Information Governance Alliance

Records Management Code of Practice for Health and Social Care 2016

Information Governance Alliance

Contents

List of Figures

List of Tables

List of Abbreviations

AoMRC	Academy of Medical Royal Colleges
CQC	Care Quality Commission
DIRKS	Design and Implementation of Record Keeping Systems
DH	Department of Health
DPA	Data Protection Act 1998
FOI	Freedom of Information
FOIA	Freedom of Information Act 2000
GP	General Practitioner
HSCIC	Health and Social Care Information Centre
ICO	Information Commissioner's Office
IG	Information Governance
IGA	Information Governance Alliance
ISO	International Organization for Standardization
NHS	National Health Service
PoD	Place of Deposit
PRSB	Professional Records Standards Body
TNA	The National Archives

Foreword

The Records Management Code of Practice for Health and Social Care 2016 has been published by the Information Governance Alliance (IGA) for the Department of Health (DH).

This Records Management Code of Practice for Health and Social Care 2016 (from this point onwards referred to as the Code) is a guide for you to use in relation to the practice of managing records. This Code is relevant to organisations who work within, or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where there is joint care provided within the NHS.

The Code is based on current legal requirements and professional best practice. It will help organisations to implement the recommendations of the Mid Staffordshire NHS Foundation Trust Public Inquiry[1] relating to records management and transparency.

The Code was drafted by a working group of representatives from the Information Governance Alliance, the Health and Social Care Information Centre, NHS England, the Department of Health, The National Archives and from a range of NHS and social care organisations, including Acute and integrated Mental Health Trusts, Clinical Commissioning Groups, GP practices and professional bodies. For details of those involved, please see Appendix One.

The Code is a key component of information governance arrangements for the NHS. Standards and practice covered by the Code will change over time so this document will be reviewed regularly and updated as necessary.

This Code of Practice replaces the previous guidance listed below:

- Records Management: NHS Code of Practice: Parts 1 and 2: 2006, revised 2009
- HSC 1999/053 – For the Record
- HSC 1998/217 – Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients (Replacement for FHSL (94)(30))
- HSC 1998/153 – Using Electronic Patient Records in Hospitals: Legal Requirements and Good Practice.

The Code forms part of a series of information governance guidance including the DH published Confidentiality: NHS Code of Practice[2] and the Information Security Management: NHS Code of Practice[3].

This Code must also be read in conjunction with the Academy of Medical Royal Colleges' Standards for the clinical structure and content of patient records[4] and the 'Lord

---

[1] http://webarchive.nationalarchives.gov.uk/20150407084003/http://www.midstaffspublicinquiry.com/report

[2] NHS Code of Practice on Confidentiality: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

[3] Information Security Management: NHS Code of Practice: https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice

[4] Standards for the clinical structure and content of patient records: https://www.rcplondon.ac.uk/projects/outputs/standards-clinical-structure-and-content-patient-records

Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000'[5] (FOIA).

At the time of writing the Independent Inquiry into Child Sexual Abuse (IICSA), chaired by Hon. Dame Lowell Goddard, has 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.

This includes children's records and any instances of allegations or investigations or any records of an institution where abuse has, or may have occurred[6]. Future inquiries may lead to specific records management requirements. If that happens we will publish additional guidance on our website.

This document is endorsed by the following organisations:

The Archives & Records Association (ARA)
Institute of Health Records and Information Management (IHRIM)
Information and Records Management Society (IRMS)
The National Archives (TNA).

[5] https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf
[6] Full details of the scope can be found on the Inquiry website www.iicsa.org.uk

Section 1: Regulatory Framework

Types of Record Covered by the Code

The guidelines in this Code apply to NHS records, including records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records, regardless of the media on which they are held. This includes records of staff, complaints, corporate records and any other records held in any format including both paper and digital records. The guidelines also apply to Adult Social Care records where these are integrated with NHS patient records.

Organisations that process data under the Health and Social Care Information Centre's (HSCIC) Code of practice on confidential information[7] should use this Code. This is because there is an expectation that the records management considerations highlighted in the HSCIC Code of practice on confidential information will be guided by this Code.

What is a record?

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management[8] defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'.

The Data Protection Act 1998 (DPA) S68(2) defines a health record which 'consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'.

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

Function:

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

Format:

- Photographs, slides, and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc
- E-mails
- Computerised records

[7] http://systems.hscic.gov.uk/infogov/codes/cop
[8] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542

- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient) such as Twitter and Skype
- Websites and intranet sites that provide key information to patients and staff.

Introduction

The guidelines in this Code draw on published guidance from The National Archives (TNA) and best practice in the public and private sectors. The guidelines provide a framework for consistent and effective records management that is based on established standards and are integrated with other information governance work areas such as confidentiality and information security.

All organisations and managers need to enable staff to conform to the standards in this Code. This includes identifying organisational changes or other requirements needed to meet the standards, for example the resource required (such as people, money and the correct tools). Information Governance performance assessments, such as the HSCIC hosted Information Governance Toolkit[9], and own organisation management arrangements will help you identify any necessary changes. Those responsible for monitoring overall performance within parameters, for example NHS England and the Care Quality Commission (CQC)[10], help in ensuring that effective management systems are in place.

General Context

Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958[11]. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. This applies regardless of the records format.

The Public Records Act 1958 requires that all public bodies have effective management systems in place to deliver their functions. For health and social care, the primary reason for managing information and records is for the provision of high quality care. The Secretary of State for Health and all NHS organisations have a duty under this Act to make arrangements for the safe keeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public Records, who is answerable to Parliament.

Public health and social care records, where a local authority is the provider, must be managed in accordance with the requirement to make proper arrangements under Section 224 of the Local Government Act 1972[12].

The NHS Standard Contract notes a contractual requirement to manage records for those health and social care records in organisations that are not bound by the Public Records Act 1958 or the Local Government Act 1972[13].

The FOIA[14] and the DPA[15] have records management codes of practice that recommend the systems and policies that must be in place to comply with the law. Other legislation

[9] Information Governance Toolkit: https://www.igt.hscic.gov.uk/
[10] CQC Standards http://www.cqc.org.uk/sites/default/files/documents/guidance_about_compliance_summary.pdf
[11] http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51
[12] http://www.legislation.gov.uk/ukpga/1972/70/contents
[13] In the 2015/6 contract this is service condition 23 - http://www.england.nhs.uk/nhs-standard-contract/
[14] http://www.legislation.gov.uk/ukpga/2000/36/contents

requires information to be held as proof of an activity against the eventuality of a claim. Examples of legislation include the Limitation Act 1980[16] or the Consumer Protection Act 1987[17].

For most professionals working in health and social care, there are relevant codes of practice issued by the registration bodies and membership organisations of staff. That guidance is designed to guard against professional misconduct and to provide high quality care in line with professional bodies.

This Code concentrates on the management of records through their lifecycle, i.e. from creation to eventual archiving or destruction. This Code must be read in conjunction with the materials published by the Professional Records Standards Body (PRSB) for Health and Social Care standards[18].

Monitoring Records Management Performance

Organisations may be asked for evidence to demonstrate they operate a satisfactory records management regime and there are a range of sanctions where records management is found to not meet the required standard. Sanctions previously made range from formal warnings, dismissal and professional deregistration, CQC intervention and fines.[19] A prison sentence (Criminal Justice and Immigration Act 2008 s77) is a possibility but to date this has not been used. Staff that are professionally registered may be asked to provide evidence of their professional work to support continued registration – such as social workers with the Health & Care Professions Council[20].

Legal and Professional Obligations

The principal legislation governing the management of records is Section 46 of the FOIA. This directs organisations covered by the Act to have records management systems which will help them to perform their statutory function.

The DPA is the principal legislation governing how care records are managed. It sets in law how personal and sensitive personal information may be processed. Records managers are expected to adhere to a code of practice[21] issued under Section 51(4).

The DPA principles are:

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection.

---

[15] http://www.legislation.gov.uk/ukpga/1998/29/contents
[16] http://www.legislation.gov.uk/ukpga/1980/58/contents
[17] http://www.legislation.gov.uk/ukpga/1987/43
[18] http://theprsb.org/standards
[19] ICO Enforcement webpage https://ico.org.uk/action-weve-taken/enforcement/
[20] Health and Care Professions Council - http://www.hcpc-uk.org/
[21] http://www.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf

The FOIA was designed to create transparency in Government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of those organisations to supply information through good records management programmes. Records managers are recommended to adhere to a code of practice[22] issued under Section 46 of the FOIA.

The Caldicott principles[23] outline seven areas that all health and social care staff are expected to adhere to in addition to the DPA. These principles are:

1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality.

To maintain the confidence of the individual in the records held about them, the NHS[24] and Social Care[25] 'Care Record Guarantees' outline twelve guarantees that record keeping must adhere to. The records must be held so that only authorised persons can access the record and so that it will be possible to tell the individual about who has accessed their record.

Professional Standards for record keeping

For staff working in health and social care there are a number of record keeping codes that people associated with certain professional bodies must adhere to as part of their profession.

The Academy of Medical Royal Colleges (AoMRC) generic medical record keeping standards (hosted by the Royal College of Physicians) were prepared for use in the NHS in a primarily acute setting, but the standard is useful to be considered in all settings. The AoMRC note that a medical record, whether paper or electronic, must adhere to the standards[26] in Table 1.

[22] https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf
[23] http://systems.hscic.gov.uk/infogov/caldicott/caldresources
[24] http://systems.hscic.gov.uk/rasmartcards/strategy/nhscrg
[25] http://webarchive.nationalarchives.gov.uk/20130513181011/http://www.nigb.nhs.uk/pubs/screngland
[26] For more information please see https://www.rcplondon.ac.uk/projects/outputs/generic-medical-record-keeping-standards

Table 1 - AoMRC medical record keeping standards

Standard Number	Description
1	The patient's complete medical record should be available at all times during their stay in hospital
2	Every page in the medical record should include the patient's name, identification number (must include NHS number, may include local ID) and location in the hospital
3	The contents of the medical record should have a standardised structure and layout
4	Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order
5	Data recorded or communicated on admission, handover and discharge should be recorded using a standardised proforma
6	Every entry in the medical record should be dated, timed (24 hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned, dated and timed[27]
7	Entries to the medical record should be made as soon as possible after the event to be documented (for example change in clinical state, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded
8	Every entry in a medical record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made
9	On each occasion a transfer of care occurs, the consultant responsible for the patient's care will change the name of the responsible consultant and the date and time of the agreed transfer of care
10	An entry should be made in the medical record whenever a patient is seen by a doctor. When there is no entry in the hospital record for more than four (4) days for acute medical care or seven (7) days for long-stay continuing care, the next entry should explain why
11	The discharge record/discharge summary should be commenced at the time a patient is admitted to hospital
12	Advanced Decisions to Refuse Treatment, Consent, and Cardiopulmonary Resuscitation decisions must be clearly recorded in the medical record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney

Further information about professional standards for records can be obtained from your relevant professional body. The main standard setting bodies in health and social care in England are noted at Appendix Two.

[27] For paper records a single line through the words must be used so the content remains visible. For electronic records deletions from the medical record must be reversible to prevent fraud.

Social Care and Public Health Records

The DH is the government department with responsibility for oversight of NHS and adult social care delivery. The Department for Education remains responsible for the oversight of children's social care.

This Code is designed to support the integration of health and adult social care provision. The Code applies to areas of health and social care integration, such as jointly held care records, in addition to other health care records which may be held by local authorities, such as public health records and contraceptive and sexual health services records. These services are now commissioned by public health departments in local authorities, but are essentially health care records.

Management and Organisational Responsibility

The records management function should be recognised as a specific corporate responsibility within every organisation. It should provide a managerial focus for records of all types in all formats, including electronic records, throughout their lifecycle from creation through to ultimate disposal. The records management function should have clear responsibilities and objectives, and be adequately resourced to achieve them.

A designated member of staff of appropriate seniority (i.e. Care Home Manager or Practice Manager or in larger organisations board level/reporting directly to a board member) should have lead responsibility for records management within the organisation. This lead role should be formally acknowledged and communicated throughout the organisation.

It is essential that the manager(s) responsible for the records management function are directly accountable to, or work in close association with, the manager(s) responsible for freedom of information, data protection and other information governance work areas.

As records activity is undertaken throughout the organisation, mechanisms must be in place to enable the designated corporate lead to exercise an appropriate level of management of this activity, even where there is no direct reporting line. This might include cross-departmental records and information working groups or individual information and records champions, who may also be information asset owners[28]. It is good practice to use the information asset register to help with managing information.

All staff, whether clinical or administrative, must be appropriately trained so that they are fully aware of their personal responsibilities in respect of record keeping and records management and that they are competent to carry out their designated duties. No patient or client records or systems should be handled or used until training has been completed.

Training should include the use of electronic records systems and it should be done through generic and/or organisation-wide training programmes which can be department or context specific. These should be complemented by organisational policies and procedures and guidance documentation. An example is health records managers who have lead responsibility for patient case notes and who manage the 'records library' and other storage areas where records are kept. Health records managers must have an up-to-date knowledge of, or access to, expert advice on the laws and guidelines concerning

[28] Government SIRO Manual https://www.gov.uk/service-manual/making-software/information-security.html#information-asset-owner or see HSCIC Information risk Management http://systems.hscic.gov.uk/infogov/security/risk

confidentiality, data protection (including subject access requests), and freedom of information requests.

Individual Responsibility

Under the Public Records Act 1958 employees are responsible for any records that they create or use in the course of their duties. Therefore, any records created or received by an employee of the NHS are public records and may be subject to both legal and professional obligations. For those records created in a local authority setting, such as adult social care and public health, section 224 of the Local Government Act 1972 applies[29] as 'without prejudice to the powers of the custos rotulorum to give directions as to the documents of any county, a principal council shall make proper arrangements with respect to any documents that belong to or are in the custody of the council or any of their officers'.

Policy and Strategy

Each organisation should have an overall policy statement on how it manages all of its records, including electronic records. The statement should be endorsed by the management team, board (or equivalent) and made available to all staff at induction and through regular updates and training.

The policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an organisation's commitment to create, keep and manage records and document its principal activities in this respect. The policy should also:

- Outline the role of records management within the organisation and its relationship to the organisation's overall strategy
- Define roles and responsibilities within the organisation, including the responsibility of individuals to document their actions and decisions in the organisation's records and to dispose of records appropriately when they are no longer required
- Provide a framework for supporting standards, procedures and guidelines and regulatory requirements (such as CQC and the HSCIC hosted DH Information Governance Toolkit)
- Indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored and maintained
- Provide the mandate for final disposition of all information by naming the committee or group that oversees the processes and procedures
- Provide instruction on meeting the records management requirements of the FOIA, the DPA and the Environmental Information Regulations 2004.

The policy statement should be reviewed at regular intervals (at least once every two years) and if appropriate should be amended to maintain its relevance. The policy is also an important component of the organisation's information governance arrangements and should be referenced in the organisation's Information Governance Management Framework. The Information Governance Toolkit gives the basic content of a records management policy.

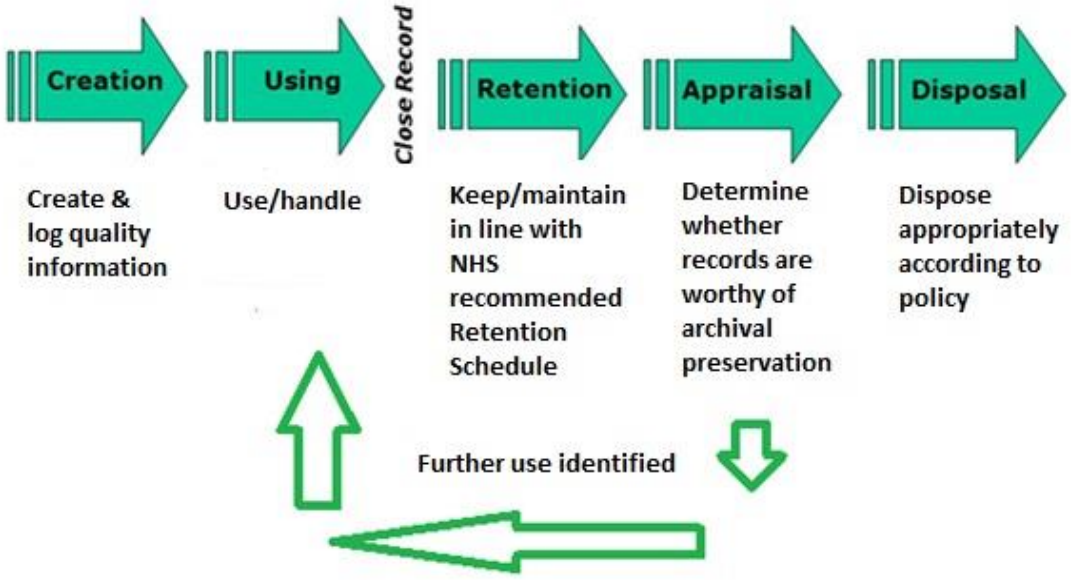
[29] National Archives snapshot of the content of the Communities and Local Government website - Guidance on the 'proper arrangements' for archivists taken for preservation 5/3/2000 http://webarchive.nationalarchives.gov.uk/+/http:/www.communities.gov.uk/localgovernment/360902/constitutionsandethics/constitutionalarrangements/guidanceproper

Section 2: How to manage records

The Records / Information Lifecycle

The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest. This can be seen diagrammatically in Figure 1.

Figure 1 – The Records/Information Lifecycle



Characteristics of authoritative records

ISO 15489-1:2016 Information and documentation - Records management,[30] published by the International Organization for Standardization (ISO), focuses on the business principles behind records management and how organisations can establish a framework to enable a comprehensive records management programme.

The standard also describes the characteristics of a record (see Table 1) and these characteristics allow strategies, policies and procedures to be established that will enable records to be authentic, reliable, integral and usable throughout their lifecycle.

In order to ensure that these characteristics are maintained, sufficient persistent metadata must be attached to each record. It is essential that a record keeping regime is designed that will allow records to possess these characteristics.

[30] ISO15489-1:2016: http://www.iso.org/iso/catalogue_detail?csnumber=62542

Table 2 - Characteristics of authoritative records

Derived from Section 5.2 - ISO15489-1:2016

Record characteristic	How to evidence
Authentic	• It is what it purports (claims) to be • To have been created or sent by the person purported to have created or sent it and • To have been created or sent at the time purported.
Reliable	• Full and accurate record of the transaction/activity or fact • Created close to the time of transaction/activity • Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity.
Integrity	• Complete and unaltered • Protected against unauthorised alteration • Alterations after creation can be identified as can the persons making the changes.
Useable	• Located, retrieved, presented and interpreted • The context can be established through links to other records in the transaction/activity.

Designing Record Keeping Systems

Design and Implementation of Record Keeping Systems (DIRKS)

The industry standard for the design and implementation of record keeping systems, as given in the ISO standard ISO15489-1:2001[31], is an eight stage process that can be summarised as:

1. Conduct preliminary investigation
2. Analyse business activity
3. Identify requirements for records
4. Assess existing systems
5. Identify strategies to satisfy requirement
6. Design records system
7. Implement records systems
8. Conduct post implementation review.

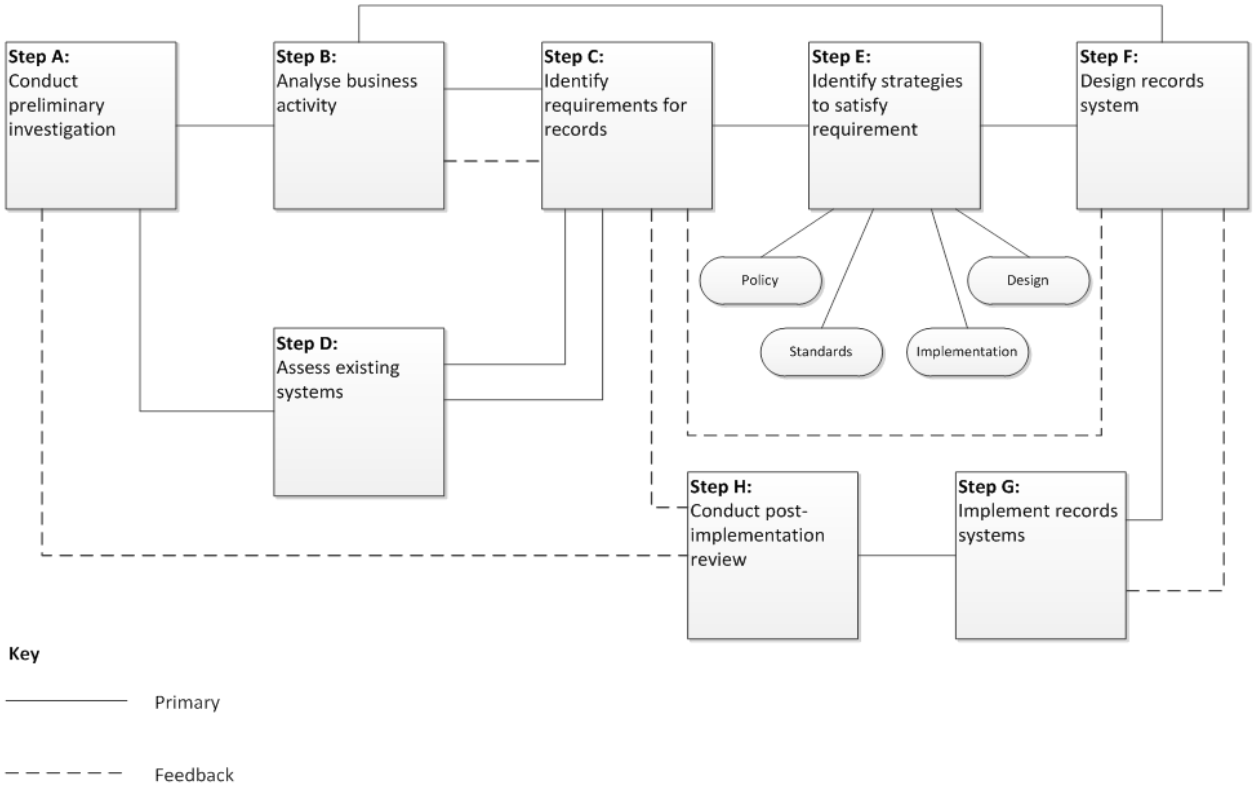
Figure 2 indicates the relationship of the stages. Further details can be sought from the ISO standard and supplementary guidance. In addition to the stages outlined above, a privacy impact assessment must also be conducted where necessary. For more advice and information please see the Information Commissioner's Office (ICO) Privacy Impact Assessment Code of Practice[32].

[31] This has been revised in ISO15489-1:2016 and will be evaluated and the Code updated where necessary at the next revision. Early indications are that changes are presentational as opposed to material.

[32] ICO Privacy Impact Assessment Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

There are a series of other British and international standards that are used to produce record keeping systems. For details of the standard making bodies, please see Appendix Two. These all interrelate and work within the same guiding principles and where possible use the same terminology. They all rely upon defining roles and responsibilities, processes, measurement, evaluation, review and improvement.

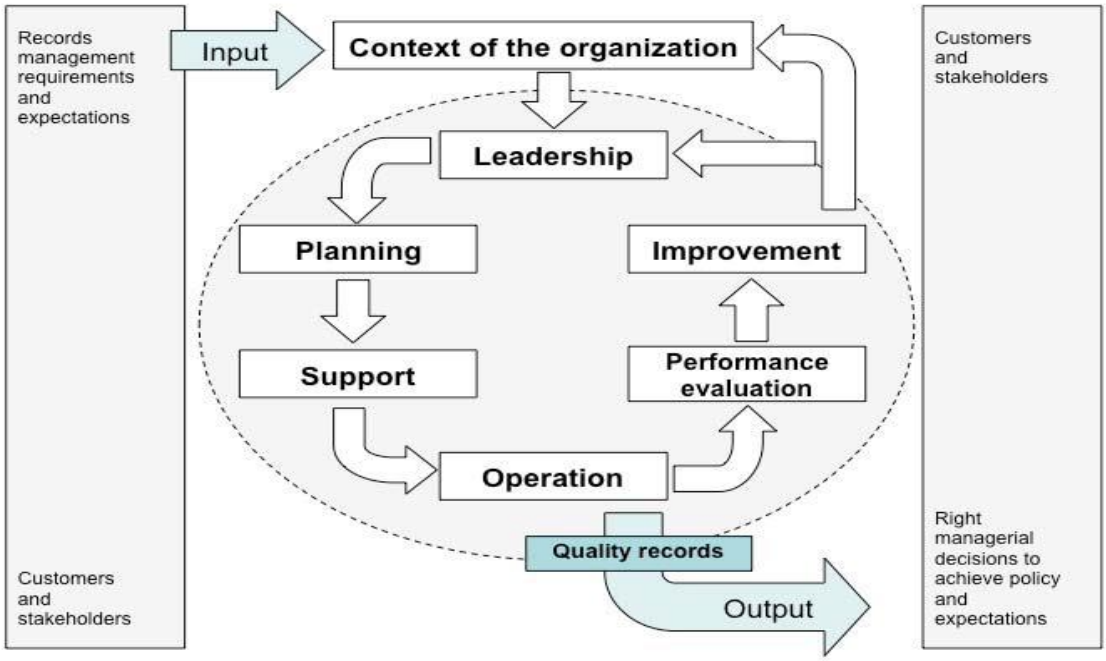
Figure 2 – The DIRKS Process



The diagram in Figure 3 shows the basic processes required to implement a records management system if the DIRKS process is not used. This is taken from ISO30300:2011[33].

[33] ISO30300-211: Information and documentation - Management systems for records - Fundamentals and vocabulary http://www.iso.org/iso/catalogue_detail.htm?csnumber=53732

Figure 3 - Information and documentation – management systems for records



Records and Metadata

Record keeping systems must have a means of physically arranging or organising records. This is often referred to as a file plan or by the technical name of a business classification scheme. The scheme can be designed along several lines:

- Function (recommended)
- Hierarchy/organisation
- Hybrid function/hierarchy
- Subject/thematic

The scheme will enable appropriate management controls to be applied and support more accurate retrieval of information from record systems. When the recommended functional classification has been selected, the scheme can be further refined to produce a classification tree based on function, activity and transaction.

Function-Activity-Transaction

Classification schemes should try and follow the rule of classifying by function then by the activity and finally the transactions that relate to the activity. The transaction can then be assigned a rule (such as retention period) a security status or other action based on the organisational policy.

At the simplest level, the business classification scheme can be anything from an arrangement of files and folders on a network to an Electronic Document and 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.

Declaring a Record

Within the record keeping system, there must be a method of deciding 'what is a record?' and therefore 'what needs to be kept?' This process is described as 'declaring a record'. A declared record is then managed in a way that will hold it in an accessible format until it is appraised for further value or it is destroyed, according to retention policy that has been adopted.

Some activity will be predefined as a record that needs to be kept, such as clinical records. Other records will need to fulfil criteria as being worth keeping, such as unique instances of a business document or email. Key legislation, such as the DPA or FOIA, applies to all recorded information of the types covered by these Acts, whether declared as a formal record or not.

Declaration makes it easier to manage information in accordance with the legislation and business need. Accumulations of informal recorded information should be minimised as they will rarely meet these requirements.

A record can be declared at the point it is created or it can be declared at a later date, but the process of declaring a record must be clear to staff.

Declared records can be held in the 'business as usual' systems or they can be moved into a protected area, such as an EDRMS, dependant on the record keeping system in use.

It is harder to manage records over their lifecycle if they clutter up the folders or the workspace used on a daily basis or they are held in personal systems where only one person can access them. Just as a paper file was once closed when full or it ran over into the following year's business cycle, electronic information must also be closed off and filed in a place that does not clutter up the current business.

This declared information can be moved into the appropriate part of the business classification scheme, if it does not already reside there, following creation. The individual staff and teams have the flexibility to apply the organisational policy to keep the records for the appropriate length of time in their business context. This system, while flexible, runs the risk of staff and teams not applying the policy correctly and records may be missed.

Metadata Standard

The Cabinet Office e-Government Metadata Standard v3.1 2006 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'[34]. There are 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 have to be present for any piece of information. A further three elements are mandatory if applicable and two more are recommended. These can be found in Table 3.

[34] Cabinet Office e-Government Metadata Standard v 3.1
http://www.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf

Table 3 - Metadata elements

Mandatory elements	Mandatory if applicable	Recommended
Creator	Accessibility	Coverage
Date	Identifier	Language
Subject	Publisher	
Title		

An example in practice of a box label on the side of a box of records would be created as shown in Table 4.

Table 4 – An example of the use of the metadata standard

Box label	Local interpretation	Metadata standard
Tiverton Community NHS Trust	Organisation Name	Creator
Midwifery	Service Name	Creator
Patient case records surname A-F	Description of record	Subject/Title
2000	Date/year of discharge	Date
2025	Date/year of destruction	Date

In addition to any metadata needed to manage information through the lifecycle, all information possesses a security classification.

Both central government and local government use the Cabinet Office Government Security Classifications April 2014 defined protective marking scheme[35]. This policy describes how HM Government classifies information assets to: ensure they are appropriately protected; support public sector business and the effective exploitation of information. The policy also describes how government can meet the requirements of relevant legislation and international/bilateral agreements and obligations. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.

The NHS use a variation of this scheme[36] based on patient data being classed as 'NHS Confidential' having the equivalence of Official Sensitive under the 2014 scheme[37].

Where a record has enough metadata it can be managed through the lifecycle, possess a security classification and be easily found if needed.

More information about metadata elements and the Cabinet Office e-Government Metadata Standard 2006, including a full description of the 25 elements, can be found on the TNA website[38].

[35] 2014 Protective Marking Scheme https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
[36] NHS Protective Marking Scheme https://www.igt.hscic.gov.uk/KnowledgeBaseNew/DH_NHS%20IG%20-%20Info%20Classifications.pdf
[37] NHS Number guidance from IGA describing how to integrate the NHS and Government protective marking schemeshttp://systems.hscic.gov.uk/infogov/iga/resources/nhsnumberfaq.pdf

Metadata only Classification

If a record has sufficient metadata, the arrangement between itself and other records in the same class can be established without the application of a business classification scheme. At present, ISO 15489 and the 'Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000[39]' calls for records to be arranged into a classification scheme.

Records that are not stored or arranged in logical filing systems often lack their characteristic of 'context' which will reduce the ability to produce an authentic record. They are often reliant on a powerful search tool used to 'mine' the data or use a process called 'digital archaeology'. This records management method is not recommended because it is so time-consuming to determine authenticity but it has been included in this Code as legacy record keeping systems may not have been organised logically.

As record keeping systems are updated and the more traditional files and folders and bespoke storage for electronic records are decommissioned, the ability to recover records is only as good as the metadata applied to records when they were created.

Business Classification Scheme Design

The technical name for the process to create business classification system is 'functional decomposition'. In the most basic form this is a list of activities arranged by business functions; however it is often linked to organisations hierarchical structure. An example is given in Table 5.

Table 5 - Business Classification Scheme Design

Functional classification example	Hierarchical classification example
Finance-Accounts-Payments-HR Payments (Note All payments including HR team are recorded under the activity of accounts)	Finance team-Accounts Team- Payments HR Team – Finance- Payments (Note The payment is recorded twice)

Good Practice for business classification scheme design:

The NHS Business Services Authority has devised a business classification scheme that allows it to manage records so they can be easily found and managed through the lifecycle. Each record can be assigned a retention once it is declared into the system.
http://www.nhsbsa.nhs.uk/Documents/NHSBSACorporatePoliciesandProcedures/NHSBSARM014_Business_Classification_v1.0_2011.pdf

[38] Government Metadata Standard http://www.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf
[39] Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000: https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf

Storage

Paper: to establish the authenticity of paper records and to meet the Care Records Guarantee that the service user can see who has accessed their records, the records must be held according to the standard that allows access to be audited.

The current guidance to identify and support the requirements for offsite storage of physical records is issued by TNA[40]. The standard issued by TNA (Tracking Records – RMS 2.1[41]) is a best practice benchmark for all organisations creating or holding public records. The standard provides advice and guidance on the tracking of records at all stages of the information life cycle up to destruction, or transfer to TNA or an approved place of deposit.

Digital: digital information must be stored in such a way that throughout the lifecycle it can be recovered in an accessible format in addition to providing information about those who have accessed the record, as required by the Care Records Guarantees. When considering standards, the European Commission DLM Forum Foundation[42] 'Modular Requirements for Record Systems'[43] is frequently used as the overarching standard.

The authenticity of a record is dependent on a number of factors not least that it has sufficient metadata to allow it to remain reliable, integral and usable. This will include the structure of the record, the business context and links between other documents that form part of the transaction the record relates to.

It should not be underestimated how technically difficult and time consuming this process can be to maintain digital records over time. 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 cannot be said to be 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.

Offsite: It is vital to highlight the importance of actively managing records which are stored in offsite storage. This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and privacy impact assessments are conducted on the offsite storage providers.

Appraisal

The process of deciding what to do with records when their business use has ceased is called appraisal. This must be defined in a policy and any decisions must be auditable and linked to a mandate to act, derived from the Board. No record or series can be automatically destroyed or deleted. It is good practice to get authorisation for deletion or

[40] The National Archives: Identifying and specifying requirements for offsite storage of physical records: January 2009 http://www.nationalarchives.gov.uk/documents/information-management/considerations-for-developing-an-offsite-store.pdf and TNA Records Tracking http://www.nationalarchives.gov.uk/documents/information-management/tracking-records.pdf
[41] Guidance on digital continuity is given by TNA Managing digital continuity http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/
[42] DLM Forum Foundation: http://dlmforum.eu/
[43] MoReq2010® Modular requirements for records systems: http://moreq.info/

destruction from an appointed committee or group with a designated function to appraise working to a policy or guidelines. There is some guidance from TNA on appraisal[44].

There will be one of three outcomes from appraisal:

- Destroy / delete
- To keep for a longer period
- To transfer to a place of deposit appointed under the Public Records Act 1958.

The retention schedule included in this Code lists those records which should or may be selected for transfer to a place of deposit. There are also a number of other records which may be of interest to a local place of deposit. Appraisal may also result in a record being retained for longer.

If as a result of appraisal, a decision is made to destroy a record there must be evidence of the decision.

Records selected as a result of an appraisal may also have security classifications applied which may continue to exempt them from Freedom of Information (FOI) requests or disclosure after transfer to a place of deposit. This may be part of the annual cycle of the records committee or other appropriate person where a record will be retained in an official document such as committee papers. Records transferred to a place of deposit, such as unpublished board papers, may continue to be subject to FOIA exemptions on public access following transfer.

Electronic records can be appraised if they are arranged in an organised filing system which can differentiate the year the records were created and the subject of the record. 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.

Good Practice for Selection and Appraisal:

The Tavistock and Portman NHS Foundation Trust have a policy for the selection of material for permanent archive and a method of selecting the works of eminent clinician's work and a panel for selecting historical records. Where a clinician has amassed a lifetime of research or important cases these may be identified and retained.

Destruction

Paper: paper records can be destroyed to an international standard. They can be incinerated, pulped or shredded (using a cross cut shredder) under confidential conditions. Do not use the domestic waste or put them on a rubbish tip, because they remain

[44] The National Archives – appraising your records: http://www.nationalarchives.gov.uk/information-management/manage-information/selection-and-transfer/appraising-records/

accessible to anyone who finds them. The relevant standard for destruction in all formats is BSIA EN15713:2009 – Secure Destruction of Confidential Material[45].

As referenced in the retention schedule, it is important to keep accurate records of destruction and appraisal decisions. Destruction implies a permanent action. For electronic records 'deletion' may be reversed and may not meet the standard as the information can/may be able to be recovered or reversed.

Digital media: destruction of digital information is more challenging. Records management is concerned with accounting for information so any destruction of hard assets, like computers and hard drives and backup tapes, 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 has indicated 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 DPA[46]. Their advice is to only procure systems that will allow permanent deletion of records to allow compliance with the law.

Please contact the HSCIC for procurement advice and example documentation for procurement of information systems that support the requirements for care record systems.

Requests made to organisations under the FOI Act have indicated that once the appropriate limit for costs incurred for that FOI has been reached, there are no more requirements to recover information held[47]. This will **not** apply if a court has instructed information to be destroyed where permanent destruction will be required, including all copies and instances of the information.

Good Practice for a destruction process:

Barts Health NHS Trust have a process where before any records are disposed of they are referred back to the creators for a final approval of the decision to either destroy, keep for longer or to transfer to a place of deposit. This means that decision to destroy records does not sit with one person and it gives an opportunity for any legal holds to be applied.

A service level agreement has also been created to include the process for disposing of records where the creators are no longer available to make a decision. A listing of the records is provided to the Trust's Information Governance Committee which has the authority to dispose of the records or to retain them for a further period.

[45] BSIA EN15713:2009 - http://www.bsia.co.uk/Portals/4/Publications/form_204_id_en15713.pdf
[46] ICO Deleting personal data https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf
[47] ICO Determining whether information is held https://ico.org.uk/media/for-organisations/documents/1169/determining_whether_information_is_held_foi_eir.pdf

At present there are two ways of permanently destroying digital information and these are either: overwriting the media a sufficient number of times or the physical destruction of the media[48].

No information can be destroyed if it is the subject of a request under the DPA and/or FOIA or any other legal process, such as an inquest following a death.

Review for Continued Retention

The periods given in the schedules to this Code are the **minimum** periods for which records must be retained for NHS business and clinical purposes. In most cases, it will be appropriate to destroy records immediately once this period has expired, unless they have been selected for transfer under the Public Records Act 1958. If personal data is held for longer than necessary it may breach principle five of the DPA[49].

Organisations must have procedures and policies for any instances where it is necessary to maintain records for longer than the stated minimum, including temporary retention where records due for destruction are required to support reasonably foreseeable litigation, public inquiries, an on-going FOI request or similar exceptional statutory reasons, such as a public inquiry.

Organisations may also set local policies, for example for retention of clinical records in relation to specific circumstances beyond those identified in this Code.

Where records contain personal data, the decision to retain must comply with the DPA 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.

Records **may** be retained beyond the statutory period (20 years from the last date at which content was added) set by the Public Records Act 1958 **only** with the approval of the Secretary of State for Culture, Media and Sport. Applications for approval should be made to TNA in the first instance.

Retention Instrument 122 [50]has been approved by the Secretary of State for Culture, Media and Sport to permit extended retention of NHS individual staff and patient records where this is mandated by this Code or is otherwise necessary for continued NHS operational use. Where organisations use the provisions of the Instrument to extend retention, this must be documented in published policies. TNA website has details of those currently in force[51].

Transfer to a Place of Deposit

The Public Records Act 1958 requires organisations to select core records for permanent preservation at the relevant Place of Deposit[52] (PoD) appointed by the Secretary of State

[48] HSCIC Destruction and Disposal of Sensitive Data: http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/dadosd.pdf
[49] ICO Guide to data protection: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/
[50] http://www.nationalarchives.gov.uk/documents/information-management/access-to-public-records.pdf
[51] http://www.nationalarchives.gov.uk/archives-sector/nhs-information-governance-toolkit.htm
[52] http://www.nationalarchives.gov.uk/information-management/manage-information/places-of-deposit/

for Culture, Media and Sport. PoDs are usually public archive services provided by the relevant local authority.

The selection and transfer must take place at or before records are 20 years old and is a separate process from appraisal for retention to support current service provision. Potential transfers of digital records should be discussed with the PoD in advance to ensure that technical issues can be resolved.

Records no longer required for current service provision may be temporarily retained pending transfer to a PoD and records containing sensitive personal data should not normally be transferred early.

Transferred records should be in good condition and appropriately packed, listed and reviewed for any FOIA exemptions. For more detail on the transfer process and sensitivity review, see the TNA guidance on their website[53].

More detailed guidance on the selection for records for transfer under the Public Records Act 1958 is contained in the schedules to this Code. The relevant PoD will provide additional local guidance on how the schedules should be implemented. Current contact details of PoDs and the organisations which should transfer to them can be found on the TNA website[54]. As a general rule national public sector organisations will deposit with TNA while local organisations will deposit with a local PoD.

Audit of Records/Information Asset Management

Organisations must, once a year, complete a survey or audit of their records to ensure that they understand the extent of their records management responsibilities. This will not mean that every single record has to be recorded in a central index but it will involve knowing what series of records are held by which business areas and that there are named information asset owners managing all records appropriately.

It may be possible to link this process to information asset management. To do this, it must identify where the records are being held and that they are being held under the correct security conditions and in the case of clinical records, remain confidential. The process can be used as an opportunity for asset owners to identify how long their records need to be held. The process will also identify business critical assets and ensure that there are adequate business continuity measures in place to assure access.

Digital Records, Digital Continuity, Digital Preservation and Forensic Readiness

Digital information presents a unique set of issues which must be considered and overcome to ensure that records remain authentic and reliable, retaining their integrity and 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. 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

---

53 http://www.nationalarchives.gov.uk/documents/A_brief_guide_to_transferring_Records_of_Local_Interest.pdf and http://www.nationalarchives.gov.uk/documents/information-management/access-to-nhs-records-transferred-to-places-of-deposit.pdf

54 http://www.nationalarchives.gov.uk/archives-sector/approved-places-of-deposit.htm

record system may need to be accessible in 100 years (including an audit trail to show lawful access and maintain authenticity) to support continuity of care. As there are no digital records in existence today that are of such an age, it is difficult to even plan continued access in an authentic form over such a timeframe. For example:

- Just as paper records can deteriorate so can electronic media as the magnetic binary code can demagnetise in a process called 'bit rot' leading to unreadable or altered information
- Software upgrades can leave other applications unusable as they may no longer run on updated operating systems
- Media used for storage may become obsolete and the technology required to read them may not be commercially available
- File formats become obsolete over time as more efficient ones are developed.

To leave digital information unmanaged in the hope a file can be used in the future is not recommended. TNA has produced a variety of technical and role based guidance and useful checklists to support this management process[55].

Good practice for digital preservation:

The HSCIC have migrated decommissioned and orphaned clinical systems from their host Trusts onto a separate platform so they can be retained for the necessary period of retention, to enable subsequent access for clinical purposes.

Many of the Trusts have also placed the data onto their replacement systems and data warehouses. This active process of digital curation means that the records which may have been lost are available for future care.

To preserve a digital record over even a short period of time can be challenging but can be made easier through the application of techniques of digital preservation.

There are several strategies that can be adopted to ensure that digital information can be kept in an accessible form over time. Among the most common strategies adopted are:

- Emulation (using software to simulate the original application)
- Preservation of host system
- Conversion to a standard file format (or a limited number of formats)
- Migration to new system (retaining existing formats).

The Digital Preservation Coalition[56] has produced a handbook that will help organisations understand some of the issues associated with retaining digital records for long periods of time.

The UK Government CESG[57] provides good practice guidelines on Forensic Readiness[58] and defines it as 'the achievement of an appropriate level of capability by an organisation in

[55] http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/digital-continuity/
[56] Digital Preservation Coalition Handbook: http://www.dpconline.org/publications/digital-preservation-handbook
[57] https://www.cesg.gov.uk/

order for it to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be effectively used in any legal matters, in security investigations, in disciplinary matters, in an employment tribunal or in a court of law'.

The CESG notes that 'it is important for each organisation to develop a forensic readiness of sufficient capability and that it is matched to its business need'.

Forensic readiness involves specification of a policy that lays down a consistent approach, detailed planning against typical (and actual) case scenarios that an organisation faces, identification of (internal or external) resources that can be deployed as part of those plans, identification of where and how the associated digital evidence can be gathered that will support case investigation and a process of continuous improvement that learns from experience.

In many organisations forensic readiness is managed by information security or informatics staff but records managers need to ensure that they input to policy development and feed in case scenarios as necessary.

58 https://www.cesg.gov.uk/content/files/guidance_files/Forensic%20Readiness%20(Good%20Practice%20Guide%2018)_1.2.pdf

Section 3: How to deal with specific types of records

We have written this section to deal with a number of issues raised by health and social care records managers to TNA, the HSCIC and the DH between 2009 and the end of 2015 since the previous Code was issued in 2006.

These issues relate to the following health and social care records:

- General Practitioner Records
- Records at Contract Change
- Prison Health Records
- Youth Offending Service Records
- Secure Units for patients detained under the Mental Health Act 1983
- Family Records
- Child School Health Records
- Integrated Records
- Integrated Viewing Technology and Record Keeping
- Complaints Records
- Specimens and Samples
- Continuing Care Decisions Records
- Records of Funding
- Ambulance Service Records
- Adopted Persons Health Records
- Health Records of Transgender Persons
- Witness Protection Health Records
- Controlled Drugs Regime
- Asylum Seeker Records
- Occupational Health Records
- Public Health Records
- Records of non-NHS funded patients treated on NHS premises
- Patient/Client Held Records
- Records dealt with under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000
- Staff Records
- Email and Record Keeping Implications
- Records Created via Social Media
- Records Created Through Bring Your Own Device (BYOD)
- Cloud Based Records
- Website as a Business Record
- Scanned Records
- Duplicate Records
- Edisclosure/Ediscovery and Records Implications

Care Records

General Practitioner Records

It is important to note that the General Practitioner (GP) record, usually held at the General Practice, is the primary record of care and that 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.

Following the move to digital GP records after the 'paperlite' accreditation process there was an instruction not to destroy the paper Lloyd George folders. The guidance from 2011 advises not to destroy the paper contents[59] and the GP2GP programme still requires the Lloyd George paper records to be transferred until further notice[60]. GPs are obliged by their contract to follow the HSCIC, DH and NHS England good practice guidance.

Records at Contract Change

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.[61] This will usually be to ensure the continuity of service provision 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.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also be a consideration to identify the legal entity which must manage the records.

Where the content of records is confidential, for example care records, it may 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 may require individual communications or obtaining explicit consent. Although the conditions of the DPA may be satisfied in many cases there is still a duty of confidence which requires a patient or client (in some cases) to agree to the transfer.

It is vital to highlight the importance of actively managing records which are stored in offsite storage. This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and

[59] Department of Health, BMA & RCGP - The Good Practice Guidelines for GP electronic patient records Version 4 (2011) page 179.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215680/dh_125350.pdf
[60] HSCIC GP2GP release notes http://systems.hscic.gov.uk/gp2gp/gp2gprelease
[61] Most organisations subject to this Code will have a standard NHS contract which can be accessed through the link http://www.england.nhs.uk/nhs-standard-contract/

privacy impact assessments are conducted on the offsite storage providers. Table 6 summarises some possible scenarios and, for each option, patient consent and an information sharing agreement or a contract may be required to share the information.

Good Practice at Organisation Closure:

In 2012, the Strategic Health Authority and the 30 Primary Care Trusts of London ran a transition programme with a Records Management stream to prepare both paper and electronic records for organisation closure. All records were reviewed by the teams that owned the assets. Some were passed to successor organisations to support business as usual. Others that were passed their retention period were reviewed and destroyed appropriately.

A proportion of GP records where there was no clear successor organisations were passed to the Department of Health (DH). The DH reviewed the records and they were put into long term secure storage.

Table 6 - Records at Contract Change Scenarios

Characteristic of new service provider	Fair processing required [62]	What to transfer?	Sensitive records
NHS provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light- notice on appointment letter explaining that there is a new provider. Local publicity campaign such as signage or posters located on premises.	Entire record or summary of entire caseload.	N/A
Non NHS provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	N/A
NHS provider from different premises but with the same staff.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record.	N/A
NHS provider from different premises and different staff.	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	Individual communications may not be possible so consent of current caseload may need to be sought before transfer. It may not be possible to transfer the record without explicit patient consent so in some cases no records will be transferred.
Non NHS provider from different premises but with same staff	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	

[62] Service users must be informed about processing to meet DPA fair processing requirements and to avoid breaching confidentiality – see the ICO Data Sharing Code of Practice https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

Characteristic of new service provider	Fair processing required [62]	What to transfer?	Sensitive records
Non NHS from different premises and with different staff.	High – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider.	

Good Practice for records at provider/contract change:

The Rotherham Doncaster and South Humber NHS Foundation Trust (RDASH) policy is that when transferring patient data to a new provider/contract change, the original records must always stay with RDASH.

RDASH only give the new provider current patient information and, of those, only the relevant information is given. The new provider can contact RDASH for a continuation of care request should they need any non-current patients' information.

Prison Health Records

When the responsibility for offender health in HM Prison Service transferred from the Ministry of Justice to NHS England, a national computer based record was created to facilitate the provision of care and the transfer of care records associated with inmate transfers throughout imprisonment. However, a significant number of paper records remain and some offender health services operate hybrid paper/electronic heath records.

Prison records should be treated as hospital episodes and may be destroyed after the appropriate retention has been applied. The assumption is that a discharge note has been sent to the GP. Where a patient is sent to prison the GP record must not be destroyed but rather held until release or normal retention periods of GP records have been met.

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. However for purposes of clinical liability and for continuity of care, the health 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.

Secure Units for Patients Detained Under the Mental Health Act 1983

Some institutions that deal with offenders are categorised as hospitals because the inmate is considered a patient. Such patient records are classed as mental health records and

must be retained for longer periods of time. This is normally in excess of 30 years for purposes of the continuity of care - or another lawful basis for the continued retention is required.

Family Records

Family records are common within health visiting and in some therapy services where a holistic picture of the family is needed to deliver care. This creates a particular problem when the NHS and social care record keeping systems deal with the individual. It may be necessary to specify one person as the focus of the record and hold the entire record against that individual and link the other family members' records together. This will create an issue when the record is shared or disclosed in some way. Special care must be taken not to disclose information about a third party without a lawful basis to do so (for example consent).

Child School Health Records

It is good practice for each child to have an individual record. A file for the school or a yearly intake is not considered good practice as this means the record is not about the individual child. The focus of a care record must be the individual and not the legal entity. Furthermore when a child changes school or district a record or copy must also be transferred but only when the receiving authority has confirmed that the child is resident there. Failure to carry this out properly will mean a large number of misplaced records will reside with the wrong child health or school nursing service. Where a child's record is stored on a school premises, access must be restricted to the health staff delivering care unless there is another lawful basis to access the record.

Integrated Records

Integrated or joint care records create additional issues which must be resolved locally. This includes a means of attributing ownership and access to the records between all parties where there is a lawful basis to access the records.
These arrangements may include:

- Nominating one organisation to own the records
- Separating the records so that each party retains their own information
- Each party keeps their own record but has access to the shared part of the other record.

For each option, some form of patient consent is necessary to enable all parties to access information lawfully. An information sharing agreement is recommended as a mechanism for providing clarity and transparency on the standards that all participants must meet[63].

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. Where these are used, it may be necessary to recreate the instance of viewing to allow an audit trail of decision making. It may be necessary to make a note in the record that the information has been obtained by this means to attribute the source of evidence for any interventions taken.

Complaints Records

Where a patient or client complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Complaint information should

[63] Guidance on information sharing agreements is available from the IGA at iga@nhs.net

never be recorded in the clinical record. A complaint may be unfounded or involve third parties and the inclusion of that information in the clinical 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 and the health care team.

Where multiple teams are involved in the complaint handling, all the associated records must be amalgamated to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. It is common for the patient or client 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. The ICO has issued guidance on complaints files and who can have access to them, which will drive what must be stored in them[64].

Specimens and Samples

The retention of human material is not covered in this Code and is **not** in scope. The metadata or information about the sample or specimen **is** in scope. Relevant professional bodies such as the Human Tissue Authority[65] or the Royal College of Pathologists[66] have issued guidance on how long to keep human material.

Just because the human material is not kept for long periods, does not mean that the information 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 pathology reports may be retained by the individual pathology departments, a copy must always be included on the patient record.

Continuing Care Decisions Records

In order to process applications and appeals for funding continuing care, it is necessary for the relevant organisation to have access to clinical records. This will be based on consent and organisations need to have arrangements in place to facilitate sharing or put systems in place to allow access to view records or take copies. Any access must be lawful and the decision to grant access recorded.

Records of Funding

Funding records are primarily administrative records but they contain large amounts of care information and as such must be managed as clinical records for their access and management. This includes having rigorous processes for access and the appropriate lawful basis to share them.

Ambulance Service Records

Ambulance service records will contain evidence of clinical interventions and it is necessary to treat them as a clinical record. This means that they must be retained for the same time as clinical records. 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. Where the ambulance record is

[64] https://ico.org.uk/media/for-organisations/documents/1179/access_to_information_held_in_complaint_files.pdf
[65] https://www.hta.gov.uk/codes-practice
[66] https://www.rcpath.org/Resources/RCPath/Migrated%20Resources/Documents/G/G031_RetentionAndStorage_Apr15.pdf

handed over to another service or NHS Trust there must be a means by which the ambulance trust can obtain them again if necessary. Alternatively they can be copied and only the copy transferred.

Adopted Persons Health Records

Notwithstanding any other centrally issued guidance by the DH or Department for Education, the records of adopted persons can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.

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 was considered appropriate to do so, following the adoption.

Health Records of Transgender Persons

A patient 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 that can be made by the Gender Recognition Act 2004[67]. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. 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. It is important to discuss with the patient 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.

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 (such as 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 medical records. For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person.

Controlled Drugs Regime

NHS England in conjunction with the NHS Business Services Authority has established procedures for handling information relating to controlled drugs. This guidance includes conditions for storage, retention and destruction of information. Where information about controlled drugs is held please refer to NHS England guidance[68].

Asylum Seeker Records

Any service provided to any client must have a record. For reasons of clinical continuity or professional conduct, records for asylum seekers must be treated in exactly the same way as other care records. Where the asylum seeker is given a patient held record, the

[67] Gender Recognition Act 2004: http://www.legislation.gov.uk/ukpga/2004/7/contents
[68] http://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf

provider must satisfy themselves that they have a record of what they have done in case of litigation or matters of professional conduct.

Occupational Health Records

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. However, 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 any contractor can retain the records for the necessary period after the termination of service for purposes of adequately recording any work based health issues.

Public Health Records

The public health function is normally hosted by a local authority (as enacted by the Health and Social Care Act 2012) but the function still processes and usually involves the handling of clinical information. For this reason public health functions are considered in the scope of this Code.

Where clinical information is being processed by the public health function it is expected that the standards which will apply to the handling of confidential information will be those set by the HSCIC Code of Practice for Confidential Information[69].

Records of non-NHS funded patients treated on NHS premises

Where records of individuals who are not NHS or social care funded are held in the record keeping systems of NHS or social care organisations, they must be kept for the same minimum retention periods as other records outlined in this Code. The same levels of security and confidentiality will also apply.

Patient/Client Held Records

Where it is necessary to leave records with the individual who is the subject of care, it must be indicated on the records that they remain the property of the issuing organisation and include a return address if they are lost. Organisations must be able to produce a record of their work which includes services delivered in the home where the individual holds the record. Upon the termination of treatment where the records are the sole evidence of the course of treatment or care, they must be recovered and given back to the issuing organisation. An example of this would be the maternity file that is held by the mother until the first GP visit after the birth of the baby or until it is no longer required.

A copy can be provided if the individual wishes to retain a copy of the records. Where the individual retains the actual record after care, the organisation must be satisfied it has a record of the contents. An example is a child's red book where the parent retains the record but the contents are also recorded in the health visiting file.

Records dealt with under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000

The directions impose an additional obligation of confidentiality on employees and trustees of NHS Trusts, Clinical Commissioning Groups, local authority public health functions and those providing services under contract regarding information about sexually transmitted diseases.

[69] http://systems.hscic.gov.uk/infogov/codes/cop

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

Corporate Records

Staff Records

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters[70]. The nucleus of any staff file will be the paperwork collected through the recruitment process and this will include the job advert, application form, right to work, identity checks and any correspondence relating to acceptance of the contract. The central file must be the repository for this information.

It is common practice for the line manager to hold staff records which can contain large portions of an employee's employment history (for example training records). This practice runs the risk of much of the employment record being lost if there is an internal move of the employee or upon termination of contact. It is important that there is a single record of the employment of an employee.

Good Practice for staff training records:

It can be difficult to categorise staff training records to determine retention requirements but keeping all for the same length of time is also hard to justify. The IGA recommends:

- **Clinical training records:** to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer
- **Statutory and mandatory training records:** to be kept for ten years after training completed
- **Other training records:** keep for six years after training completed.

Upon termination of contract, records must be held up to and beyond their statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS business purposes, in accordance with Retention Instrument 122. They are not exempt from Principle 5 of the DPA.

To reduce the burden of storage and for reasons of confidentiality it is recommended that a summary be prepared and held until the employee's 75th birthday or 6 years after leaving whichever is the longer and then reviewed.

[70] CIPD – Retention of records factsheet (registration required) http://www.cipd.co.uk/hr-resources/factsheets/retention-hr-records.aspx and ACAS - Advisory booklet - Personnel data and record keeping http://www.acas.org.uk/index.aspx?articleid=717

Where a summary is made it must contain as a minimum:

- A summary of the employment history with dates
- Pension information including eligibility
- Any work related injury
- Any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- Professional training history and professional qualifications related to the delivery of care
- List of buildings where the member of staff worked and the dates worked in each location.

Good Practice for a Staff Record Summary:

Barts Health NHS Trust staff record summary contains the following fields:

- Name
- Previous names
- Assignment number
- Pay bands
- Date of birth
- Addresses
- Positions held
- Start and end dates
- Reason for leaving
- Building or sites worked at.

Disciplinary case files can 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.

Email and Record Keeping Implications

One of the most important, yet often neglected, containers of information are the email accounts of staff, which is why it deserves a special mention in this Code[71]. 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.

A common problem with email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Solutions such as email archiving and ever larger mailbox quotas do not encourage staff to meet the standard of storing email in the correct business context and to declare the email as a record.

Where email archiving solutions are of benefit is as a backup, or to identify key individuals where their entire email correspondence can be preserved as a public record. Where

[71] TNA Managing emails
http://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/managing-email/

email is declared as a record or as a component of a record, the entire email must be kept including attachments so the record remains integral - for example an email approving a business case must be saved with the business case file.
All staff need to be adequately trained in required email storage and organisations need to undertake periodic audits of working practice to identify and address poor practice.

Automatic deletion of email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation[72].

Legal holds can take many forms and records cannot be destroyed if there is a known process or an expectation that records will be needed for a future legal process. This may include national or local inquiries, criminal investigation, and expected cases of litigation or records that may be requested under FOI or subject access.

This means that no records 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 NHS mail system allows a single email account for every staff member that can follow the individual through the course of their career. When staff transfer from one NHS organisation another NHS organisation, they must ensure that no sensitive personal data relating to the former organisation is transferred.

It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of security classified information. This is facilitated by staff storing only those that need to be retained on an ongoing basis. Emails that are the sole record of an event or issue, for example an exchange between a clinician and a patient, should be copied in to the relevant clinical record rather than being simply deleted.

Records Created via 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.

Records Created Through Bring Your Own Device (BYOD)

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

When an individual staff member no longer works for the employing organisation, any information that staff take away could be a risk to the organisation. If this includes sensitive personal data, this is reportable to the ICO and may be a breach of confidentiality. For this reason it is not permitted to store patient confidential data on any

[72] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31

insecure device or system that does not meet national requirements. The IGA has issued a guide for BYOD which clarifies the issues[73].

Cloud Based Records

Use of cloud based solutions for health and social care are increasingly being considered 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[74]. The ICO has guidance on cloud storage[75] they also advise to conduct a privacy impact assessment for any potential cloud solutions.

The NHS has a prohibition on storing patient identifiable data outside of England[76] where there is any link to national systems or applications (e.g. N3 or NHSmail), so any solution must have servers that can be traced to England if it is going to be used to store patient data.

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 and this may be technically challenging.

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.

Where personal data is stored there is also the risk of breaching the requirements of the DPA not to store personal information longer than necessary.

Website as a Business Record

As people interact with their public services, more commonly it is the internet and websites in particular that provide information, just as posters, publications and leaflets once did exclusively.

A person's behaviour may be a result of interaction with a website and it is considered part of the record of the activity.

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate, or 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 place of deposit, but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record.

The UK Government Web Archive[77] (part of TNA) undertook two central crawls of all NHS sites in 2011 and 2012 and may have captured some from 2004 onwards, but the information captured will not include all levels of the sites or some dynamic content.

[73] IGA Bring Your Own Device IG Guidance https://www.igt.hscic.gov.uk/Resources/BYOD.pdf
[74] TNA Guidance on Cloud Storage and Digital Preservation http://www.nationalarchives.gov.uk/documents/CloudStorage-Guidance_March-2015.pdf
[75] ICO Cloud Computing https://ico.org.uk/for-the-public/online/cloud-computing/
[76] HSCIC Information Governance Offshore Support Requirements http://systems.hscic.gov.uk/infogov/igsoc/links/offshoring.pdf
[77] The UK Government Web Archive: http://www.nationalarchives.gov.uk/webarchive/default.htm

Scanned Records

This section applies to health and care records as much as it does to corporate records.

Where scanning is used, the main consideration is that the information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it can be demonstrated that the scan is an authentic record and there are technical and organisational means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.

If this is a record type which must or may be selected and transferred to a place of deposit, the place of deposit should be asked whether they wish to preserve the hard copy and/or the scans. If the hard copy is retained, this will constitute 'best available evidence' for legal purposes, rather than the scanned copy.

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 of electronic, can be admissible as evidence[78].

The standard, 'BS 10008 Electronic Information Management - Ensuring the authenticity and integrity of electronic information', specifies the method of ensuring that electronic information remains authentic[79]. The standard deals with both 'born digital' and scanned records. The best way to ensure that records are scanned to the appropriate standard is to use a supplier or service that meets the standard. It is expected that all large scale digitisation projects will receive assistance from industry experts to ensure that the records are scanned to standard.

For small scale scanning requirements or those records where there is a low risk of being required to prove their authenticity, organisations may decide to do their own scanning.

Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original. 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:

- 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
- 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 such as Portable Document Format (PDF).

Before you begin scanning, check that those for whom you may have to produce records for will accept an authentic copy.

[78] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31
[79] BS 10008 Electronic Information Management - Ensuring the authenticity and integrity of electronic information (subscription required)
http://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/

Some common mistakes occur in scanning by:

- Only scanning one side and not both sides, including blank pages
- 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
- Not having a long term plan to enable the digitised records to be stored or accessed over the period of their retention.

Duplicate Records

Within any record keeping system, there is a primary instance which can be considered the version that needs to be kept and this will be normally be held by the person or the team with the function to provide the service or activity about which the records relates.

It is not necessary to keep duplicate instances of the same record unless it is used in another process and is then a part of a new record. An example of this is incident forms. Once the information is transcribed into the incident management system, there is no longer a need to hold the (now) duplicate instance of the original form used to record the incident. Where clinical systems produce duplicate records such as print outs of clinical records these must be marked as a copy to prevent their use as a primary record.

Edisclosure/Ediscovery and Records Implications

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 disclose to the other party and dispute authenticity. In some jurisdictions this is called discovery, but in UK the process is known as disclosure. The disclosure of electronic records is referred to as Edisclosure or Ediscovery.

The relevant rule for disclosure and admissibility of evidence is given in the Ministry of Justices Civil Procedure Rules' Rules and Practice Directions as Rule 31[80]. Proof statements can be required in some cases[81].

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, this process will be much easier to provide documents as evidence.

[80] Civil Procedure Rules part 31 Disclosure and Inspection of Documents https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31
[81] Civil Evidence Act 1995 http://www.legislation.gov.uk/ukpga/1995/38/section/8

Section 4: Retention Schedule

Note on Public Records Act 1958

Retention periods given in this schedule are those for operational purposes. Selection for transfer under the Public Records Act 1958 (referred to in this section as the Act) is a separate process designed to ensure the permanent preservation of a small core (typically 2-5%) of key records which will:

- Enable the public to understand the working of the organisation and its impact on the population it serves and
- Preserve information and evidence likely to have long-term research value.

PoDs have a good working knowledge of the use made of records after transfer and will be able to provide more detailed advice to supplement the guidance in this Code.

Selection may take place at any time in advance of transfer and in the case of digital records, preferably at or before the point at which they are created. Records may be selected as a class (for example all board minutes) or at lower levels down to individual files or items. Where it is known a record will form part of the public record at creation, it must be preserved locally until such time it can be transferred. The retention periods must be applied at creation and not as part of a reactive process such as organisational change. Older records that may still be in the possession of organisation may need to be reviewed and reappraised in the light of the more explicit recommendations for retention of records for the public record in this Code.

Records must be selected in accordance with the guidance contained in this Code, and any supplementary guidance issued by TNA or local guidance from the relevant PoD, which should always be consulted in advance:

- 'Transfer to PoD' - this class of records should normally transfer in its entirety to the PoD (trivial or duplicate items may be excepted)
- 'Possible transfer to PoD' - all, some or none of this class may be selected as agreed with the PoD
- Other records should not normally be selected for transfer

If this includes a decision not to select a class listed for transfer, or to select records not listed for transfer, the reason should be published in the records management policy or equivalent.

Records of individual persons may be selected and transferred if the PoD agrees, provided this is necessary and proportionate in relation to the broadly historical purposes of the Public Records Act 1958. Historically about 20% of NHS organisations have selected some individual patient records.

The Public Records Act 1958 is not designed to support the current operational research activities of the NHS and records should not be selected if that is the only or primary purpose in doing so. As patient confidentiality will normally prevent use for many decades after transfer and the resource involved will be substantial, it should only be considered where one or more of the factors listed below apply and for a sample or sub-set of records[82]. Any records selected should normally be retained within the NHS (under the

[82] For possible approaches to this see:

terms of Retention Instrument 122, which applies to individual patient records in general) until the patient is known, or can be assumed to be deceased. This is so that they continue to be readily available to support further medical care if necessary.

Any policy to select patient records should only be agreed after consultation with appropriate clinicians, including the Caldicott Guardian and research lead. This decision and the reasoning behind it should be published in the records management policy of the organisation or its equivalent. Any objections by patients to the selection of their individual patient record should be respected.

The following factors should be taken into account when considering selection of patient records:

- The organisation has an unusually long or complete run of records of a given type
- The records relate to population or environmental factors peculiar to the locality
- The records are likely to support research into rare or long-term conditions
- The records relate to an event or issue of significant local or national importance (for example a public inquiry or a major incident)
- 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 concerned
- The records throw particular light on the functioning, or failure, of the organisation, or the NHS in general
- The records relate to a significant piece of published research

Retention of records in the digital age can be problematic. This is because of a number of factors inherent to electronic record keeping. The fragility of software and the equipment it runs on means that long term retention of digital information is very difficult.

Good Practice about blanket retention rules:

Rotherham Doncaster and South Humber NHS Foundation Trust (RDASH) as a mental health and community provider has now agreed to retain all discharged adult patient files for a minimum of 20 years, where there is a possibility that patients may have a dual diagnosis one of which may be related to mental health.

The retention of information for the purpose of direct care of a patient will never be questioned and the ability of electronic care systems to store information means that the potential of 'whole care records' may be possible for the life of a patient across all care sectors.

The retention periods listed in this retention schedule must always be considered minimum.

For more information, see R v Northumberland County Council and the Information Commissioner (23 July 2015)[83]. This provides assurance that it is legitimate to vary common practice/guidance where a well-reasoned case for doing so is made.

---

http://www.healtharchives.org/docs/hospital_case_records_2006_final_version.pdf

[83] http://www.bailii.org/ew/cases/EWHC/Admin/2015/2134.html

Clinical records are problematic to preserve permanently in an archive or by the organisations that created them. Following appraisal, medical records or a series of records, may be worthy of permanent preservation for reasons other than care, usually as part of a portfolio of clinical work. Section 33 of the DPA is often quoted as the basis for preservation. An application of the Section 33 exemption must have regard for the patient's wishes where they have been indicated, which respects the duty of confidence as this is a limited exemption which only provides exemption from DPA Principles 2 and 5 and some subject access requests.

Good Practice at The National Archives:

Some of the allegations relating to abuse by Jimmy Savile at NHS sites dated back to 1954 and in many cases, investigators reported great difficulty in tracing records or witnesses over such a long period of time.

With the exception of visitor books, all the types of records found useful by investigation teams were core records listed in the 2006 NHS Records Management Code of Practice as appropriate for potential selection and transfer to places of deposit appointed under the Public Records Act 1958.

In 16 out of 39 cases, investigators referred to transferred material and where significant transfers had been implemented in accordance with the Act, such as at South London and Maudsley NHS Foundation Trust, Greater Manchester West Mental Health NHS Foundation Trust, Nottinghamshire Healthcare NHS Trust or Leeds Teaching Hospitals NHS Trust; this was useful in identifying visits by Saville, tracing staff or patient witnesses and corroborating statements.

There were a number of Trusts where no transfers had been made and no records at all had survived.

Where the patient has died the DPA no longer applies, the FOIA becomes the relevant legislation as the FOIA applies regardless as to whether the individual is or is not alive.

Section 41 of the FOIA and the duty of confidence remains relevant and the records cannot be accessed by anyone who does not have a lawful basis to view the records. Section 41 will therefore apply if the applicant does not have a claim under the Access to Health Records Act 1990 and the duty of confidence will need to be considered. An exemption will apply if the disclosure of the information would constitute a breach of confidence actionable by that or any other person. See Pauline Bluck v Information Commissioner and Epsom & St Helier University Hospitals NHS Trust (EA/2006/0090, 17 5 Information about the deceased 20130522 Version: 1.1 September 2007[84])

When a person is deceased the Access to Health Records Act 1990 may be used to access the health record for a limited purpose by specified individuals. Therefore FOIA decisions indicate that, in general, clinical information will remain confidential for several decades after death. The duty of confidence must always be considered to apply unless there can

[84] https://ico.org.uk/media/for-organisations/documents/1202/information-about-the-deceased-foi-eir.pdf

be no persons who would suffer a detriment if the information were released. This is often quoted as 100 years but will be different for every case[85].

[85] The National Archives - Access to NHS Records transferred to places of deposit under the Public Records Act 1958: http://www.nationalarchives.gov.uk/documents/information-management/access-to-nhs-records-transferred-to-places-of-deposit.pdf

Records Held by Health and Social Care Organisations

See Appendix Three or click on item headings below for full details.

1. Care Records with standard retention periods

- Adult health records
- Adult social care records
- Children's records including midwifery, health visiting and school nursing
- Electronic Patient Records Systems
- General Dental Services records
- GP patient records
- Mental Health records
- Obstetric records, maternity records and antenatal and post natal records

2. Care Records with non-standard retention periods

- Cancer/oncology - the oncology records of any patient
- Contraception, sexual health, family planning and Genito-Urinary Medicine (GUM)
- Human Fertilisation & Embryology Authority (HFEA) records of treatment provided in licenced treatment centres
- Medical record of a patient with Creutzfeldt-Jakob disease (CJD)
- Record of long term illness or an illness that may reoccur

3. Pharmacy Records

- Information relating to controlled drugs
- Pharmacy prescription records - see also Information relating to controlled drugs

4. Pathology Records

- Pathology Reports/Information about specimens and samples

5. Event & Transaction Records

- Blood bank register
- Clinical Audit
- Chaplaincy records
- Clinical Diaries
- Clinical Protocols
- Data sets released by HSCIC under a data sharing agreement
- Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media
- Equipment maintenance logs
- General Ophthalmic Services patient records related to NHS financial transactions
- GP temporary resident forms
- Inspection of equipment records
- Notifiable disease book
- Operating theatre records
- Pathology Reports/Information about Specimens and samples
- Patient Property Books
- Referrals not accepted
- Requests for funding for care not accepted

- Screening, including cervical screening and information where no cancer/illness is detected
- Smoking cessation
- Transplantation Records
- Ward handover sheet

6. **Telephony Systems & Services Records - 999 phone numbers, 111 phone numbers, ambulance, out of hours and single point of contact call centres.**
   - Recorded conversation which may later be needed for clinical negligence purpose
   - Recorded conversation which forms part of the health record
   - The telephony systems record

7. **Births, Deaths & Adoption Records**
   - Birth Notification to Child Health
   - Birth Registers
   - Body Release Forms
   - Death - cause of death certificate counterfoil
   - Death register information sent to General Registry Office on monthly basis
   - Local Authority Adoption Record (normally held by the local authority children's services)
   - Mortuary records of deceased
   - Mortuary Register
   - NHS medicals for adoption records
   - Post Mortem records

8. **Clinical Trials & Research Records**
   - Advanced Medical Therapy Research Master File
   - Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014
   - European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states' area
   - Research data sets
   - Research Ethics Committee's documentation for research proposal
   - Research Ethics Committee's minutes and papers

9. **Corporate Governance Records**
   - Board Meetings
   - Board Meetings (Closed Boards)
   - Chief Executive records
   - Committees Listed in the Scheme of Delegation or that report into the Board and major projects
   - Committees/Groups/sub-committees not listed in the Scheme of Delegation
   - Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media
   - Incidents (serious)
   - Incidents (not serious)
   - Non-Clinical Quality Assurance Records
   - Patient Advice and Liaison Service (PALS) records

- Policies, strategies and operating procedures including business plans

10. Communications

- Intranet site
- Patient information leaflets
- Press releases and important internal communications
- Public consultations
- Website

11. Staff Records & Occupational Health

- Duty Roster (Staff providing Care)
- Exposure monitoring information
- Occupational Health Reports
- Occupational Health Report of Staff member under health surveillance
- Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses
- Staff Record
- Staff Record Summary
- Timesheets (original record)
- Staff Training records

12. Procurement

- Contracts sealed or unsealed
- Contracts - financial approval files
- Contracts - financial approved suppliers' documentation
- Tenders (successful)
- Tenders (unsuccessful)

13. Estates

- Building plans and records of major building work
- CCTV
- Equipment monitoring and testing and maintenance work where asbestos is a factor
- Equipment monitoring and testing and maintenance work
- Inspection reports
- Leases
- Minor building works
- Photographic collections of service locations and events and activities
- Radioactive Waste
- Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhydrin Test
- Surveys

14. Finance Records

- Accounts
- Benefactions
- Debtor records cleared
- Debtor records not cleared
- Donations
- Expenses
- Final annual accounts report
- Financial records of transactions
- Petty cash

- Private Finance initiative (PFI) files
- Salaries paid to staff
- Superannuation records

15. Legal, Complaints & Information Rights

- Complaints case file
- Fraud case files
- Freedom of Information (FOI) requests and responses and any associated correspondence
- FOI requests where there has been a subsequent appeal
- Industrial relations including tribunal case records
- Litigation records
- Patents / trademarks / copyright / intellectual property
- Software licences
- Subject Access Requests (SAR) and disclosure correspondence
- Subject access requests where there has been a subsequent appeal

Useful websites and links

Archives and Records Association: http://www.archives.org.uk/

British Association for Sexual Health and HIV - Guidelines:
http://www.bashh.org/BASHH/Guidelines/Guidelines/BASHH/Guidelines/Guidelines.aspx?hkey=072c83ed-0e9b-44b2-a989-7c84e4fbd9de

Department of Health Information Governance Toolkit (hosted by the HSCIC):
https://nww.igt.hscic.gov.uk/

Department of Health - Reference guide to consent for examination or treatment 2009 Second edition:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/138296/dh_103653__1_.pdf

Directions given under the Human Fertilisation and Embryology Act 1990 as amended:
http://www.hfea.gov.uk/docs/General_directions_0012.pdf

Information Commissioner's Office: https://ico.org.uk/

Information and Records Management Society: http://www.irms.org.uk/

Information Governance Alliance: www.hscic.gov.uk/iga

Local Government Association ESD standards: http://standards.esd.org.uk/?

Ministry of Justice: Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (2009):
https://ico.org.uk/media/for-organisations/research-and-reports/1432475/foi-section-46-code-of-practice-1.pdf

The National Archives: http://www.nationalarchives.gov.uk/

The National Archives - Records management in SharePoint 2010-Implications and issues:
http://www.nationalarchives.gov.uk/documents/information-management/review-of-records-management-in-sharepoint-2010.pdf

NHS Scotland - Decommissioning of NHS Premises:
http://www.gov.scot/resource/doc/310165/0097865.pdf

NHS Security Management Service - Procedures for placing a risk of violence marker on electronic and paper records:
http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/SecurityManagement/Procedures.pdf

Professional Record Standards Body for health and social care:
http://theprsb.org/standards-matters/

Royal College of Nursing - Abbreviations and other short forms in patient/client records:
http://www.rcn.org.uk/__data/assets/pdf_file/0011/328925/003595.pdf

The State Records Authority of New South Wales - Managing authentic and reliable records in SharePoint 2010:
http://www.records.nsw.gov.au/recordkeeping/advice/designing-implementing-and-managing-systems/sharepoint-2010-recordkeeping-considerations/managing-authentic-and-reliable-records#5.1%20Access%20and%20security

Appendix One

The Information Governance Alliance and the Department of Health are very grateful to the following that provided their time and expertise on the project group, authoring team and reviewing team developing this update:

Daniel Beaumont (NHS Scotland); Richard Birmingham (Health and Social Care Information Centre); Jan Gavin (NHS England); Laura Hynds (Archives and Records Association); Kevin Mulley (The National Archives); Denise Nixon (Department of Health Northern Ireland); Emily Overton (Rotherham Doncaster & South Humber NHS Foundation Trust / RM Girl); Daniel Scott-Davies (Archives and Records Association); Martin Staples (NHS England) and Lynn Young (NHS England /The British Library).

Additionally, the Information Governance Alliance was supported by the following who participated in the Expert Reference Group to review the draft versions:

Sarah Ames; Raz Bassi; Kim Bellis; Elisabeth Belisle; Vikki Cochran; Yvonne Cutler; Nicola Gould; Theresa Hogan; Barry Moult; Juliet Norris; Jonathan McKee; Patricia O'Rourke; Cora Suckley; Helen Thorn; Tom Walker and Lynn Wyeth.

We are very grateful to the following for the time and effort put into responding to the public consultation:

5 Boroughs Partnership NHS Foundation Trust; ARA; Betsi Cadwaladar University Health Board (Wales); Block Lane Surgery; British Medical Association (Ethics, IT and Joint GP IT areas); Care Quality Commission; Department of Health; EMIS Health; Frimley Health NHS Foundation Trust; Genomics England; Gloucestershire Hospitals NHS Foundation Trust; Great Ormond Street Hospital for Children NHS Foundation Trust; Group 5 Training; Health and Social Care Information Centre; Health Research Authority; IHRIM; IRMS; Medicines and Health Regulatory Authority; Medway NHS Foundation Trust; NHS Arden and Greater East Midlands Commissioning Support Unit; NHS England; NHS Research and Development Forum; Northumberland, Tyne and Wear NHS Foundation Trust; Pennine Care NHS Foundation Trust; Peterborough City Council; Public Health England; Royal Cornwall Hospital NHS Trust; Royal Liverpool and Broadgreen University Hospitals NHS Foundation Trust; Salford Royal NHS Foundation Trust; ScanDox; Shropshire Community Health NHS Trust; South Tyneside NHS Foundation Trust; Tech UK; Western Sussex Hospitals NHS Foundation Trust and Yorkshire Ambulance Service NHS Trust.

Appendix Two

The main standards setting bodies for health and care in England are:

- Academy of Medical Royal Colleges (AoMRC) (hosted by the Royal College of Physicians)
  https://www.rcplondon.ac.uk/projects/outputs/generic-medical-record-keeping-standards

- British Medical Association
  http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records

- General Medical Council
  http://www.gmc-uk.org/guidance/index.asp

- Health and Care Professions Council
  http://www.hcpc-uk.org/

- Nursing and Midwifery Council
  https://www.nmc.org.uk/standards/code/

  Royal College of General Practitioners (with the DH and the BMA)
  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/215680/dh_125350.pdf

- Royal College of Nursing
  http://www.rcn.org.uk/development/health_care_support_workers/professional_issues/record_keeping

- Royal College of Obstetricians & Gynaecologists
  https://www.rcog.org.uk/en/guidelines-research-services/guidelines/

- Royal College of Pathologists
  http://www.rcpath.org/Resources/RCPath/Migrated%20Resources/Documents/G/G031_RetentionAndStorage_Apr15.pdf

- Royal Pharmaceutical Society
  http://www.rpharms.com/home/about-pharmacy.asp

- Royal College of Physicians
  https://www.rcplondon.ac.uk/

- Standardisation Committee for Care Information
  http://www.hscic.gov.uk/isce

Appendix Three

The Independent Inquiry into Child Sexual Abuse (IICSA) chaired by Hon. Dame Lowell Goddard has 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. Investigations will take into account a huge range of records which may include, but are not limited to, adoption records, safeguarding records, incident reports, complaints and enquiries. Outside of this inquiry, it is also important to consider that these records are likely to require longer than the standard retention periods given in this Code. Before any records are destroyed you are advised to check for any further update from the inquiry website at www.iicsa.org.uk.

Before considering the selection of records under the Public Records Act 1958, this should be discussed with the relevant place of deposit to take account of exceptional local circumstances and defunct record types not listed here.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
1. Care Records with standard retention periods				
Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Adult social care records	End of care or client last seen	8 years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Electronic Patient Records System (EPR) NB: The IGA is undertaking further work to refine the rules for record retention and to specify requirements for EPR systems	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.
General Dental Services records	Discharge or patient last seen	10 Years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
GP Patient records	Death of patient	10 years after death - see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: • Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated • Where a patient is known to have emigrated records may be reviewed and destroyed after 10 years • If the patient comes back within the 100 years, the retention reverts to 10 years after death.
Mental Health records	Discharge or patient last seen	20 years or 8 years after the patient has died	Review and if no longer needed destroy	Covers records made where the person has been cared for under the Mental Health Act 1983 as amended by the Mental Health Act 2007. This includes psychology records. Retention solely for any persons who have been sectioned under the Mental Health Act 1983 must be considerably longer than 20 years where the case may be ongoing. Very mild forms of adult mental health treated in a community setting where a full recovery is made may consider treating as an adult records and keep for 8 years after discharge. All must be reviewed prior to destruction taking into account any serious incident retentions.
Obstetric records, maternity records and antenatal and post natal records	Discharge or patient last seen	25 years	Review and if no longer needed destroy	For the purposes of record keeping these records are to be considered as much a record of the child as that of the mother.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
2. Care Records with Non-Standard Retention Periods				
Cancer/Oncology - the oncology records of any patient	Diagnosis of Cancer	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of any cancer must be retained in case of future reoccurrence. Where the oncology records are in a main patient file the entire file must be retained. Retention is applicable to primary acute patient record of the cancer diagnosis and treatment only. If this is part of a wider patient record then the entire record may be retained. Any oncology records must be reviewed prior to destruction taking into account any potential long term research value which may require consent or anonymisation of the record.
Contraception, sexual health, Family Planning and Genito-Urinary Medicine (GUM)	Discharge or patient last seen	8 or 10 years (see Notes)	Review and if no longer needed destroy	Basic retention requirement is 8 years unless there is an implant or device inserted, in which case it is 10 years. All must be reviewed prior to destruction taking into account any serious incident retentions. If this is a record of a child, treat as a child record as above.
HFEA records of treatment provided in licenced treatment centres		3, 10, 30, or 50 years	Review and if no longer needed destroy	Retention periods are set out in the HFEA guidance at: http://www.hfea.gov.uk/docs/General_directions_0012.pdf
Medical record of a patient with Creutzfeldt-Jakob Disease (CJD)	Diagnosis	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of CJD must be retained. Where the CJD records are in a main patient file the entire file must be retained. All must be reviewed prior to destruction taking into account any serious incident retentions.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care. The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
3. Pharmacy The IGA are conducting further work to expand this section which will be updated in the near future. As an interim measure you can view a list of Pharmacy records and their associated retention periods and actions by clicking on this link to the NHS East and South East Specialist Pharmacy Services retention schedule.				
Information relating to controlled drugs	Creation	See Notes	Review and if no longer needed destroy	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) guide can be found at the link (subscription required): http://www.rpharms.com/support/mep.asp Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years. NHS BSA will hold primary data for 20 years and then review. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see: http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/
Pharmacy prescription records. See also **Information relating to controlled drugs.**	Discharge or patient last seen	2 Years	Review and if no longer needed destroy	There will also be an entry in the patient record and a record held by the NHS Business Services Authority. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see: http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/

Record Type	Retention start	Retention period	Action at end of retention period	Notes
4. Pathology				
Pathology Reports/Information about specimens and samples	Specimen or sample is destroyed	See Notes	Review and consider transfer to a Place of Deposit	This Code is concerned with the information about a specimen or sample. The length of storage of the clinical material will drive the length of time the information about it is to be kept. For more details please see: https://www.rcpath.org/resourceLibrary/the-retention-and-storage-of-pathological-records-and-specimens--5th-edition-.html Retention of samples for clinical purposes can be for as long as there is a clinical need to hold the specimen or sample. Reports should be stored on the patient file. It is common for pathologists to hold duplicate reports. For clinical purposes this is 8 years after the patient is discharged for an adult or until a child's 25th birthday whichever is the longer. After 20 years for adult records there must be an appraisal as to the historical importance of the information and a decision made as to whether they should be destroyed of kept for archival value.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
5. Event & Transaction Records				
Blood bank register	Creation	30 Years minimum	Review and consider transfer to a Place of Deposit	
Clinical Audit	Creation	5 years	Review and if no longer needed destroy	
Chaplaincy records	Creation	2 years	Review and consider transfer to a Place of Deposit	See also Corporate Governance Records
Clinical Diaries	End of the year to which they relate	2 years	Review and if no longer needed destroy	Diaries of clinical activity & visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.
Clinical Protocols	Creation	25 years	Review and consider transfer to a Place of Deposit	Clinical protocols may have archival value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (see Corporate Records).
Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	http://www.hscic.gov.uk/media/15729/DARS-Data-Sharing-Agreement/pdf/Data_Sharing_Agreement_2015v2%28restricted_editing%29.pdf
Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	20 Years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by an instrument of retention and if a Place of Deposit or the National Archives do not class them as a record of archival importance they are to be destroyed after 20 years.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Equipment maintenance logs	Decommission-ing of the equipment	11 years	Review and consider transfer to a Place of Deposit	
General Ophthalmic Services patient records related to NHS financial transactions	Discharge or patient last seen	6 Years	Review and if no longer needed destroy	
GP temporary resident forms	After treatment	2 years	Review and if no longer needed destroy	Assumes a copy sent to the responsible GP for inclusion in the primary care record
Inspection of equipment records	Decommission-ing of the equipment	11 Years	Review and if no longer needed destroy	
Notifiable disease book	Creation	6 years	Review and if no longer needed destroy	
Operating theatre records	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	If transferred to a Place of Deposit the duty of confidence continues to apply and can only be used for research if the patient has consented or the record is anonymised.
Patient Property Books	End of the year to which they relate	2 years	Review and if no longer needed destroy	
Referrals not accepted	Date of rejection.	2 years as an ephemeral record	Review and if no longer needed destroy	The rejected referral to the service should also be kept on the originating service file.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Requests for funding for care not accepted	Date of rejection	2 years as an ephemeral record	Review and if no longer needed destroy	
Screening, including cervical screening, information where no cancer/illness detected is detected	Creation	10 years	Review and if no longer needed destroy	Where cancer is detected see **2 Cancer / Oncology**. For child screening treat as a child health record and retain until 25th birthday or 10 years after the child has been screened whichever is the longer.
Smoking cessation	Closure of 12 week quit period	2 years	Review and if no longer needed destroy	
Transplantation Records	Creation	30 Years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.hta.gov.uk/codes-practice
Ward handover sheet	Date of handover	2 years	Review and if no longer needed destroy	This retention relates to the ward. The individual sheets held by staff must be destroyed confidentially at the end of the shift.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
6. Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).				
Recorded conversation which may later be needed for clinical negligence purpose	Creation	3 Years	Review and if no longer needed destroy	The period of time cited by the NHS Litigation Authority is 3 years
Recorded conversation which forms part of the health record	Creation	Store as a health record	Review and if no longer needed destroy	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.
The telephony systems record (not recorded conversations)	Creation	1 year	Review and if no longer needed destroy	This is the absolute minimum specified to meet the NHS contractual requirement.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
7. Births, Deaths & Adoption Records				
Birth Notification to Child Health	Receipt by Child health department	25 years	Review and if no longer needed destroy	Treat as a part of the child's health record if not already stored within health record such as the health visiting record.
Birth Registers	Creation	2 years	Review and actively consider transfer to a Place of Deposit	Where registers of all the 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 a Place of Deposit at the end of this retention period. Information is also held in the NHS Birth Notification Service electronic system and by the Office for National Statistics. Other information about a birth must be recorded in the care record.
Body Release Forms	Creation	2 years	Review and consider transfer to a Place of Deposit	
Death - cause of death certificate counterfoil	Creation	2 years	Review and consider transfer to a Place of Deposit	
Death register information sent to General Registry Office on monthly basis	Creation	2 years	Review and consider transfer to a Place of Deposit	A full dataset is available from the Office for National Statistics.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Local Authority Adoption Record (normally held by the Local Authority children's services)	Creation	100 years from the date of the adoption order	Review and consider transfer to a Place of Deposit	The primary record of the adoption process is held by the local authority children's service responsible for the adoption service.
Mortuary Records of deceased	End of year to which they relate	10 Years	Review and consider transfer to a Place of Deposit	
Mortuary Register	Creation	10 Years	Review and consider transfer to a Place of Deposit	
NHS Medicals for Adoption Records	Creation	8 years or 25th birthday	Review and consider transfer to a Place of Deposit	The health reports will feed into the primary record held by the local authority children's services. This means that the adoption records held in the NHS relate to reports that are already kept in another file which is kept for 100 years by the appropriate agency and local authority.
Post Mortem Records	Creation	10 years	Review and if no longer needed destroy	The primary post mortem file will be maintained by the coroner. The coroner will retain the post mortem file including the report. Local records of post mortem will not need to be kept for the same extended time.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
8. Clinical Trials & Research For clinical trials record retention please see the MHRC guidance at https://www.gov.uk/guidance/good-clinical-practice-for-clinical-trials				
Advanced Medical Therapy Research Master File	Closure of research	30 years	Review and consider transfer to a Place of Deposit	See guidance at: https://www.gov.uk/guidance/advanced-therapy-medicinal-products-regulation-and-licensing
Clinical Trials Master File of a trial authorised under the European portal under Regulation (EU) No 536/2014	Closure of trial	25 years	Review and consider transfer to a Place of Deposit	For details please see: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.158.01.0001.01.ENG
European Commission Authorisation (certificate or letter) to enable marketing and sale within the EU member states area	Closure of trial	15 years	Review and consider transfer to a Place of Deposit	For details please see: http://ec.europa.eu/health/files/eudralex/vol-2/a/vol2a_chap1_2013-06_en.pdf
Research data sets	End of research	Not more than 20 years	Review and consider transfer to a Place of Deposit	For details please see: http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf
Research Ethics Committee's documentation for research proposal	End of research	5 years	Review and consider transfer to a Place of Deposit	For details please see: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/

Record Type	Retention start	Retention period	Action at end of retention period	Notes
				Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research the data may not need to be kept once the purpose has expired. For example data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For more significant research a Place of Deposit may be interested in holding the research. It is best practice to consider this at the outset of research as orphaned personal data can inadvertently cause a data breach.
Research Ethics Committee's minutes and papers	Year to which they relate	Before 20 years but as soon as practically possible	Review and consider transfer to a Place of Deposit	Committee papers must be transferred to a Place of Deposit as a public record: http://www.hra.nhs.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/

Record Type	Retention start	Retention period	Action at end of retention period	Notes
9. Corporate Governance				
Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings
Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Act. If records are not excluded by such an instrument they must either be transferred to a Place of Deposit as a public record or destroyed 20 years after the record has been closed.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Incidents (serious)	Date of incident	20 Years	Review and consider transfer to a Place of Deposit	
Incidents (not serious)	Date of incident	10 Years	Review and if no longer needed destroy	
Non-Clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed destroy	
Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	
Policies, strategies and operating procedures including business plans	Creation	Life of organisa-tion plus 6 years	Review and consider transfer to a Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
10. Communications				
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
11. Staff Records & Occupational Health Although pension information is routinely retained until 100th birthday by the NHS Pensions Agency employers must retain a portion of the staff record until the 75th birthday.				
Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	
Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Record Summary	6 years after the staff member leaves	75tn Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see the good practice box Staff Record Summary used by an organisation.
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: • **Clinical training records** - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer • **Statutory and mandatory training records** - to be kept for ten years after training completed • **Other training records -** keep for six years after training completed.

Record Type	Retention start	Retention period	Action at end of retention period	Notes
12. Procurement				
Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
13. Estates				
Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
CCTV		See ICO Code of Practice	Review and if no longer needed destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Equipment monitoring and testing and maintenance work where asbestos is a factor	Completion of monitoring or test	40 years	Review and if no longer needed destroy	
Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed destroy	
Inspection reports	End of lifetime of installation	Lifetime of installation	Review	
Leases	Termination of lease	12 years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Minor building works	Completion of work	retain for 6 years	Review and if no longer needed destroy	
Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.
Radioactive Waste	Creation	30 years	Review and if no longer needed destroy	
Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhydrin Test	Date of test	11 years	Review and if no longer needed destroy	
Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
14. Finance				
Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. For benefactions, endowment, trust fund/legacies, offer to a Place of Deposit.
Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	
Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Expenses	Close of financial year	6 years	Review and if no longer needed destroy	
Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
15. Legal, Complaints & Information Rights				
Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.
FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed destroy	
Industrial relations including tribunal case records	Close of financial year	10 Years	Review and consider transfer to a Place of Deposit	Some organisations may record these as part of the staff record but in most cases they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit	

Record Type	Retention start	Retention period	Action at end of retention period	Notes
Patents / trademarks / copyright / intellectual property-	End of lifetime of patent or termination of licence/ action	Lifetime of patent or 6 years from end of licence/ action	Review and consider transfer to Place of Deposit	
Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed destroy	
Subject Access Request (SAR) and disclosure correspondence	Closure of SAR	3 Years	Review and if no longer needed destroy	
Subject Access Request where there has been a subsequent appeal	Closure of appeal	6 Years	Review and if no longer needed destroy	