welsh language speaking practitioners.
- English service user/ English practitioner – the practitioner writes up the record note in English.
- English service user/ Welsh practitioner – the Welsh practitioner would undertake the consultation in English and the interaction would be recorded in English (the language of the interaction).

Bilingual records:

Bilingual records will be required for services users accessing services in Welsh in the following scenarios:

- Welsh service user/Welsh practitioner – a Welsh speaking service user receives a consultation in Welsh from a Welsh practitioner. The practitioner can write up the record note in English or in Welsh (the language of the interaction) and arrange for a full English translation to also be included within the record. If the service user requests a copy of the record in Welsh the English record will be translated and provided bilingually.
- Welsh service user/English practitioner – if a Welsh speaking service user receives a consultation from a practitioner in English the interaction will be recorded in English (the language of the interaction). If the service user request a copy of the record in Welsh the record will be translated and provided bilingually.

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. This 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.

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. NHS Wales and DHCW have an All Wales Email Use Policy which should be followed.

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 NADEXID 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 in Wales to another, 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.

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 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 Wales' due diligence. Using a 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.

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. Most NHS organisations' web sites in Wales are monitored and captured by the National Library of Wales and are stored in the UK Web Archive.

Appendix IV:

Records at contract change

Characteristic of new service provider	Fair processing required	What to transfer	Sensitive records
NHS Wales 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 Wales 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 Wales 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

Characteristic of new service provider	Fair processing required	What to transfer	Sensitive records
NHS Wales 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 Wales 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 Wales 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.	