Aneurin Bevan University Health Board

RECORDS MANAGEMENT CODE OF PRACTICE

N.B. Staff should be discouraged from printing this document. This is to avoid the risk of out of date printed versions of the document. The Intranet should be referred to for the current version of the document.

Status: Issue 1
Approved: Executive Team
Owner: Information Governance Unit

Issue Date:21 May 2021
Review date 20 May 2024
ABUHB/IMT/1043

Contents:

1. Introduction/Overview

The Records Management Code of Practice for Health and Social Care 2020 (from this point onwards referred to as the Code) is a guide for the practice of managing records. It has been adapted for use within Aneurin Bevan University Health Board (ABUHB) and replaces the current Non-Clinical and Clinical Record Retention Schedule and the former Health Records Management Policy. The guide also includes Public Health functions in local authorities and Adult Social Care.

The Code provides the Health Board with a framework for consistent and effective records management based on established standards. It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records. It also advises on how to design and implement a records management system including advice on organising, storing, retaining and deleting records.

2. Policy Statement

This Code is intended for use by staff within the Health Board to help deliver a practical approach and guidance to all records management in order to safeguard the Health Board and ensure compliance with current legislation. The Code replaces previous guidance listed below:

ABUHB Non-clinical and clinical record retention schedule

ABUHB Health Records Management Policy

HSC 1999/053 – For the Record - managing records in NHS Trusts and health authorities

HSC 1998/217 – Preservation, Retention and Destruction of GP General replacement for FHSL (94) (30)

HSC 1998/153 – Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice

In particular, the following should be noted:

There are a number of on-going inquiries including the Independent Inquiry into Historic Child Sex Abuse (IICSA) and the Infected Blood Public Inquiry (IBI). This means that records must not be destroyed until guidance is issued by the relevant Inquiry. Future inquiries may lead to further specific records management requirements being set.

3. Aims/Purpose

The Health Board and managers need to ensure that staff are enabled to follow the standards in this Code of Practice. This includes identifying any Health Board changes or other requirements needed to meet the standards, for example, the resources and tools required. Information Governance performance assessments form an integral part of our internal assessment against the standards.

The guidelines in this Code draw on published guidance from The National Archives (TNA) and best practice in the public and private sectors. It is further informed by lessons learnt and is designed to implement the recommendations of the Mid Staffordshire NHS Foundation Trust Public Inquiry relating to records management and transparency.

This Code must also be read in conjunction with the following:

Academy of Medical Royal Colleges' standards for the clinical structure and content of patient records

Professional Records Standards Body (PRSB) Structure and content of health and care records standards

Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (FOIA).

4. Objectives

The code is designed to ensure that the framework for records management is applied consistently across the Health Board and draws on best practice as well as ensuring that services meet the legal, professional and individual

responsibilities associated with record keeping. There are 3 important appendices that relate to the Code and which will be applied to ensure robust records management across the organisation:

- **Appendix I** - Information on Public Inquiries
- **Appendix II** - A retention schedule for different types of record (corporate and health)
- **Appendix III** -Detailed advice on managing different types and formats of records such as integrated care records and staff records.

5. Scope

The guidelines in this Code apply to NHS and Adult Social Care records where integrated with NHS patient records and will include the adoption of the Welsh Clinical Communication Information system (WCCIS). The guidelines include:

- Records of patients treated by NHS organisations
- Records of patients treated on behalf of the NHS in the private healthcare sector
- Records of private patients treated on NHS premises
- Adult Service User Records where there is integration with health services e.g. jointly held records and Local Health and Care Records
- Records held by local authorities such as public health records, contraceptive and sexual health service records
- Staff Records
- Complaints Records
- Corporate Records – administrative records relating to all functions of the organisation

The Code does not cover children's social care records. These are within the remit of the Department for Education.

Whilst not strictly covered by this guide, private providers who are engaged in undertaking NHS work on behalf of the organisation will also be expected to use this Code for guidance in relation to their records management.

6. Roles and Responsibilities

All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law. Health and care professionals also have professional responsibilities for example complying with the **Caldicott Principles** and **records keeping standards** set out by registrant bodies. Whilst every employee has individual responsibilities, the Health Board requires to have a designated member of staff who leads on records management.

There are legal obligations in terms of Records Management with which the Health Board must comply:

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 Health Board has a duty under the Act to make arrangements for the safekeeping and eventual disposal of all types of records.

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 whereby 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.

Freedom of Information Act 2000

The Freedom of Information Act (FOIA) governs the management of 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 the organisation to supply information through delivery of a good records management programme. Records managers must adhere to the code of practice on record keeping issued 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.

Data Protection Act 2018

The DPA18 supplements the UK GDPR in UK law. It 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 DPA18 principles are also relevant to the management of records. Under the DPA18 organisations may be required to undertake Data Protection Impact Assessments as set out in Section 3 of this Records Management Code.

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/service users, employment of staff and overall management.

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 that a claimant 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.

The main standard setting bodies are:

- Academy of Medical Royal Colleges
- British Medical Association
- General Medical Council
- Health and Care Professions Council
- Nursing and Midwifery Council
- Royal College of General Practitioners

Records management is a specific corporate responsibility within the Health Board. Records management must 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 has clear responsibilities and objectives and is adequately resourced to achieve them.

A designated member of staff e.g. the Head of Health Records has lead responsibility for health records management within the Health Board. Within different settings this will vary with responsibility lying with for example: Care Home Manager/Practice Manager. This lead role should be formally acknowledged and communicated throughout the Health Board. It is essential that the manager(s) responsible for the records management function (corporate and health records) is directly accountable to, or works in close association with, the manager(s) responsible for other information governance work areas.

As records management activities are undertaken throughout the Health Board, 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 Governance Development Groups (IDG's) (information working groups) and includes the centrally retained Information Asset Register which identifies the information asset owners and information governance stewards. These stewards will ensure that systems are used appropriately for the sharing and storage of information for the care of the patient but not without appropriate consent. The stewards will report any inappropriate record sharing/storage e.g. MS Teams.

7.0 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 a record that needs to be kept, such as clinical records. Other records will need to fulfil the criteria as being worth keeping, such as unique instances of a business document or email.

Declared records can be held in the 'business as usual' systems e.g. Clinical Workstation, SharePoint or they can be moved into a protected area such as an Electronic Document and Records Management System (EDRMS). ABUHB teams should only hold locally the records they need to conduct business.

Records and information relating to closed cases (clinical) may be kept locally within a department for a short period of time (e.g. community mental health facilities for a maximum of a year). This is in case a patient/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 whether digitised, electronic or paper.

7.1 Organising Records:

Record keeping systems must have a means of physically arranging or 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 (e.g. finance or HR) arranged by business functions; however, it is often linked to the Health Board's hierarchical structure.

Records should be arranged into a classification scheme, as required by ISO 15489 and the Lord Chancellor's Code of Practice. The business classification scheme can be anything from an arrangement of files and folders on a network to an Electronic Document Records Management System (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 must try to classify by function first. Once a recommended functional classification has been selected, the scheme can be further refined to produce a classification tree based on function, activity and transaction. For example:

Function: Corporate governance

Activity: Board minutes and associated papers
Transaction: April 2018-March 2019

The transaction can then be assigned a rule (such as retention period) a security status or other action based on the organisational policy. The scheme will enable appropriate management controls to be applied and support more accurate retrieval of information from record systems.

7.2 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**	**Recommend**
Creator	Accessibility	Coverage
Date	Identifier	Language
Subject	Publisher	
Title		

Box label	Local	Metadata
ABUHB	Accessibility	Coverage
Hospital/Service/locat	Organisation	Creator
Midwifery	Service	Creator
Patient case records		
surname A-F	Description	Subject/Tit
2000	Date/year of	Date
2025	Date/year of	Date

The above 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.

7.3 Management and Storage of Digital Records

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 authenticity of a record is dependent on a number of factors:

- Sufficient metadata to allow it to remain reliable, integral and usable
- 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 maintain effort with 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 cannot be said to be 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 Digital strategy will be developed over the next few years to ensure that the Health Board can meet this requirement.

Paper records can deteriorate over time - so can electronic 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.

These factors must be taken into account when purchasing new systems and software therefore consultation and

partnership working with the Digital Directorate is required to ensure that the requirements are met.

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'.

7.4 Managing Offsite Records

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 current guidance to identify and support the requirements for offsite storage of physical records is issued by The National Archives (TNA). 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 life cycle up to disposal.

Staff must conduct a DPIA if looking to start storing records offsite. 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 (e.g. change from destruction by pulping to destruction by shredding)
- If you end the service by bringing it in-house.
- The Data Controller must action all processing

7.5 Managing Paper Health Records

Health record storage areas should provide a safe working environment with secure storage that allows health records to be retrieved as and when required. These areas should only be accessible to authorised staff and should conform to agreed standards to protect records from damp, fire, flood and chemical contamination.

- Health records storage areas and office accommodation should conform to all
- current legislation and guidance in respect of health and safety
- Regular risk assessments are undertaken in line with the risk management strategy.
- Racking, where this is in use, is stable and of strong enough construction to
- support the weight of the health records and mostly complies with current
- health and safety regulations
- There are safety step ladders and stools appropriate to the number of staff employed and to the size of the different storage areas.
- The staff are trained in the manual handling procedures associated with the library areas.
- Equipment within the department conforms to the appropriate legislation and equipment checks are routinely conducted.
- Access to the libraries is restricted to authorised personnel. The keys/access codes to areas that are locked are made available to staff to facilitate the retrieval of health records during the out-of-hours service.
- The health records areas should be capable of accommodating the current needs and annual growth of health records.
- Health records must be stored securely when in clinical areas, offices and arrangements made within these areas to allow retrieval of records when required.

7.6 Appraisal

This section includes information on the destruction and deletion of records; reviewing records for continued retention once their minimum period for retention has expired; and the selection of records for permanent preservation. It also includes information and advice about the transfer of records to Gwent Archives.

Appendix I relates to Public Inquiries which should also be considered before destroying any records.

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.

Under no circumstances should a record or series be automatically destroyed or deleted.

Electronic records can be appraised if:

- They are arranged in an organised filing system
- They can differentiate the year of creation
- They can be organised by year of closure
- The subject of the record is clear
- If electronic 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 / delete
- Continued retention – this will require justification and documented reasons
- Permanent Preservation

If as a result of appraisal a decision is made to destroy or delete a record, there must be evidence of the decision. Best practice within the Health Board dictates that approval for destruction or deletion must be from the Clinical Council or sign off by the Medical Director in respect of health records. 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 Health Board.

7.7 Destruction of Paper Records

Paper records selected for destruction can be destroyed, subject to following ISO 15489-1:2016. Destruction is conducted in-house and under contract with a contracted offsite company. The Health Board is responsible for ensuring that the provider meets the necessary requirements and can evidence this. This evidence is checked as part of due diligence through the procurement framework.

Destruction provider companies provide a certification of destruction for the bulk destruction of records. This certification is linked to a list of records so that the Health Board 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/bags that do not provide certificates of destruction).

If in doubt, material should be treated as confidential and evidentially destroyed. Staff are reminded not to use the domestic waste or put records on a rubbish tip to destroy identifiable and/or confidential material, because they remain accessible to anyone who finds them**.**

7.8 Destruction of Digital Records

Destruction implies a permanent action. For digital records 'deletion' may be reversed and may not meet the standard as the information can/may be able to be recovered or reversed. Destruction of digital information is therefore more challenging. If an offsite company is used, the Health Board as the data controller must check with the ISO as part of the procurement as to 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 the DPA18. Their

advice is to only procure systems that will allow permanent deletion of records to allow compliance with the law.

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 Health Board is instructed by a court order.

The following are examples of when information cannot be destroyed or disposed of:

1. If it is subject to a form of **access r**equest (e.g. Subject Access Request, FOIA request)
2. If it is required for notified **legal** proceedings (e.g. court order), or where there is reasonable prospect of legal proceedings commencing (an impending court case), as this information will possibly be required for the exercising or defending of a legal right or claim
3. If it is required for a **Coroner's** Inquest
4. If it is of interest to a **Public Inquiry** (who will issue guidance to the Health Board 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.

7.9 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.

The Health Board have procedures and policies for any instances where it is necessary to maintain records for longer than the stated minimum, including:

1. Temporary retention
2. Public Inquiries
3. Ongoing access request (e.g. 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)
4. Where there is a continued business need beyond the minimum retention period, and this is documented in local policy
5. Where records contain personal data, the decision to retain must comply with the DPA18 principles. 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.
6. 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. For records that have a recommended retention period beyond 20 years, e.g. maternity records, these can be retained for longer as specified in Appendix II, in this case for 25 years.

7.10 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:

1. Enable the public to understand the working of the organisation and its impact on the population it serves
2. Preserve information and evidence likely to have long-term research or archival value
3. Records for preservation must be selected in accordance with the guidance contained in this Code, any supplementary guidance issued by TNA and local guidance from the relevant Place of Deposit (Gwent Archives) which, should always be consulted in advance.
4. 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:

1. Transfer to Archives - this class of records should normally transfer in its entirety to the Archive– trivial or duplicate items can be removed prior to transfer**.**

2. Consider transfer to Archivist- all, some or none of this class may be selected (as agreed with the Archivist).
3. No Archival Interest

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 Gwent Archives.

Where it is known that particular records will be transferred to the archives routinely, this should be noted in the records management policy (or equivalent) alongside the reason for the routine transfer. (Birth Registers/Operation Registers/Admission and Discharge Registers)

Likewise, one-off transfers should also be noted for reference. If records whether corporate or health are identified that are more than 20 years old it should be notified to the Health Records Department and it will be assessed and catalogued for transfer if appropriate and preserved locally until such time as it can be transferred. Board minutes, agendas should be routinely offered to the archives for permanent preservation as part of the public body history and Public Records Act.

7.11 Patient/Service user records for permanent preservation

Records of individual persons may also be selected and transferred to the Archives provided this is necessary and proportionate in relation to the broadly historical purposes of the Public Records Act 1958 and Archives 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. The Health Board has transferred early Mental Health (1919) and wartime records that have been found in past years. Patient/service user confidentiality will normally prevent use for many decades after transfer therefore the transfer of patient/ service users records should only be considered where one or more of the factors listed apply:

1. The organisation has an unusually long or complete run of records of a given type
2. The records relate to population or environmental factors peculiar to the locality
3. The records are likely to support research into rare or long-term conditions

4. The records relate to an event or issue of significant local or national importance e.g. Covid 19
5. The records relate to the development of new or unusual treatments or approaches to care and/or the organisation is recognised as a national or international leader in the field of medicine or care concerned
6. The records throw particular light on the functioning, or failure, of the organisation, or the NHS or social care in general (lookback exercises)
7. Any policy to select patient or service user records should only be agreed after consultation with appropriate clinicians, the Clinical Council 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.

7.13 Transfers of Records to the Place of Deposit

1. Records selected for permanent preservation should be transferred to Gwent Archives following discussion with the archivist and an assessment of the records. An Accession Notice will be provided once the Archives have catalogued the transferred records.
2. Once transferred to the Archives, records will still be owned by the Health Board and all relevant laws will apply. Individual records deposited with Gwent Archives are still protected by the DPA18, FOIA and duty of confidentiality.
3. If Gwent Archives holds records and access is requested, the Archivist will liaise with the Health Board before releasing any information (including any checks for subject access requests required by DPA18 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 Health Board must carry this out and inform the Gwent Archives of the result. The Health Board must make a decision on what information to release and where information is withheld, explain the reason why (except in exceptional circumstances e.g. a court order to the Gwent Archives)

8. 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. Training should be complemented by appropriate Health Board policies, procedures and guidance documentation.

All staff employed by the Health Board 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 the Department will be given basic records practice training as part of the induction process. Training in the specifics of health records management for staff out-with the Department will be provided through Records Awareness sessions conducted by Assistant Health Record Managers. Record keeping standards are promoted through the junior doctor induction programme.

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

9. Health and Care Standards Wales

The health board is required to meet set criteria for Effective Care Standard 3.5 Record Keeping. Adherence to the Code of Practice will ensure that the Health Board meets all the requirements of this Standard.

10. 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.

11. Review

The Code of Practice will be in place for 3 years unless legislation changes in which case it will be updated as appropriate.

12. References

Academy of Medical Royal Colleges - standards for the clinical structure and content of patient records
Access to Health Records Act 1990
British Medical Association
Caldicott principles
Consumer Protection Act 1987
DPA18 principles
e-Government Metadata Standard
FOIA
General Medical Council
GOV.UK
Human Tissue Authority
The Independent Inquiry into Child Sexual Abuse
Inquiry website
ISO 15489-1:2016
Local Government Act 1972
MHRA guidance
Mid Staffordshire NHS Foundation Trust Public Inquiry
HFEA guidance
Limitation Act 1980
Lord Chancellor's Code of Practice
National Cyber Security Centre (NCSC)
NHS BSA
NHS Resolution
Nursing and Midwifery Council
PRSB - Structure and content of health and care records standards
Public Records Act 1958
Royal College of General Practitioners
Royal College of Nursing
Royal College of Obstetricians & Gynaecologists
Royal College of Pathologists
Royal Pharmaceutical Society
Royal College of Physicians
Social Care Wales
NWIS Information Standards & Business Analysis
TNA offsite storage of physical records

13. Appendices

Appendix 1 – Records relating to Inquiries
Appendix 11 – Retention Schedule for Records
Appendix 111 – Records Management for specific types of Records

Appendix 1 - Records Relating to 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, discuss any inquiries with Gwent Archives to take account of exceptional local circumstances and defunct record types not listed here.

Currently 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:

1. The Independent Inquiry into Child Sexual Abuse (IICSA) - 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

2. The Infected Blood Inquiry - Further information about the records required can be found on the Inquiry website. There is currently an embargo on records destruction for a five year term or until the publication of the findings and recommendations of the Inquiry.

Appendix 11 – Retention Schedule for Records:

This Appendix sets out the retention period for different types of records relating to health and care. Where indicated to refer to Appendix 111 this sets out further detail relating to the management of specific types and formats of records.

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.

Retention periods begin when the record ceases to be operational. This is usually at point of discharge from care, when the record is no longer required for current on-going business, or the patient/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.

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.
>
> Review and dispose of if no longer required – Dispose of refers to the secure destruction of a record OR the transfer to Gwent Archives for permanent preservation. A certificate of transfer will be provided as proof of transfer (and can act as evidence of disposal).
>
> Review and consider transfer to Gwent Archives – This refers to records that are more likely to be transferred to the Gwent Archives subject to their agreement.
>
> Review and transfer to Gwent Archives – This refers to records that should be transferred to Gwent Archives.

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 e.g. the case where the records relate to rare conditions such as Creutzfeldt-Jacob disease or new cancer treatments.

Record Type	Retention Period	Disposal Action	Notes
Adult health records not covered by any other part in this schedule (includes medical illustration records such as X-rays and scans as well as video and other formats. Also includes care plans and all therapy records – dietetics, SALT, Physio, OT, Podiatry and Orthotics)	8 years	Review and consider transfer to Gwent Archives	Records involving pioneering or innovative treatment may have archival value. 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 vising 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 26 if the patient was 17 when treatment ended.
Clinical Records that predate the NHS (July 1948)		Review and transfer to Gwent Archive	Health Records to be contacted and will arrange review and transfer. Records not selected by the Gwent Archive must be securely destroyed.
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 electronic as well as paper records, with a log kept of destructions. 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.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
General Dental Services records	6 years	Review and destroy if no longer required	This covers the period required by the Dental Contract and financial audit requirement. (It is recognised the Dental Services Contract states to retain records for 2 years (Discussions taking place to change the Contract to reflect this Code).
GP Patient Records – Living patients	Continual Retention	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 Welsh 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. If they have died, or transferred to a new Practice, transfer the record to NHSE or the new Provider respectively. These records cannot be disposed of as

			they may require further services as they get older. (***Also see Appendix III - GP Records***).
GP Patient Records/deceased patients	10 years	Review and destroy if no longer required	Confidentiality generally ceases to apply after 10 years and retention covers requirements of the Limitation Act 1980. (Also refer to Appendix III GP Records).
Integrated Records – All organisations contribute to the **same single instance** of the record	Retain for period of longest specialty	Review and consider transfer to Gwent Archives	The retention will vary depending upon which type of health and care services 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 Gwent Archives	This is where all organisations contribute into the same record system but have their own area to contribute to and the system shows a contemporaneous view of the patient record.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Integrated Records – All **organisations keep their own records**, but enable	Retain for relevant specialty period	Review and consider transfer to Gwent Archives	This is the most likely model currently in use. Organisations keep their own records on their patients/service users but can grant *view only* access

them to be viewed by other organisations			to other organisations, to help them provide health and care to patients/ service users.
Mental Health Records including psychology records	20 years, or 8 years after death	Review and consider transfer to Gwent Archives	Covers records made under the Mental Health Act 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 judgement).
Child & Adolescent Mental Health records	Up to 25th or 26th birthday	Review and destroy if no longer required	Retain until 25th birthday, or 26 if the patient was 17 when treatment ended.
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.
Oncology/Cancer Records – any patient*	30 years, or 8 years after death	Review and consider transfer to Gwent Archives	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.
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 organisation/s if the running of the service changes hands.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Sexual Health/Contraception/Family Planning/Genito-Urinary Medicine (GUM)	8 or 10 years	Review and destroy if no longer required	8 years for basic retention requirements increasing 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 111*** – Records dealt with under Sexually Transmitted Disease Directions 2000).
HFEA Records – Treatment provided in licenced centres	3, 10, 30 or 50 years	Review and destroy if no longer required	These retentions are set out in HFEA guidance.
Creutzfeldt-Jakob Disease – Patient Records	30 years or 8 years after death	Review and dispose of if no longer required	Diagnosis records must be retained for clinical care purposes.
Long-term illness, or illness that may reoccur –Patient records	20 years, or 8 years after death	Review and dispose of 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.
PHARMACY			

Information relating to controlled drugs*	See notes	Review and destroy if no longer required	NHS England has issued guidance stating that locally held controlled drugs information should be retained for seven years. NHS BSA will hold primary data for 20 years and then review it. (***Also refer to***
Pharmacy Prescription Records	2 years	Review and destroy if no longer required	A record of the Prescription will also be held by NHS BSA and there will be an entry on the patient record.
PATHOLOGY			
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Pathology Reports/ Information about samples	Refer to notes	Review and consider transfer to Gwent Archives.	This Code is concerned with the information about a specimen or sample. The length of time clinical material (e.g. a specimen) is stored will drive how long the information relating to it is retained. Sample retention can be for as long as there is a clinical need to hold it. Reports should be stored on the patient file. It is common for Pathologists to hold duplicate records. For clinical purposes, these should be retained for eight years after discharge or until a child's 25th birthday. If information is retained for 20 years, it must be appraised for historical value, and a

			decision made about its disposal. (***Also refer to Appendix III specimens and samples).***
EVENT AND TRANSACTION RECORDS			
Blood Bank Register*	30 years minimum	Review and consider transfer to Archivist	Need to be disposed of if there is no on-going need to retain them subject to any transfer to the Archivist.
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 Archivist	Refer also 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 8 years. Some staff keep hardback diaries of their appointments/business meeting. If these contain no personal data they can be disposed of after two years.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Clinical Protocols*	25 years	Review and consider transfer to Archivist	Clinical protocols may have preservation 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 NWIS/WISB and its predecessors	Delete with immediate effect	Delete in line with NWIS/WISB instructions	
Destruction Certificates, or Electronic Metadata destruction stub, or Record of clinical information held on physical media	20 years	Review and consider transfer to Archivist	Destruction Certificates created by public bodies are not covered by a retention instrument (if they do not relate to patient care) there is no need to accession them. They need to be destroyed after 20 years.
Equipment Maintenance Logs	11 years	Review and destroy if 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 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 Archivist	10 years from the end of the year to which they relate.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
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.
Requests for care funding – ***NOT ACCEPTED***	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record. NB: These may have potential archival interest as to what the NHS/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/illness detected is returned	10 years	Review and destroy if no longer required	Where Cancer is detected, refer to the Cancer/Oncology schedule.
Screening – Children	10 years or 25th birthday	Review and destroy if no longer required	Treat as a child health record and retain for either 10 years or up to 25th birthday, whichever is the LONGER.
Smoking cessation	2 years	Review and destroy if no longer required	Retention begins at the end of the 12-week quit period.
Transplantation Records*	30 years	Review and destroy if no longer required	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.
Recorded Conversations– which may be needed later for clinical negligence or other legal purposes*	6 years	Review and destroy if no longer required	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980. Further guidance is issued by NHS Resolution.

Record Type	**Retention Period**	**Disposal Action**	**Notes**
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	
BIRTHS, DEATHS & ADOPTION RECORDS			
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 Archives	Where registers of all births that have taken place in a particular hospital/birth centre exist, these will have archival value and should be retained for 25 years and offered to the Archivist at the end of the retention period. Information is also held by the Welsh Birth Notification Service electronic system. Other information about a birth must be recorded in the maternity care record.
Body Release Forms*	2 years	Review and destroy if no longer required	
Death - Register information sent to the General Registry Office on a monthly basis*	2 years	Review and consider transfer to Archivist	A full dataset is available from ONS.

Record Type	**Retention Period**	**Disposal Action**	**Notes**
Death - Register information sent to the General Registry Office on a monthly basis*	2 years	Review and consider transfer to Archivist	A full dataset is available from ONS.
Local authority Adoption Record (usually held by the LA)*	100 years	Review and consider transfer to Archivist	The local authority Children's Social Care Team hold the primary record of the Adoption process and Community paediatricians in secondary care. Consider transferring to Archives only if there are known gaps in the primary local authority record, or the records pre-date 1976. (See Appendix III Adoption Records)
Mortuary Records of deceased persons	10 years	Review and consider transfer to Archivist	Retention begins at the end of the year to which they relate.
Mortuary Register*	10 years	Review and consider transfer to Archivist	
NHS Medicals for Adoption Records*	8 years or 25th birthday	Review and consider transfer to Archivist	The health reports will feed into the primary record held by the local authority. This means that adoption records held in the NHS relate to reports that are already kept in another file, which is kept for 100 years by the relevant agency and/or local authority. Consider transferring to Archivist 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. Local Records of post mortem will therefore not need to be kept for the same extended time period.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
CLINICAL TRIALS & RESEARCH			
Advanced Medical Therapy Research - **Master File**	30 years	Review and consider transfer to Archivist	Further guidance can be found on GOV.UK.
Clinical Trials – Master File of a trial authorised under the European portal, under Regulation 536/2014	25 years	Review and consider transfer to Archivist	For clinical trials records retention refer to the MHRA guidance.
European Commission Authorisation (certificate or letter) to enable marketing and sale within EU member state's area	15 years	Review and consider transfer to Archivist	

Research - Datasets	No longer than 20 years	Review and consider transfer to Archivist	
Research – Ethics Committee's documentation for research proposal	5 years	Review and consider transfer to Archivist	Further guidance can be found on the HRA website. This category applies to minutes and papers of RECs that are not held centrally by HRA. Data must be held for sufficient time to allow any questions to be answered. Data may not need to be kept once the purpose has expired. For more significant research, an archivist may be interested in holding the research. It is best practice to consider this at the outset of any research, as orphaned personal data can cause a data breach (An orphaned record is a record which is from a service or organisation that ceases to exist and has no known successor).
Research – Ethics Committee's minutes and papers	As soon as is practically possible	Review and consider transfer to Archivist	Retention period begins from the year to which they relate and can be as long as 20 years. Committee papers must be transferred to archives
Record Type	**Retention Period**	**Disposal Action**	**Notes**
CORPORATE GOVERNANCE			

Board Meetings*	Up to 20 years	Review and transfer to Archivist	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 Archives or TNA (for National Bodies).
Board Meetings (Closed Boards)*	Up to 20 years	Review and transfer to Archivist	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 Archivist	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 Archivist	
Committees (Minor) – Not listed in Scheme of Delegation*	6 years	Review and consider transfer to Archivist	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 Archivist	Contact Gwent Archives to arrange review and transfer. Records not selected by the Archives must be securely destroyed.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Data Protection Impact Assessments (DPIAs)	6 years	Review and destroy if no longer required	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one -off, then 6 years from completion.
Destruction Certificates or Record of Information held on destroyed physical media	20 years	Review and dispose of if no longer required	Where a record is listed for potential transfer to archivist 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 Stub/s			Refer to Destruction Certificates.
Incidents – Serious	20 years	Review and consider transfer to Archivist	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 Archivist	These include independent investigations into incidents. These may have permanent retention value so consult with the local Archives. 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.
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 Archivist	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 Archives
Quarterly reviews from NHS Trusts/Health Boards	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	Permanent retention	Review and consider transfer to Archives	
Health Board Submission forms	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980
COMMUNICATIONS			
Intranet Site*	6 years	Review and consider transfer to Archivist	
Patient Information leaflets	6 years	Review and consider transfer to Archivist	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 Archivist	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Public Consultations	5 years	Review and consider transfer to Archivist	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 Archivist	The Archivist may be able to receive these by a regular crawl. Consult with the Archives on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken.
STAFF RECORDS/ OCCUPATIONAL HEALTH/ ESTATES			
Building Plans, including Records of major building works	Lifetime (or disposal) of building plus 6 years	Review and consider transfer to Archivist	Building plans and records of works are potentially of historical interest and where possible, should be kept and transferred to the local Archives
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.
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.

Equipment monitoring – general testing and maintenance work	10 years	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.
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Leases	12 years	Review and destroy if no longer required	Retention begins at point of lease termination.
Minor Building works	6 years	Review and destroy if no longer required	Retention begins at the point of WORKS COMPLETION.
Photographic Collections – Service locations, events and activities	Up to 20 years	Review and consider transfer to Archivist	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 Waste	30 years	Review and destroy if no longer required	Retention begins at the CREATION of the waste.
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 Archives	Retention period begins at the END of INSTALLATION period.
FINANCE			
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 Archivist	These may already be in the financial accounts and may be captured in other reports/records/ committee papers. Benefactions, endowments, Trust Fund/Legacies should be offered to the local archives
Record Type	**Retention Period**	**Disposal Action**	**Notes**
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 Archivist	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with Board Papers for that year to keep a complete set of governance papers.
Financial Transaction records	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Invoices	6 years from end of the financial year they relate to	Review and destroy if no longer required	
Petty Cash	2 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
Private Finance Initiatives (PFI) files	Lifetime of PFI	Review and consider transfer to Archivist	Retention begins at the END of the PFI agreement. This applies to the key papers only in the PFI.
Record Type	**Retention Period**	**Disposal Action**	**Notes**

Staff Salary Information/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			
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 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 sent 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 Archivist	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).
Record Type	**Retention Period**	**Disposal Action**	**Notes**
Litigation Records	10 years	Review and consider transfer to Archivist	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 Archives.
IntellPatents, Trademarks, Copyright, IP	Lifetime of Patent, or 6 years from end of licence/ action	Review and consider transfer to Archivist	Retention begins at the END of lifetime or patent, or TERMINATION of licence/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 111 - Types of Records

This Appendix provides detailed advice on records management relating to **specific types** of records e.g. 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 e.g. emails, cloud-based records and scanned records.

Adopted Persons Health Records

Notwithstanding any other centrally issued guidance, 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 and the Community Paediatricians perform this function on behalf of the Health Board.

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 Health Board, there must be a means by which the Welsh Ambulance Service 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. Patient/service user held records most commonly in use within maternity should be subject to a risk assessment because the record legally belongs to the Health Board, and if required, the

Health Board must be able to get it back. There is a risk that patient/service user held records could be tampered with or altered in an unauthorised way so careful consideration needs to be given to this decision.

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 electronic 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. Complaint information should never be recorded in the clinical 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/service user and the health and care team.

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/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. Staff should be aware that where there is a complaint or Serious Incident, the patient record must be passed to the Health Records Department for scanning within 24 hours and on no account should it be passed around

to multiple personnel for a response before being digitised. This practice safeguards the Health Board and its staff.

Health and care organisations should have a local policy to follow with regards to complaints, covering how information will be used once any complaint is raised, and after the complaint has been investigated, regardless of outcome. The ICO has also issued guidance on complaints files and who can have access to them, which will drive what must be stored in them.

Contract Change Records

Once a contract ends, any service provider still has a liability for the work they have done and, as a general rule, at any change of contract the records must be retained until the time period for liability has expired.

In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision (for current cases) upon termination of the contract. It is also the case that after the contract period has ended, the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

When a service is taken over by a new Provider, the records of the service (current and discharged cases) all transfer to the new Provider (unless directed otherwise by the Commissioner of the service). This is to ensure that the records for the service remain complete and enable patients/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 e.g. Gwent Healthcare NHS Trust – Aneurin Bevan University Health Board. This may also include consideration of the identity of the legal entity, which must manage the records.

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 the DPA18 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 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).

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/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/ 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 to ensure the CHC process runs effectively – an example being appointment letters asking the patient/service user to attend a panel. There may be a requirement for access to health and care information to determine a patient/service user's entitlement to services.

Consent is not required to process personal data in relation to CHC but consent will be required to satisfy the duty of confidence. Health Boards will need to have systems in place to allow for the safe and secure sharing of patient/service user information with relevant partners as necessary, and to inform patients/service users of how their data will be used as part of this process. Electronic viewing and sharing of records may be preferable to paper copies being printed and used for CHC, due to the risk of accidental loss or disclosure.

Controlled Drugs Regime

The Health Board 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

https://www.legislation.gov.uk/wsi/2008/3239/made/data.pdf 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 electronic 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 electronic records is referred to as E-Disclosure or E-Discovery. The relevant rule for disclosure and admissibility of evidence is given in the Ministry of Justice's Civil Procedure Rules' Rules and Practice Directions as Rule 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.

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/electronic 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 electronic) 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 deregistration. A review is taking place to ascertain how long this period should be 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. For further information on GP records please see:

http://www.primarycareservices.wales.nhs.uk/sitesplus/documents/1150/GOOD%20PRACTICE%20GUIDE%20-%20Final%20Feb16.pdf

Individual Funding Requests (IFRs)

Similar to Continuing Healthcare, IFR cases are mainly administrative records, but also contain large amounts of personal/confidential patient information and as such, should be treated in the same way as CHC records.

As IFRs are unique to an individual, it may be that the care package given to the patient/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 Archivist. Local discussions should be held with the Gwent Archives 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.

APPENDIX 3

Integrated Records

Since 2013, there has been an increase in the number of initiatives promoted and launched that involve integrated records. There has also been recognition nationally that joined up delivery of health and care services can increase the quality of care delivered, and also deliver those services more efficiently. Examples include:

A Healthier Wales - https://gov.wales/sites/default/files/publications/2019-10/a-healthier-wales-action-plan.pdf

Well-being of Future Generations Act https://gov.wales/sites/default/files/publications/2019-08/well-being-of-future-generations-wales-act-2015-the essentials.pdf#:~:text=The%20Wellbeing%20of%20Future%20Generations%20%28Wales%29%20Act%20is,prevent%20problems%20and%20take%20a%20more%20joined-up%20approach.

Welsh Community Care Information System https://nwis.nhs.wales/systems-and-services/in-the-community/digital-community-care-record/

Depending on the agreements under which integrated records are established these may be subject to the Public Records Act. Generally if an NHS Body is at least partly responsible for the creation and control of the record, it will normally be considered a public record to be managed in accordance with the Act. The Archives should be notified that this is the case.

The options for ABUHB and other organisations who co-produce healthcare 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:

- All organisations contribute to a single record, creating the only record for that patient/service user. Consideration must be given to how this is managed in practice (e.g. 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).
- 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)All organisations keep their own records, but allow others to view their records, but not amend/add to (retain for each specialty as applicable – because they are not merged). (Also refer to the section on Integrated viewing technology and Record Keeping.)

APPENDIX 3

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 the 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.

Patient/Service User Held Records

Some clinical or care services may benefit from the patient/service user holding their own record e.g. maternity services. Where this is considered to be the case a risk assessment must be carried out by the service on behalf of the Health Board. 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 Health Board and include a return address if they are lost. Upon the discharge of the patient/service user, the record must be returned to the Health Board which has been involved in the person's care.

The Health Board 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 Health Board (e.g. district nursing).

A copy can be provided if the individual wishes to retain a copy of the records through the Subject Access Request process. In cases where the individual retains the actual record after care, the Health Board must be satisfied it has a full record of the contents.

Prison Health Records

The overall responsibility for the development of prison healthcare in the **public** sector prisons in Wales rests with the Welsh

Government. Accountability for the planning of health services for prisoners is held by NHS Wales, as for all other citizens of Wales. However, this responsibility and accountability can only be exercised in partnership with the National Offender Management Service (NOMS) and the Prison Service.

The principal aim of the partnership between the Welsh Government and NOMS/the Prison Service is to **provide access to the same quality and range of health care services as the general public receives from the NHS in Wales**.
http://www.wales.nhs.uk/governance-emanual/healthcare-services-for-prisoners

A significant number of paper records still remain and some offender health services operate a mix of paper and electronic health 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/service user is sent to prison the GP 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 deregistered GP records, with a view to further retention (with justification) and a potential transfer to the archives subject to their approval.

Private Patients treated on NHS premises

Where records of individuals who are not NHS or social care funded are held in the record keeping systems of the Health Board 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 **Confidentiality**: **Code of Practice for Health and Social Care in Wales**
http://www.wales.nhs.uk/sites3/documents/950/codeofpractice.pdf#:~:text=Confidentiality%3A%20Code%20of%20Practice%20for%20Healt

h%20and%20Social,authorities%20operating%20in%20Wales%20concerning%20confidentiality%20and%20the

Records relating to Sexually Transmitted Diseases

The Health Board provides care and support under the WG Strategic Framework for Promoting Sexual Health in Wales: http://www.wales.nhs.uk/sitesplus/documents/888/wagstrategicframework.pdf

Staff must be aware of the additional requirements relating to confidentiality these records impose on the Health Board. This includes the Health Board, GP's, local authority public health teams and any other organisation providing services under contract.

This obligation differs from the duty of confidentiality generally because it prohibits some types of sharing but enables sharing where this supports treatment of patients/service users. For this reason, it is recommended that services dealing with sexually transmitted diseases partition their record keeping systems to comply with the Framework and more generally to meet patient/ service users expectations that such records should be treated as particularly sensitive.

Secure Units for Patients Detained Under the Mental Health Act 1983

Mental Health Units operate on a low, medium and high-risk category basis. Not all patients on these units will have been referred via the criminal justice system. Some patients may be deemed a risk under the Mental Health Act and will need to be accommodated accordingly. Some patients may be high-risk due to the nature of a crime they have committed because of their mental health and therefore will need to be treated in a high secure hospital. 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.

Specimens and Samples

The retention of human material is covered by this Code, as some specialities will include physical human material as part of the patient/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 and/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 within the Health Board 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 is also potentially expedient to do so.

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 Health Board 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 departments 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 electronic current staff files.

Where a department 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

Transgender Records

Some patients may undergo medical treatment to change their gender. Records relating to these patients/service users are often seen as more sensitive than other types of medical records, and the use and disclosure of the information contained in them is subject to the Gender Recognition Act 2004.

There are established processes in place with WDS for patients undergoing transgender care in relation to the NHS number and the closing and opening of new records. In practice, nearly all actions relating to transgender records will be based on explicit consent under common law. 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 e.g. a patient may not be called for a gender specific screening programme. Any decisions made regarding their record must be respected and the records actioned accordingly.

A patient/service user can request that their gender be changed in a record by a statutory declaration but this does not give them the same rights as those the Gender Recognition Act 2004. 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/ service user. It is important to discuss with the patient/service user what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record. The content of the new record will be based on explicit consent under common law.

Witness Protection Health Records

Where a record is that of someone known to be under a witness protection 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 witness protection, the individual will be given a new name and NHS Number, so the records may appear to be that of a different person.

Youth Offending Service Records

Due to the nature of youth offending it is common for very short retention periods to be imposed on the general youth offending record. For purposes of clinical liability and for continuity of care the health or social care portion of the record must be retained as specified in this Code, which will generally be until the 25th birthday of the individual concerned.

Format of record

Bring Your Own Device (BYOD) created records

Any record that is created in the context of health and care business is the intellectual property of the employing organisation and this extends to information created on personally owned computers and equipment. This in turn extends to emails and text messages sent in the course of business on personally owned devices from personal accounts. They must be captured in the record keeping system if they are considered to fall within the definition of a record.

When an individual staff member no longer works for the Health Board, any information that staff take away could be a risk to the organisation. If this includes personal data/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 managing 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. The Health Board 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 electronic 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 DPA18 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/service user's rights.

Email and Record Keeping Implications

Email is now seen as a communication tool used every day by all levels of staff in organisations. They often contain business (or in some cases clinical) information that is not captured elsewhere and so need to be managed just like other records. The National Archives has produced guidance on managing emails but also refer to the Health Board policy:

http://howis.wales.nhs.uk/sitesplus/documents/866/ABHB_IM%26T_0167%20Email%20Policy_Issue%203.pdf

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. Emails are an important part of the corporate record and are subject to the Public Records Act, the Data Protection Act and the Freedom of Information Act. Therefore they need to be managed in a way that meets legislative requirements.

Staff will need to:

- **define** clearly which emails need to be kept for business or historical value
- **communicate** simply and often to users the rules for what emails to keep
- **keep** emails with related digital information in a shared corporate information management system
- **limit** what users can keep in personal email accounts by the use of:
  – email account quotas OR
  – automatic deletion after a set period of time
- 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 the Health Board needs to:
- Undertake periodic audits of working practice to identify poor practice

- Have a policy in place that covers email management
- 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 the Health Board 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 (e.g. a patient has indicated they will take the Health Board to court)
- A Subject Access Request (known or reasonably expected)
- Freedom of Information 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 place of deposit.

The NADEX ID 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 ABUHB to another NHS organisation, they must ensure that no sensitive data relating to ABUHB is transferred. It is good practice for staff to review their emails and ensure that business emails that support business dealing are provided for storage within the organisation

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.

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, the Health Board 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/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 Archives 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 electronic, can be admissible as evidence.

The British Standards Institute has published a standard that specifies the method of ensuring that electronic information remains authentic. The standard deals with both 'born digital' and scanned records. The best way to ensure that records are scanned in accordance with the standard is to use a supplier or service that meets the standard following a comprehensive procurement exercise, which complies with NHS due diligence. For local scanning requirements or for those records where there is a low risk of being required to prove their authenticity, the Health Board decided to do their own scanning following due diligence and internal compliance processes. This was subject to a business case being drawn up and approved, and procurement rules followed to purchase the necessary equipment, hardware and software.

Where scanned records have been digitised and the appropriate quality checks completed, the paper original is destroyed, unless the format of the original has historical value, in which case consideration is given to keeping it with a view to permanent transfer. Where paper is disposed of post-scanning, this was as part of a decision making process by the former Health Records 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 using commonly available tools.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 schedule

Social Media

Where social media is used as a means of communicating information for business purposes or it is a means of interacting with clients, it may be a record that needs to be kept. Where this is the case, information must be retained within the record keeping system. This may not necessarily mean that the social media must be captured but rather the information of the activity through transcription or periodic storage.

Website as a Business Record

As people interact with our public facing services, more commonly it is the internet and websites in particular that provide information, just as posters, publication and leaflets previously did. A person’s behaviour may be a result of interaction with a website and it is considered part of the record of the activity.

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate or there must be some other method to recreate what the website or intranet visitor viewed. It may be possible to arrange regular crawls of the site with the relevant Archives but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record.