Corporate Records Management Retention Appendix

Retention Appendix:
This Appendix sets out the retention period for different types of records relating to health and care organisations. Where indicated, Appendix III of the NHS Code of Practice should also be referred to. This sets out further detail relating to the management of specific types and formats of records. The following areas are covered: **Appendix – Part 1: Public and Statutory Inquiries** **Appendix – Part 2: Retention Schedule** **Appendix – Part 3: Guidance for operation use**

Appendix detail:

Appendix – Part 1: Public and Statutory Inquiries

Records form an important part of the evidence in inquiries. Inquiries take into account a huge range of records and what is required can vary by inquiry. When an inquiry is conducted, the Inquiry Team will issue detailed guidance setting out what types of records they are interested in. If you have any records that an inquiry requests, you must produce them or explain why you cannot produce them. Before any records relating to inquiries are destroyed, you must check with the Inquiries Team that they are no longer required. If you are in doubt regarding records that may or may not be of use for an inquiry, you must retain them until there is clear instruction from the inquiry.
Before considering the selection of records for permanent preservation under the Public Records Act 1958 (refer to section 5), you should discuss any inquiries with the relevant PoD to take account of exceptional local circumstances and defunct record types not listed here.
At the time of writing there are two independent Inquiries which have requested that large parts of the health and social care sector do not destroy any records that are, or may fall into the remit of the Inquiry:

- The Independent Inquiry into Child Sexual Abuse (IICSA) - this is due to finish in 2022. Records that should not be destroyed include children's records and any instances of allegations or investigations or any records of an institution where abuse has or may have occurred
- The Infected Blood Inquiry - further information about the records required can be found on their website

The Government has also committed to holding a public inquiry into its response to the coronavirus pandemic that began in March 2020. No details of what records will be required are known at this stage, but it is likely to require records relating to policy and decision making as a minimum.

Appendix – Part 2: Retention Schedule

The following information is important to ensure the retention schedule is used correctly.

The retention periods listed in this retention schedule must always be considered the minimum period. With justification, a retention period can be extended for the majority of cases, up to 20 years (refer to section five of the Code). For more information, refer to R v Northumberland County Council and the Information Commissioner (23 July 2015). This provides assurance that it is legitimate to vary common practice or guidance where a well-reasoned case for doing so is made.

Retention periods begin when the record ceases to be operational. This is usually at the point of discharge from care when the record is no longer required for current on-going business, or the patient or service user has died. There are some exceptions to this rule, whereby the retention begins from the date the record is created (for corporate records, such as policies, the retention may start from the date of publication). These are marked with an asterisk (*) in the schedule and may also contain further information in the notes for that entry.

If a record comes back into use during its retention period, then the retention period will reset and begin again from the end of the second period of use. This may mean that records will look as if they are being kept for longer than the retention times stated here, or even maximum periods as suggested by law, but this is acceptable where retention periods reset due to use (refer to section five of the Code).

The actions following review as set out in the schedule are as follows:

- Review and destroy if no longer required: Destroy refers to the confidential and secure destruction of the record with proof of destruction. These will be records with no archival value and there is no longer an ongoing business need to retain them for longer
- Review and dispose of if no longer required: 'Dispose of' refers to the secure destruction of a record OR the transferral to the appointed PoD for permanent preservation. A certificate of transfer will be provided as proof of transfer (and can act as evidence of disposal). Refer to section five of the Code for further information about permanent preservation.
- Review and consider transfer to PoD: This refers to records that are more likely to be transferred to the PoD, subject to their discussion and agreement about potential accession. Not all records considered for accession will be taken by the PoD. If the record has been offered and declined to be taken, and it has no further retention value, then it must be securely destroyed. Where you have potentially a new series of records for the PoD, you must discuss accessioning them before any action is taken
- Review and transfer to PoD: This refers to records that should be transferred to the PoD such as trust board minutes and final annual financial report - local agreement will already be in place to accession these

It is very important that any health and care records are reviewed before they are destroyed. This review should take into account:

- serious incidents which will require records to be retained for up to 20 years as set out in the schedule
use of the record during the retention period which could extend its retention
potential for long-term archival preservation - this may particularly be the case where the records relate to rare conditions such as Creutzfeldt-Jakob Disease records or innovative treatments, for example, new cancer treatments

If setting a retention period not covered by this Code, there are a number of factors to consider including:

- Legal or regulatory obligations: There may be a specific legal or regulatory reason to keep a record, which may also provide guidance on how long that record needs to be kept to meet that obligation
- Purpose of the record: The reasons you have created the record may also help define how long you need to keep them for. A record created for medico-legal reasons may need to be for a long period of time, whereas a record created for a specific event that has no post-event actions will attract a short retention period
- Number of records: The number of records in a series can help you set a retention period. It is worth noting that the number of records is not directly proportionate to a longer retention period (for example, the more records created, then the longer they must be kept). It should also be noted that the number of records is also not

indicative of historical value. Due to its type, one record may have historical value, where a series of 200+ records might not

- Service delivery: The uniqueness or niche way a service is delivered may lend itself to a longer retention period. PoDs can be interested in taking records relating to services that were delivered in a unique way
- Call or recall of records: If a record or series has a low recall rate, it could be indicative of a shorter retention period. Likewise records that are continually in use may require a longer retention period

Appendix – Part 3: Guidance for operation use

This appendix provides detailed advice on records management relating to specific types of records for example, transgender records, witness protection records and adopted persons records. These are presented in alphabetical order. It also provides advice on managing certain formats of records, for example, emails, cloud-based records and scanned records.

Category	Record Type	Retention Period	Disposal Action	Notes
CARE RECORDS	Adult health records not covered by any other section in this schedule (includes medical illustration records such as x-rays and scans as well as video and other formats. Also includes care plans)	8 years	Review and consider transfer to PoD	Records involving pioneering or innovative treatment may have archival value, and their long term preservation should be discussed with the local PoD or The National Archives. Also refer to Appendix III: ambulance service records.
CARE RECORDS	Adult social care records (including care plans)	8 years	Review and destroy if no longer required	
CARE RECORDS	Children's records (including midwifery, health visiting and school nursing) - can include medical illustrations, as well as video and audio formats	Up to 25th or 26th birthday	Review and destroy if no longer required	Retain until 25th birthday, or 26th if the patient was 17 when treatment ended.
CARE RECORDS	Clinical records that pre- date the NHS (July 1948)		Review and transfer to PoD	Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed.
CARE RECORDS	Dental records - clinical care records	15 years	Review, and destroy if no longer required	Based on Limitations Act 1980. This applies to all dental care settings and the BSA. This also includes FP17 or FP17O forms.
CARE RECORDS	Dental records - finance related	2 years	Review, and destroy if no longer required	These include PR forms. NHS BSA may retain financial records for a minimum of 6 years.

CARE RECORDS	Electronic Patient Record Systems (EPR)	Refer to notes	Review and destroy if no longer required	Where the system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain, demonstrating the destruction, then the Code should be followed in the same way for digital as well as paper records with a log kept of destruction. If the EPR does not have this capacity, then once records reach the end of their retention period, they should be made inaccessible to system users upon decommissioning. The system (along with the audit trails) should be retained for the retention period of the last entry related to the schedule.
CARE RECORDS	GP patient records - deceased patients	10 years	Review and destroy if no longer required	Confidentiality generally continues after death and records should be retained for medico-legal and possible public interest (for example, research) reasons. Review retention after 10 years when possible medico- legal reasons will lapse under requirements of the Limitation Act 1980. Destroy if the record holds no value for researchers. Also refer to Appendix III: GP records.
CARE RECORDS	GP patient records – living patients	Continual retention		If the patient has not been seen for 10 years, or a request for transfer to a new GP has not been received, the GP practice should check the Personal Demographics Service (PDS) for indication of death or other reason for no contact. If there is no reason to suggest no contact, then the record must be kept by the GP practice. If they have died, or transferred to a new practice, transfer the record to NHSE or the new provider respectively. These records cannot be disposed of as they may require further services as they get older. Also refer to Appendix III: GP records
CARE RECORDS	GP patient records – de-registered cases where the reason is unknown	100 years	Review and dispose of if no longer required	These are cases where the patient has de-registered from the practice, but the reason is unknown. It would be good practice for GPs to check if there is a reason for de-registration (death, missed registration at another practice, emigration etc.). It is not suggested that a retrospective check be carried out, but it would be good practice going forward to conduct a check for these cases. Once checked under General Medical Services (GMS) regulations, records should be sent to NHSE via Primary Care Support England (PCSE) operational processes. Also refer to Appendix III: GP records

CARE RECORDS	GP patient registrations form	6 years after the year of registration	Review and dispose of if no longer required	These need to be kept for 6 years as GP per capita payments are made based on registered patient numbers. Most GP practices scan the form into the patient's electronic record once it is created. The paper form can be destroyed securely once the minimum retention period has been reached, unless there is another reason to keep the form longer (this would be identified at the review stage).
CARE RECORDS	Integrated records – all organisations contribute to the same single instance of the record	Retain for period of longest specialty	Review and consider transfer to PoD	The retention time will vary depending upon which type of health and care settings have contributed to the record. Areas that use this model must have a way of identifying the longest retention period applicable to the record.
CARE RECORDS	Integrated records – all organisations contribute to the same record, but keep a level of separation (refer to notes)	Retain for relevant specialty period	Review and consider transfer to PoD	This is where all organisations contribute into the same record system but have their own area to contribute to and the system still shows a contemporaneous view of the patient record.
CARE RECORDS	Integrated records – all organisations keep their own records, but enable them to be viewed by other organisations	Retain for relevant specialty period	Review and consider transfer to PoD	This is the most likely model currently in use. Organisations keep their own records on their patients or service users but can grant 'view only' access to other organisations, to help them provide health and care to patients or service users.
CARE RECORDS	Mental health records including psychology records	20 years, or 10 years after death	Review and consider transfer to PoD	Covers records made under the Mental Health Act (MHA) 1983 (and 2007 amendments). Records retained solely for any person who has been sectioned under MHA1983 must be considered for longer than 20 years where the case is ongoing, or the potential for recurrence is high (based on local clinical judgment). This applies to records of patients or service users, regardless of whether they have capacity or not.
CARE RECORDS	Obstetrics, maternity, antenatal and postnatal records	25 years	Review and destroy if no longer required	For record keeping purposes, these are considered to be as much the child's record as the parent, so the longer retention period should be considered.

CARE RECORDS	Prison health records	10 years	Review and destroy if no longer required	A summary of their prison healthcare is sent to the person's new GP upon release and the record should be considered closed at the point of release. These records are unlikely to have long term archival value and should be retained by the organisations providing care in the prison, or successor organisations if the running of the service changes hands.
CARE RECORDS	Cancer/oncology records – any patient*	30 years, or 8 years after death	Review and consider transfer to PoD	Retention for these records begins at diagnosis rather than the end of operational use. For clinical care reasons, these records must be retained longer in case of re-occurrence. Where the oncology record is part of the main records, then the entire record must be retained.
CARE RECORDS	Contraception, sexual health, family planning, Genito-Urinary Medicine (GUM)	8 or 10 years	Review and destroy if no longer required	8 years for the basic retention requirement but this is increased to 10 in cases of implants or medical devices. If the record relates to a child, then retain in line with children's records. (Also refer to Appendix III: records dealt with under the NHS Trusts and Primary Care Trusts (Sexually transmitted disease) directions 2000).
CARE RECORDS	Creutzfeldt-Jakob Disease – patient records	30 years or 10 years after death	Review and consider transfer to PoD	Diagnosis records must be retained for clinical care purposes.
CARE RECORDS	Human Fertility and Embryology Authority (HFEA) records – treatment provided in licenced centres	3,10, 30 or 50 years	Review and destroy if no longer required	These retention periods are set out in HFEA guidance.
CARE RECORDS	Long-term illness, or illness that may reoccur – patient records	20 years, or 10 years after death	Review and destroy if no longer required	Necessary for continuation of clinical care. The primary record of the illness and course of treatment must be kept where the illness may reoccur or it is a life- long condition such as diabetes, arthritis or Chronic Obstructive Pulmonary Disease.

CARE RECORDS	Sexual Assault Referral Centres (SARC)	30 years, or 10 years after death (if known)	Review, and destroy if no longer required	These records need to be kept for medico- legal reasons because an individual may not be in a position to bring a case against the alleged perpetrator for a long time after the event. Once the retention period is reached, a decision needs to be made about continued retention. Records cannot be kept indefinitely just in case an individual might bring a case. Some individuals may never bring a case and indefinite retention may be seen as a breach of UK GDPR (keeping information longer than necessary). Consideration also needs to be given to the Police and Criminal Evidence Act 1984, Human Tissue Act 2004, and Criminal Procedure and Investigations Act 1996 legal requirements (other laws and regulations may also need to be taken into account).
CARE RECORDS	Controlled drugs - registers	2 years, (refer to notes)	Review and destroy if no longer required	Misuse of Drugs Act 2001. NHS England has issued guidance in relation to controlled drugs. Also refer to Appendix III: controlled drugs
CARE RECORDS	Controlled drugs - order books, requisitions etc	2 years	Review, and destroy if no longer required	Misuse of Drugs Act 2001.
CARE RECORDS	Pharmacy prescription records	2 years	Review and destroy if no longer required	A record of the prescription will also be held by NHS BSA and there will be an entry on the patient record. Further advice and guidance on pharmacy records can be found on the Specialist Pharmacy Service website.

CARE RECORDS	Pathology reports, information about samples	Refer to notes	Review and consider transfer to PoD	This Code is concerned with the information about a specimen or sample. The length of time clinical material (for example, a specimen) is stored will drive how long the information relating to it is retained. Sample retention can be for as long as there is a clinical need to hold it. Reports should be stored on the patient file. It is common for pathologists to hold duplicate records. For clinical purposes, these should be retained for eight years after discharge or until a child's 25th birthday. If information is retained for 20 years, it must be appraised for historical value, and a decision made about its disposal. Also refer to Appendix III: specimens and samples
CARE RECORDS	Blood bank register*	30 years minimum	Review and consider transfer to PoD	Need to be disposed of if there is no on-going need to retain them (such as the currently ongoing Infected Blood Inquiry), subject to any transfer to the PoD.
CARE RECORDS	Clinical audit*	5 years	Review and destroy if no longer required	Five years from the year in which the audit was conducted. This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period, for example, data from adult health records would be kept for 8 years.
CARE RECORDS	Chaplaincy records*	2 years	Review and consider transfer to PoD	Also refer to corporate governance records.
CARE RECORDS	Clinical diaries	2 years	Review and destroy if no longer required	Two years after the year to which they relate. Diaries of clinical activity and visits must be written up and transferred to the main patient record. If the information is not transferred from the diary (so the only record of the event is in the diary), then this must be retained for eight years and reviewed. Some staff keep hardback diaries of their appointments or business meetings. If these contain no personal data, they can be disposed of after two years.

CARE RECORDS	Clinical protocols*	20 years	Review and consider transfer to PoD	Clinical protocols may have preservational value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (refer to corporate governance records).
CARE RECORDS	Datasets released by NHS Digital and its predecessors	Delete with immediate effect	Delete in line with NHS Digital instructions	NHS Digital issue guidance through the Data Access Request Service (DARS) process on the retention and disposal of data released by them.
CARE RECORDS	Destruction certificates, or electronic metadata destruction stub, or record of clinical information held on physical media	20 years	Review and consider transfer to PoD	Destruction certificates created by public bodies are not covered by a retention instrument (if they do not relate to patient care and if a PoD or The National Archives do not accession them). They need to be destroyed after 20 years.
CARE RECORDS	Equipment maintenance logs	11 years	Review and destroy and no longer required	
CARE RECORDS	General ophthalmic services – patient records related to NHS financial transactions	6 years	Review and destroy if no longer required	
CARE RECORDS	GP temporary resident forms	2 years	Review and destroy if no longer required	This assumes a copy has been sent to the responsible GP for inclusion in the GP patient record.

CARE RECORDS	Inspection of equipment records	11 years	Review and destroy if no longer required	
CARE RECORDS	Notifiable diseases book*	6 years	Review and destroy if no longer required	
CARE RECORDS	Operating theatre records	10 years	Review and consider transfer to PoD	10 years from the end of the year to which they relate.
CARE RECORDS	Patient property books	2 years	Review and destroy if no longer required	Two years from the end of the year to which they relate.
CARE RECORDS	Referrals – NOT ACCEPTED	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record.
CARE RECORDS	Requests for care funding – NOT ACCEPTED	2 years	Review and destroy if no longer required	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record. NB: These may have potential PoD interest as what the NHS or social care can or cannot fund can sometimes be an issue of local or national significance and public debate. Refer to Appendix III: individual funding requests

CARE RECORDS	Screening* – including cervical screening – where no cancer or illness detected is returned	10 years	Review and destroy if no longer required	Where cancer is detected, refer to the cancer/oncology schedule.
CARE RECORDS	Screening – children	10 years or 25th birthday	Review and destroy if no longer required	Treat as a child health record and retain for either 10 years or up to 25th birthday, whichever is the LONGER.
CARE RECORDS	Smoking cessation	2 years	Review and destroy if no longer required	Retention begins at the end of the 12- week quit period.
CARE RECORDS	Transplantation records*	30 years	Review and consider transfer to PoD	Refer to guidance issued by the Human Tissue Authority.
CARE RECORDS	Ward handover sheets*	2 years	Review and destroy if no longer required	This information relates to the ward. Any individual sheets held by staff may be destroyed confidentially at the end of the shift.
TELEPHONY SYSTEMS AND SERVICES	Recorded conversations – which may be needed later for clinical negligence or other legal purposes*	6 years	Review and destroy if no longer required	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980. Further guidance is issued by NHS Resolution.

TELEPHONY SYSTEMS AND SERVICES	Recorded conversations – which form part of the health record*	Treat as a health record	Review and destroy if no longer required	It is advisable to transfer any relevant information into the main record, through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record, the recording must be considered as part of the record and be retained accordingly.
TELEPHONY SYSTEMS AND SERVICES	Telephony systems record*	1 year	Review and destroy if no longer required	This is the minimum specified to meet NHS contractual requirements.
BIRTHS, DEATHS AND ADOPTION RECORDS	Birth notification to child health	25 years	Review and destroy if no longer required	Retention begins when the notification is received by the child health department. Treat as part of the child's health record if not already stored within the health record.
BIRTHS, DEATHS AND ADOPTION RECORDS	Birth registers*	2 years	Review and consider transfer to PoD	Where registers of all births that have taken place in a particular hospital or birth centre exist, these will have archival value and should be retained for 25 years and offered to the local PoD at the end of the retention period. Information is also held by the NHS Birth Notification Service electronic system, and by ONS. Other information about a birth must be recorded in the care record.
BIRTHS, DEATHS AND ADOPTION RECORDS	Body release forms*	2 years	Review and destroy if no longer required	
BIRTHS, DEATHS AND ADOPTION RECORDS	Death – cause of death certificate counterfoil*	2 years	Review and destroy if no longer required	These detail the name of the deceased and suspected cause of death (which initially may be different to the final cause of death as stated on the official death certificate). A death notification certificate is issued if a doctor is satisfied there is no suspicious or unexpected circumstances surrounding the death, and the counterfoil retained by the setting that issued the initial cause of death certificate (which is used to obtain

				the full death certificate from a registrar of births, death and marriages). Cases referred to the coroner would not be able to issue a certificate as the cause would be unknown. These are unlikely to have archival value.
BIRTHS, DEATHS AND ADOPTION RECORDS	Death - register information sent to the general registry office on a monthly basis*	2 years	Review and consider transfer to PoD	A full dataset is available from ONS.
BIRTHS, DEATHS AND ADOPTION RECORDS	Local authority adoption record (usually held by the LA)*	100 years	Review and consider transfer to PoD	The local authority Children's Social Care Team hold the primary record of the adoption process. Consider transferring to PoD only if there are known gaps in the primary local authority record, or the records pre- date 1976. Also refer to Appendix III: adoption records
BIRTHS, DEATHS AND ADOPTION RECORDS	Mortuary records of deceased persons	10 years	Review and consider transfer to PoD	Retention begins at the end of the year to which they relate.
BIRTHS, DEATHS AND ADOPTION RECORDS	Mortuary register*	10 years	Review and consider transfer to PoD	
BIRTHS, DEATHS AND ADOPTION RECORDS	NHS medicals for adoption records*	8 years or 25th birthday	Review and consider transfer to PoD	The health reports will feed into the primary record held by the local authority. This means that adoption records held in the NHS relate to reports that are already kept in another file, which is kept for 100 years by the relevant agency or local authority. Consider transferring to PoD only if there are known gaps in the primary local authority record or the records pre-date 1976. Also refer to Appendix III: adopted persons health records

BIRTHS, DEATHS AND ADOPTION RECORDS	Post-mortem records*	10 years	Review and destroy if no longer required	The coroner will maintain and retain the primary post-mortem file including the report. Hospital post-mortem records will not need to be kept for the same extended time period as (subject to local policy) these reports may also be kept in the medical file.
CLINICAL TRIALS AND RESEARCH	Advanced medical therapy research - master file	20 years	Review and consider transfer to PoD	
CLINICAL TRIALS AND RESEARCH	Clinical trials – applications for ethical approval	5 years	Review and consider transfer to PoD	Master file of a trial authorised under the European portal, under Regulation 536/2014. For clinical trials records retention refer to the MHRA guidance. The sponsor of the study will be the primary holder of the study file and associated data. This is based on the Medicines for Human Use (Clinical Trials) Amendment Regulations 2006 (specifically Regulations 18 and 28).
CLINICAL TRIALS AND RESEARCH	European Commission Authorisation (certificate or letter) to enable marketing and sale within EU member state's area	15 years	Review and consider transfer to PoD	
CLINICAL TRIALS AND RESEARCH	Research - datasets	No longer than 20 years	Review and consider transfer to PoD	

CLINICAL TRIALS AND RESEARCH	Research – ethics committee's and HRA approval documentation for research proposal and records to process patient information without consent	5 years	Review and consider transfer to PoD	This applies to trials where opinions are given to proceed with the trial, or not to proceed. These may also have archival value.
CLINICAL TRIALS AND RESEARCH	Research – ethics committee's minutes (including records to process patient information without consent)	20 years	Review and consider transfer to PoD	Retention period begins from the year to which they relate and can be as long as 20 years. Committee minutes must be transferred to PoD.
CORPORATE GOVERNANCE	Board meetings*	Up to 20 years	Review and transfer to PoD	A local decision can be made on how long to retain the minutes of board meetings (and associated papers linked to the board meeting), but this must not exceed 20 years, and will be required to be transferred to the local PoD or The National Archives (for National Bodies).
CORPORATE GOVERNANCE	Board meetings (closed boards)*	Up to 20 years	Review and transfer to PoD	Although these may still contain confidential or sensitive material, they are still a public record and must be transferred at 20 years, and any FOI exemptions noted, or indications that the duty of confidentiality applies.
CORPORATE GOVERNANCE	Chief Executive records*	Up to 20 years	Review and transfer to PoD	This may include emails and correspondence where they are not already included in board papers.
CORPORATE GOVERNANCE	Committees (major) – listed in Scheme of delegation or report direct into the board (including major projects)*	Up to 20 years	Review and transfer to PoD	

CORPORATE GOVERNANCE	Committees (minor) – not listed in scheme of delegation*	6 years	Review and consider transfer to PoD	Includes minor meetings, projects, and departmental business meetings. These may have local historical value and require transfer consideration.
CORPORATE GOVERNANCE	Corporate records of health and care organisations and providers that pre- date the NHS (July 1948)		Review, and transfer to PoD	Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed. An example might be the minutes of the hospital board from 1932, or midwifery diaries dated Dec 1922.
CORPORATE GOVERNANCE	Data Protection Impact Assessments (DPIAs)	6 years	Review and destroy if no longer required	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one -off, then 6 years from completion.
CORPORATE GOVERNANCE	Destruction certificates or record of	20 years	Review and dispose of if no longer required	Where a record is listed for potential transfer to PoD have been destroyed without adequate appraisal, consideration should be given to a selection of these as an indicator of what has not been preserved.
CORPORATE GOVERNANCE	information held on destroyed physical media			
CORPORATE GOVERNANCE	Electronic metadata destruction stubs			Refer to destruction certificates.

CORPORATE GOVERNANCE	Incidents – serious	20 years	Review and consider transfer to PoD	Retention begins from the date of the Incident – not when the incident was reported.
CORPORATE GOVERNANCE	Incidents – not serious	10 years	Review and destroy if no longer required	Retention begins from the date of the incident – not when the incident was reported.
CORPORATE GOVERNANCE	Incidents – serious incidents requiring investigation	20 years	Review and consider transfer to PoD	These include independent investigations into incidents. These may have permanent retention value so consult with the local PoD. If they are not required, then destroy.
CORPORATE GOVERNANCE	Non-clinical QA records	12 years	Review and destroy if no longer required	Retention begins from the end of the year to which the assurance relates.
CORPORATE GOVERNANCE	Patient advice and liaison service (PALS) records	10 years	Review and destroy if no longer required	Retention begins from the close of the financial year to which the record relates.
CORPORATE GOVERNANCE	Patient surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	May be required again if analysis is reviewed.

CORPORATE GOVERNANCE	Patient surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.
CORPORATE GOVERNANCE	Policies, strategies and operating procedures – including business plans*	Life of organisation plus 6 years	Review and consider transfer to PoD	Retention begins from when the document is approved, until superseded. If the retention period reaches 20 years from the date of approval, then consider transfer to PoD.
CORPORATE GOVERNANCE	Quarterly reviews from NHS trusts	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.
CORPORATE GOVERNANCE	Risk registers	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act and corporate awareness of risks.
CORPORATE GOVERNANCE	Staff surveys – individual returns and analysis	1 year after return	Review and destroy if no longer required	Forms are anonymous so do not contain PID unless provided in free text boxes. May be required again if analysis is reviewed.
CORPORATE GOVERNANCE	Staff surveys – final report	10 years	Review and consider transfer to PoD	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.

CORPORATE GOVERNANCE	Trust submission forms	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act 1980.
COMMUNICATIONS	Intranet site*	6 years	Review and consider transfer to PoD	
COMMUNICATIONS	Patient information leaflets	6 years	Review and consider transfer to PoD	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.
COMMUNICATIONS	Press releases and important internal communications	6 years	Review and consider transfer to PoD	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.
COMMUNICATIONS	Public consultations	5 years	Review and consider transfer to PoD	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation (particularly where this resulted in changes to the services provided) and so may have historical value.
COMMUNICATIONS	Website*	6 years	Review and consider transfer to PoD	The PoD may be able to receive these by a regular crawl. Consult with the PoD on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken.

STAFF RECORDS AND OCCUPATIONAL HEALTH	Duty roster	6 years	Review and if no longer needed destroy	Retention begins from the close of the financial year.
STAFF RECORDS AND OCCUPATIONAL HEALTH	Exposure monitoring information	40 years or	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.
STAFF RECORDS AND OCCUPATIONAL HEALTH		5 years from the date of the last entry made in it		
STAFF RECORDS AND OCCUPATIONAL HEALTH	Occupational health reports	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	
STAFF RECORDS AND OCCUPATIONAL HEALTH	Occupational health report of staff member under health surveillance	Keep until 75th birthday	Review and if no longer needed destroy	
STAFF RECORDS AND OCCUPATIONAL HEALTH	Occupational health report of staff member under health surveillance where they have been subject to radiation doses	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	

STAFF RECORDS AND OCCUPATIONAL HEALTH	Staff record	Keep until 75th birthday (see notes)	Review, and consider transfer to PoD	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. Some PoDs accession NHS staff records for social history purposes. Check with your local PoD about possible accession. If the PoD does not accession them, then the records can be securely destroyed once the retention period has been reached.
STAFF RECORDS AND OCCUPATIONAL HEALTH	Staff record - summary	75th Birthday	Review, and consider transfer to PoD	Please see the good practice box staff record summary used by an organisation. Some organisations create summaries after a period of time since the staff member left (usually 6 years). This practice is ok to continue if this is what currently occurs. The summary, however, needs to be kept until the staff member's 75th birthday, and then consider transferring to PoD. If the PoD does not require them, then they can be securely destroyed at this point.
STAFF RECORDS AND OCCUPATIONAL HEALTH	Timesheets (original record)	2 years	Review and if no longer needed destroy	Retention begins from creation.
STAFF RECORDS AND OCCUPATIONAL HEALTH	Staff training records	See notes	Review and consider transfer to a PoD	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The following is recommended: **clinical training records** to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer **statutory and mandatory training records** - to be kept for ten years after training completed **other training records - keep for six years after training completed**

STAFF RECORDS AND OCCUPATIONAL HEALTH	Disciplinary records	Retain for 6 years	Review and destroy if no longer required	Retention begins once the case is heard and any appeal process completed. The record may be retained for longer, but this will be a local decision based on the facts of the case. The more serious the case, the more likely it will attract a longer retention period. Likewise, a one-off incident may need to only be kept for the minimum time stated. This applies to all cases, regardless of format.
PROCUREMENT	Contracts sealed or unsealed	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
PROCUREMENT	Contracts - financial approval files	Retain for 15 years after the end of the contract	Review and if no longer needed destroy	
PROCUREMENT	Contracts - financial approved suppliers documentation	Retain for 11 years after the end of the contract	Review and if no longer needed destroy	
PROCUREMENT	Tenders (successful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	
PROCUREMENT	Tenders (unsuccessful)	Retain for 6 years after the end of the contract	Review and if no longer needed destroy	

ESTATES	Building plans, including records of major building works	Lifetime (or disposal) of building plus 6 years	Review and consider transfer to PoD	Building plans and records of works are potentially of historical interest and where possible, should be kept and transferred to the local PoD.
ESTATES	Closed circuit television (CCTV)	Refer to ICO Code of Practice	Review and destroy if no longer required	The length of retention must be determined by the purpose for which the CCTV has been used. CCTV footage must remain viewable for the length of time it is retained, and where possible, systems should have redaction or censoring functionality to be able to blank out the faces of people who are captured by the CCTV, but not subject to the access request, for example, police reviewing CCTV as part of an investigation.
ESTATES	Equipment monitoring, and testing and maintenance work where ASBESTOS is a factor	40 years	Review and destroy if no longer required	Retention begins from the completion of the monitoring or testing. This includes records of air monitoring and health records relating to asbestos exposure, as required by the Control of Asbestos Regulations 2012.
ESTATES	Equipment monitoring – general testing and maintenance work	Lifetime of installation	Review and destroy if no longer required	Retention begins from the completion of the testing and maintenance.
ESTATES	Inspection reports	Lifetime of installation	Review and dispose of if no longer required	Retention begins at the END of the installation period. Building inspection records need to comply with the Construction (Design and Management) Regulations 2015.

ESTATES	Leases	12 years	Review and destroy if no longer required	Retention begins at point of lease termination.
ESTATES	Minor building works	6 years	Review and destroy if no longer required	Retention begins at the point of WORKS COMPLETION.
ESTATES	Photographic collections – service locations, events and activities	Up to 20 years	Review and consider transfer to PoD	These provide a visual historical legacy of the running and operation of an organisation. They may also provide secondary uses, such as use in public inquiries.
ESTATES	Radioactive records	30 years	Review and destroy if no longer required	Retention begins at the CREATION of the waste. If a person handling radioactive waste is exposed to radiation (accidental or otherwise), then the records relating to that person must be kept until they reach 75 years of age or would have attained that age. In any event, records must be kept for at least 30 years from the date of dosing or accident. This also includes patients or service users who require medical exposure to radiation, as required by the Ionising Radiation Regulations 2017.
ESTATES	Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhyndrin Test	11 years	Review and destroy if no longer required	Retention begins from the DATE OF TEST.

ESTATES	Surveys – building or installation (not patient surveys)	Lifetime of installation or building	Review and consider transfer to PoD	Retention period begins at the END of INSTALLATION period. (See Inspection reports for legal basis for these records)
FINANCE	Accounts	3 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate. Includes all associated documentation and records for the purpose of audit.
FINANCE	Benefactions	8 years	Review and consider transfer to PoD	These may already be in the financial accounts and may be captured in other reports, records or committee papers. Benefactions, endowments, trust fund or legacies should be offered to the local PoD.
FINANCE	Debtors' records – CLEARED	2 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
FINANCE	Debtors' records – NOT CLEARED	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
FINANCE	Donations	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.

FINANCE	Expenses	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
FINANCE	Final annual accounts report*	Up to 20 years	Review and transfer to PoD	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with board papers for that year to keep a complete set of governance papers.
FINANCE	Financial transaction records	6 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
FINANCE	Invoices	6 years from end of the financial year they relate to	Review and destroy if no longer required	
FINANCE	Petty cash	2 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
FINANCE	Private Finance Initiatives (PFI) files	Lifetime of PFI	Review and consider transfer to PoD	Retention begins at the END of the PFI agreement. This applies to the key papers only in the PFI.

FINANCE	Staff salary information or files	10 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
FINANCE	Superannuation records	10 years	Review and destroy if no longer required	Retention begins at the CLOSE of the financial year to which they relate.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Complaints – case files	10 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the complaint. The complaint is not closed until all processes (including potential and actual litigation) have ended. The detailed complaint file must be kept separately from the patient file (if the complaint is raised by a patient or in relation to). Complaints files must always be separate. (Also refer to Appendix III: complaints records)
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Fraud – case files	6 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the case. This also includes cases that are both proven and unproven.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Freedom of Information (FOI) requests, responses to the request and associated correspondence	3 years	Review and destroy if no longer required	Retention begins from the CLOSURE of the FOI request. Where redactions have been made, it is important to keep a copy of the response and send to the requestor. In all cases, a log must be kept of requests and the response sent.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	FOI requests – where there has been an appeal	6 years	Review and destroy if no longer required	Retention begins from the CLOSURE of the appeal process.

LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Industrial relations – including tribunal case records	10 years	Review and consider transfer to PoD	Retention begins at the CLOSE of the financial year to which it relates. Some organisations may record these as part of the staff record, but in most cases, they should form a distinctive separate record (like complaints files).
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Litigation records	10 years	Review and consider transfer to PoD	Retention begins at the CLOSURE of the case. Litigation cases of significant or major issues (or with significant, major outcomes) should be considered for transfer. Minor cases should not be considered for transfer. If in doubt, consult with the PoD.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Intel patents, trademarks, copyright, IP	Lifetime of patent, or 6 years from end of licence or action	Review and consider transfer to PoD	Retention begins at the END of lifetime or patent, or TERMINATION of licence or action.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Software licences	Lifetime of software	Review and destroy if no longer required	Retention begins at the END of lifetime of software.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	Subject Access Requests (SAR), response, and subsequent correspondence	3 years	Review and destroy if no longer required	Retention begins at the CLOSURE of the SAR.
LEGAL, COMPLAINTS AND INFORMATION RIGHTS	SAR – where there has been an appeal	6 years	Review and destroy if no longer required	Retention begins at CLOSURE of appeal.

Appendix – Part 3: How to deal with specific types of

This Appendix provides detailed advice on records management relating to specific types of records for example, transgender records, witness protection records and adopted persons records. These are presented in alphabetical order. It also provides advice on managing certain formats of records, for example, emails, cloud-based records and scanned records.

TYPE OF RECORD

Adopted persons health records

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

Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure.

It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it were considered appropriate to do so following the adoption.

Ambulance service records

Ambulance service records will contain evidence of clinical interventions delivered and are therefore clinical records. This means that they must be retained for the same time as other acute or mental health clinical records depending on where the person is taken to for treatment. Where ambulance service records are not clinical in nature, they must be kept as administrative records. There is a distinction between records of patient transport and records of clinical intervention. If the ambulance clinical record is handed over to another service or NHS trust, there must be a means by which the ambulance trust can obtain them again if necessary. Alternatively, they can be copied and only the copy transferred, providing this is legible.

Asylum seeker records

Records for asylum seekers must be treated in exactly the same way as other care records, allowing for clinical continuity and evidence of professional conduct.
Organisations may decide to give asylum seekers patient or service user held records (section below) or hold them themselves. Patient or service user held records should be subject to a risk assessment because the record legally belongs to the organisation, and if required, they must be able to get it back. There is a risk that patient or service user held records could be tampered with or altered in an unauthorised way so careful consideration needs to be given to this decision.

Audio and visual records

Audio and visual records can take many forms such as using a dictaphone (digital or analogue) to record a session or conducting a health or care interaction using videoconferencing technologies.

The following needs considering when patient or service user interactions are captured in this way:

- **Clinical appropriateness:** Organisations should decide when it is appropriate to use audio or visual methods for the provision of health or care. This should be documented in organisational policies and understood by the relevant health and care professionals.

- **Retention:** If the recording is going to be kept elsewhere (for example, as part of the health and care record) then there is no reason to keep the original recording provided the version in the main record is the same
as the original or there is a summary into words which is accurate and adequate for its purpose. If the recording is the only version or instance of the interaction, then it must be kept for the relevant retention period outlined in this Code (for example, adult, child health or mental health

retention periods). Some recordings may have archival value (although this is unlikely), and this should be considered on a case-by-case basis.

- **Digital continuity:** You must consider the medium on which the recording is made and ensure that it is available throughout its retention period (for example, if the system or file format is becoming obsolete, then you will need to migrate it to a newer platform or format to ensure availability).
  If it is a digital recording and you are looking to store it in the health and care record, ensure the transfer process captures the authenticity of the recording kept.

- **Storage:** Ensure your recordings are stored on systems you control or are provided to you under contract. If stored with the product provider, you must give them (as controller) clear instructions on the storage and retention of those images (for example, delete one month after the date
  of the recording because it has been summarised into the main health and care record, or retain for 8 years from consultation with the patient or service user, then destroy). Providers acting under contract to a controller are obliged to carry out their written instruction.

- **Transparency:** You must be transparent with patients and service users regarding the use of audio and visual technology, and associated records, so that they have a reasonable understanding of how they will be used, why, and what will happen with the recording after the interaction. For example, it would be unfair to tell participants that the recordings are deleted if they are not.

Child school health records

Similar to family records (refer to page 94), each child should have their own school health record rather than a record for the school (with consecutive entries) or per year intake. If a child transfers to a school under a different local authority, then the record will also need to be transferred to the new school health service provider. This must only be done once it is confirmed the child is now resident in the new location. The record must be transferred securely. The recipient of the record should contact the sender to confirm receiving the record (if appropriate). If the records are kept on school premises, then access must be restricted to health staff delivering care or other staff who have a legitimate reason to access them.

Local organisations may operate a paper or digital system. Records from other Child Health Teams, following a referral, must be accepted by the receiving organisation regardless of format. This is due to safeguarding risks.

Complaints records

Where a patient or service user complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Detailed complaint information should never be recorded in the health and care record. A complaint may be unfounded or involve third parties and the inclusion of that information in the health or care record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient or service user and the Health and Care Team. In some cases, it may be appropriate to share details of the complaint with the health and care professional involved in providing individual care in order to make improvements in care delivery. However, there may also be times where the complaint is about an individual but not care related and it might not be appropriate to share details of the complaint with that person, in case further action is required. The Complaints Team should review each complaint on a case- by-case basis.

Where multiple teams are involved in the complaint handling, all the associated records must be brought together to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. A complaint cannot be fully investigated if the investigation is based on incomplete information. It is common for the patient or service user to ask to see a copy of their complaint file and it will be easier to deal with if all the relevant material is in one file. Where complaints are referred to the Ombudsman Service, a single file will be easier to refer to.

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

Contract change records

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

In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision (for

current cases) upon termination of the contract. It is also the case that after the contract period has ended, the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

When a service is taken over by a new provider, the records of the service (current and discharged cases) all transfer to the new provider (unless directed otherwise by the commissioner of the service). This is to ensure that the records for the service remain complete and enable patients or service users to obtain their record if they so request it. It also makes the records easier to locate if they are required for other purposes. This will also stop the fragmentation of the archive records for the service and make it much easier to retrieve records.

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

In some cases, records may end up orphaned. This may happen where the organisation that created them is being disbanded and there is no successor organisation to take over the service or provision. In these cases, orphaned records need to be retained by the highest level commissioner of that service or provision. For example, if a GP practice closes, patients will be offered the choice to register with another nearby practice. When they register with the new practice, the record will follow the patient to that new practice. However, if a practice closes, and the patient does not re-register elsewhere, the record will transfer to NHS England and Improvement, who commission primary care services in England for ongoing management.

Where the content of records is confidential, for example, health and care records, it will be necessary to inform the individuals concerned about the change. Where there is little impact upon those receiving care, it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes will require individual communications. Although the conditions of UK GDPR may be satisfied, in many cases there is still a duty of confidentiality which may require a patient or service user (in some cases) to agree to the transfer, dependent upon the legal basis and the implications of their choice discussed with them. If the new provider has a statutory duty to provide the service, then consent does not need to be sought. If there is no
statutory duty, then consent would need to be sought to satisfy the common law duty of confidentiality.

It is vital to highlight the importance of actively managing records, which are stored in offsite storage (refer to section three of the Code for further
information on offsite storage including the importance of completing a DPIA).

These principles and guidance can also apply to non-clinical situations as well, such as when CCGs merge or a trust takes over the running of another one.

Annex 1 of this Appendix summarises the considerations and actions required relating to various contract change situations.

Duplicate records

The person or team to which the record relates will normally hold the original record however occasionally duplicates may be created for legitimate business purposes. It is not necessary to keep duplicates of the same record unless it is used in another process and is then a part of a new record. Where this is not required, the original should be kept, and the duplicate destroyed. For example, incident forms, once the data is entered into the risk information system, the paper is now a duplicate, and so can be destroyed. Some clinical systems allow printouts of digital records. Where printouts are used, these must be marked as duplicates or copies to help prevent them from being used as the primary record.

Evidence required for courts

In UK Law, the civil procedure rules allow evidence to be prepared for court and, as part of this, the parties in litigation can agree what documents they will disclose to the other party and, if required, dispute authenticity. The disclosure of digital records is referred to as E-Disclosure or E-Discovery. The relevant part for disclosure and admissibility of evidence is given in the Ministry of Justice's Civil Procedure Rules - Part 3. If records are arranged in an organised filing system, such as a business classification scheme, or all the relevant information is placed on the patient or client file, providing records as evidence will be much easier. Further advice on electronic records and evidential weighting
can be found in BIP10008: Evidential Weight and Admissibility of Electronic Information.

Family records

Family records used to be common within health visiting teams, amongst others, where a whole family view was needed to deliver care. Whilst these records should no longer be created, they are included here for legacy reasons.

Due to changes in the law and best practice, it is not advisable to create a single paper or digital record that contains the care given to all family members. Each person is entitled to privacy and confidentiality, and having all a person's

records in one place could result in a health professional or family member accessing confidential information of another family member accidentally or otherwise.

Good practice would be to create an individual file for each person but with cross references to other family members. This means that each individual has their own record, but health and care professionals can see who else is related to that
person, and so can check these records where necessary. Single records also help to protect privacy and confidentiality and (if digital) keep an audit trail of access.

General Practitioner records

It is important to note that the General Practitioner (GP) record, usually held by the General Practice, is the primary record of care and the majority of other services must inform the GP through a discharge note or a clinical
correspondence that the patient has received care. This record is to be retained for the life of the patient plus at least ten years after death. The GP record transfers with the individual as they change GP throughout their lifetime. Where the patient has de-registered, records should be kept for 100 years since de- registration. A review is taking place to ascertain how long this period should be in the going forwards.

Current guidance advises that the content of paper Lloyd George records should only be destroyed once they have been scanned to the required standard and quality assurance of the scanned images has been completed, confirming that they are a like for like copy of the original paper records. The Lloyd George envelope itself should not be destroyed at the current time and must be kept
to meet with the requirements for patient record movement. NHS England undertook a project to cease the creation of Lloyd George envelopes for all new entrants to the NHS, which was implemented in January 2021 (except in limited circumstances). They are also looking at ways to enable destruction of existing Lloyd George envelopes, though this aspect may have a longer implementation timeframe. This Code will be updated as the programme develops.

Individual funding requests (IFRs)

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

As IFRs are unique to an individual, it may be that the care package given to the patient or service user is unique and bespoke to that person. This could mean that the record may have long-term archival value, due to

the uniqueness of the care given in this way, and so potentially may be of interest to The National Archives. Local discussions should be held with the PoD to determine the level of local interest, although they would not normally get involved at this level
of discussion. It would be a joint discussion on the principle and agreement to archive this type of record and then the responsibility of the health and care organisation to choose individual records that meet this criteria.

Continuing healthcare (CHC) records

Continuing healthcare records can be split into two parts:

- **Care record:** The care record is the information relating to a patient or service user's care that enables the CHC panel to determine eligibility for CHC based on an assessment of needs. This can be provided directly by the patient or service user or obtained from health and care providers as
part of the eligibility process. Consent to obtain this information would be required to satisfy the duty of confidence. The initial checklist completed by the referrer may also contain some level of confidential information and this may also be used to determine eligibility.

- **Administrative record:** The administrative record is the information used by the CCG to ensure the CHC process runs effectively - an example being appointment letters asking the patient or service user to attend a panel. CCGs require access to health and care information to determine a patient or service user's entitlement (once the CCG has been notified).

CHC activity is covered in law by the 2012 Commissioning Board and NHS CCG Regulations. This means consent is not required to process personal data in relation to CHC but consent will be required to satisfy the duty of confidence. CCGs will need to have systems in place to allow for the safe and secure sharing of patient or service user information with relevant partners as necessary, and to inform patient or service users of how their data will be used as part of this process. Digital viewing and sharing of records may be preferable to paper copies being printed and used for CHC, due to the risk of accidental loss or disclosure.

CHC records should be kept for the same period of time as adult and child health records, from the date the case is decided by the CHC panel. Where CHC cases relate to mental health, these should be kept for the same period of time as mental health records.

Controlled drugs regime

NHS 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.

Integrated records

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

- NHS England Vanguard Programme
- Sustainability and Transformation Plans (STPs)
- Integrated Care Services (ICS)
- Local Health and Care Records (LHCR)

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

The options for organisations will depend on what local architecture and systems are already in use. There are three types of retention for integrated records, and suggested retention periods for each.

1. All organisations contribute to a single record, creating the only record for that patient or service user. Consideration must be given to how this is
   managed in practice (for example, some records will be retained for 8 years and some for 20 years but they will look the same at face value) (**retain for the longest specialty period involved**).

2. All organisations pool their records into a single place but keep a level of separation between each type of record (**retain for each specialty as applicable – because they are not merged**)

3. All organisations keep their own records, but allow others to view their records, but not amend or add to (**retain for each specialty as applicable – because they are not merged**)

Where organisations are looking to create integrated records, they must enter into a joint controller arrangement, which detail the purpose and method of integrated records. It should also set out how disputes between controllers may be resolved. Information materials for patient or service users must also reflect how their records are used.

Increasingly, where organisations are using this type of system, the information contained within has the potential to be used for purposes other than individual care, such as Population Health Management (PHM). PHM is a tool that is increasingly being used to help plan and prepare care provision in a particular geographical area or specialty. See also the section on Integrated viewing technology and record keeping in the format section below.

NHSX has published an Information Governance Framework for Shared Care Records, which provides further guidance.

Occupational health (OH) records

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. It is permitted for reports or summaries to be held in the main staff record where these have been requested by the employer and agreed by the staff member. When occupational health records are outsourced, the organisation must ensure that:

- staff are aware of the outsourcing and how their information may be used for OH purposes
- the contractor can comply as necessary with data protection and confidentiality requirements
- there is a contract in place with the outsourced provider that has legally binding clauses in relation to data protection and confidentiality
- the contractor can retain records for the necessary period after the termination of contract for purposes of adequately recording any work- based health issues and is able to present them to the organisation if required

Pandemic records

Health and care organisations will create records as part of a response to a global pandemic. Pandemic events are rare but will nevertheless create records that need to be managed.

Both patient and service user records will be created that detail the care given to people affected by the pandemic. Corporate records will also be created which record business decisions, policies and processes that were taken in response to a pandemic.

These records should be managed in accordance with the retention schedules set out in this Code. Organisations should be mindful that a public inquiry (or
inquiries) is likely to take place after a pandemic so the pandemic related records could be used or requested as part of that Inquiry. The Government has already agreed to hold a public inquiry into the coronavirus pandemic that began in 2020.

If organisations have created records specifically in response to a pandemic, these should not be destroyed when they have reached their minimum retention period, unless the public inquiry has ended, or the Inquiry has provided guidance on what type of records it will be interested in. These specific records may have historical value, so discussions should take place with your local PoD. A policy
on how to manage a new admission to a care home of an individual with a coronavirus diagnosis may be of interest to the PoD, whereas the care record might not have the same value and should be managed as a health and care record. Any guidance or advice issued by The National Archives or your local PoD in relation to the preservation of pandemic records should be followed.

Patient or service user held records

Some clinical or care services may benefit from the patient or service user holding their own record, for example, maternity services. Where this is considered to be the case a risk assessment should be carried out by the organisation. Where it is decided to leave records with the individual who is the subject of care, it must be indicated on the records that they remain the
property of the issuing organisation and include a return address if they are lost. Upon the discharge of the patient or service user, the record must be returned to the health or care organisation involved in the person's care.

Organisations must be able to produce a record of their work, which includes services delivered in the home where the individual holds the record. Upon the termination of treatment, where the records are the sole evidence of the course of treatment or care, they must be recovered and given back to the issuing organisation.

A copy can be provided if the individual wishes to retain a copy of the records through the SAR process. In cases where the individual retains the actual record after care, the organisation must be satisfied it has a record of the contents.

Patient or service user portals

Organisations may implement products that provide patients and service users with access to their records. Access may be either online or via an app or portal. There are increasing numbers of commercial organisations that are providing these products.

The provision of these products must comply with data protection legislation. Health and care organisations must conduct a DPIA if they are considering using such a product. Health and care organisations must remain controller for the patient or service user's information. In most cases, the supplier of the product or system will be a processor as the product facilitates access to the information held by health and care organisations.

Controllers must consider what is relevant and proportionate to include in this type of record. Some information may not be appropriate to add to the portal, for example, harmful information a patient does not know yet because the intention is to let them know in person during a consultation.

Information about the patient or service user must not be uploaded into the product until there is a clear legal basis for doing so, for example, patient consent. Individuals must be provided with information materials so that they can make an informed choice as to whether or not to sign up. The materials should also make it clear what information patients and service users can upload themselves directly to the portal if this is an option. It should also be clear to the patient or service user who controls the information.

Information stored in a product like this should be retained in line with the retention schedules outlined in this Code (for example, adult health records for 8 years after last seen).

Pharmacy held patient records

These are the records of patients that the pharmacy has dispensed medications to or had some other form of clinical interaction with (for example, given a flu jab) - similar to a hospital or care home patient record.

Records of prescriptions dispensed will be kept by NHS BSA so there is no need to keep a copy of the prescription locally except for audit purposes.

Other elements of the pharmacy record, for example, vaccinations provided, should be viewed in the same way as a patient record, and should be destroyed 8 years after the last interaction with the patient. However, if there is a need to keep the record for longer, then this can be extended up to 20 years, provided there is a justified, documented and approved reasons for doing so. Information materials for patients should also be reflective of the organisation's retention period.

Prison health records

In 2013 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.

A significant number of paper records remain, and some offender health services operate a mix of paper and digital records. Prison records should be treated as hospital episodes and may be disposed of after the appropriate retention has been applied. The assumption is that a discharge note has been sent to the GP.

Where a patient or service user is sent to prison the GP record (or social care record) must not be destroyed but held until the patient is released or normal retention periods of records have been met.

Prison health records may have archival value, but this is the exception rather than rule. Records should be kept in line with the same period as for de- registered GP records, with a view to further retention (with justification) and a potential transfer to a PoD, subject to their approval.

Private patients treated on NHS 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.

Public health records

A local authority normally hosts public health functions, but the functions still involve the handling of health and care information. For this reason, public health functions are in the scope of this Code. Where clinical information is being processed by the public health function it is expected to comply with the NHS Digital Code of Practice for Confidential Information.

Records relating to sexually transmitted diseases

Organisations that provide care and support under the NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000 must be aware of the additional obligations to confidentiality these impose on employees and trustees of organisations. These organisations include NHS Trusts, CCGs, local authority public health teams and those providing services under NHS contracts.

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

Secure units for patients detained under the Mental Health Act 1983

Mental health units operate on a low, medium and high-risk category basis. Not all patients on these units will have been referred via the criminal justice system.
Some patients may be deemed a risk under the Mental Health Act and will need to be accommodated accordingly. Some patients may be high-risk due to the nature of a crime they have committed because of their mental health and therefore will need to be treated in a high secure hospital, such as Broadmoor. As such, their records should be treated in the same way as other mental health records including retention periods (20 years, and longer if justified and permitted) and final disposal. A long retention time may also help staff at these units deal with subsequent long-term enquiries from care providers.

Sexual assault referral centres

Sexual assault referral centres (SARCs) are highly specialised forensic and health services co-commissioned by Police and Crime Commissioners and NHS England and Improvement. SARCs support the physical, mental health and wellbeing of service users and collect forensic evidence pertaining to alleged sexual offences. Records generated may include forensic medical examination notes, body maps, photographic records, and DNA intelligence. Reports or statements on these records may be required as evidence in a court of law, and the records management process must facilitate this. Based on relevant guidance, legal and
regulatory obligations, a minimum retention period of 30 years for SARC records has been applied by NHS England and NHS Improvement. This retention period reflects the severity of the alleged offence; the length of time for the potential bringing of criminal justice proceedings and right to appeal; and the potential for cold case review. Retaining records beyond 30 years is acceptable provided there is ongoing justification and the decision is documented and approved by the relevant committees responsible for the SARCs operational delivery.

Specimens and samples

The retention of human material is covered by this Code because some specialities will include physical human material as part of the patient or service user record (or linked to it). The record may have to be retained longer than the sample because the sample may deteriorate over time. Relevant professional bodies such as the Human Tissue Authority or the Royal College of Pathologists have issued guidance on how long to keep human material. Physical specimens or samples are unlikely to have historical value, and so are highly unlikely to be selected for permanent preservation.

The human material may not be kept for long periods, but that does not mean that the information or metadata about the specimen or sample must be destroyed at the same time. The information about any process involving human material must be kept for continuity of care and legal obligations. The correct place to keep information about the patient is the clinical record and although the individual pathology departments may retain pathology reports, a copy must always be included on the patient record. Physical specimens or samples do not have to be stored within the clinical record (unless designed to do so) but can be stored where clinically appropriate to keep the material, with a clear reference or link in the clinical file, so both the material and the clinical record can be joined together if necessary.

Staff records

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

It is common practice in some health and care organisations for the line manager to hold a truncated record, which contains portions of an employee's employment history. This can introduce risk to personal information (as it is duplicated), but also potentially expedient to do so. Organisations considering whether to use, or discontinue using, local HR files, should complete a risk assessment.

Information kept in truncated staff files should be duplicates of the original held in the central HR file. If local managers are given originals as evidence (such as a staff member bringing in a certificate of competence) they should take a copy for local use and the original should be kept with the main HR file. It is important that there is a single, complete employment record held centrally for reference and probity.

Upon termination of contract (for whatever reason), records must be held up to and beyond the statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS or organisational business purposes, in accordance with Retention Instrument 122. Usually this relates to inpatient ward areas, where the ward manager will keep a small file relating to the training and clinical competencies of ward staff. Where there is justification for long retention periods or protection is provided by the Code, this will not be in breach of GDPR Principle 5. (Refer to section 5 of the Code for further information about retention of records).

Some organisations operate a weeding system, whereby staff files are culled of individual record types that are now time expired (such as timesheets). Others have just kept the whole file as is and archived it away until 75th birthday. It is not recommended to change your system from one to the other because:

- the effort involved would be disproportionate to the end result
- if you begin to weed files, you would need to do this retrospectively to all files, to avoid having two types of central HR file
- you cannot reverse the weeding process – if you decide to keep full records, it is impossible to remake historically weeded files complete again

Both systems are acceptable, regardless of media. It is noted that organisations may have a hybrid system of paper historical staff files and digital current staff files. If possible, organisations should consider moving all their files into one format to create consistency.

Where an organisation decides to use a summary, it must contain as a minimum:

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

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
- reasons for leaving
- building or sites worked at

Disciplinary case files should be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record, as it may be pertinent to have an indication to the disciplinary case, but the full details and file must be kept separately from the main file.

With regards to staff training records, it can be difficult to categorise them to determine retention requirements but keeping all the records for the same length of time is also hard to justify. It is recommended that:

- clinical training records are retained until 75th birthday or six years after the staff member leaves, whichever is the longer

- statutory and mandatory training records are kept for ten years after training is completed

- other training records are kept for six years after the training is completed

The Chartered Institute for Personnel and Development, and the ICO have provided further information and advice on the retention of HR records.

Transgender patient's records

Sometimes patients change their gender and part of this may include medical care. Records relating to these patients or service users are often seen as more sensitive than other types of medical records. While all health and care records are subject to confidentiality restrictions, there are specific controls for information relating to patients or service users with a Gender Recognition Certificate. The use and disclosure of the information contained in these records is subject to the Gender Recognition Act 2004, (GRA) which details specific restrictions and controls for these records. The GRA is clear that it is not an offence to disclose protected information relating to a person if that person has agreed to the disclosure. The GRA is designed to protect trans patient and service user data and should not be considered a barrier to maintaining historic medical records where this is consented to by the user.

There are established processes in place with NHS Digital for patients undergoing transgender care in relation to the NHS number and the closing and opening of new Spine records. In practice, nearly all actions relating to transgender records will be based on explicit consent. Discussions will take place between the GP and the patient regarding clinical care, what information in their current record can be moved to their new record and any implications this decision may have (for example, they may not be called for a gender specific screening programme). Patients should be offered ways to maintain their historical records. This could include editing previous entries and removing references containing previous names and gendered language. Any decisions made regarding their record must be respected and the records actioned accordingly.

Any patient or service user can request that their gender be changed in a record by a statutory declaration, but the Gender Recognition Act 2004 provides additional rights for those with a GRC. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Panel issues a Gender Reassignment Certificate. At this time a new NHS number can be issued, and a new record can be created, if it is the wish of the patient or service user. It is important to discuss with the patient or service user what records are moved into the new record and to discuss how to link any records held in any other health or care settings with the new record, including editing previous records to remove names, gender references or details. The content of the new record will be based on explicit consent under common law.

However, it is not essential for a transgender person to have a GRC in order to change their name and gender in their patient record and receive a new NHS number. They do not need to have been to a Gender Identity Clinic, taken any hormones, undergone any surgery, or have a Gender Recognition Certificate.

Under the Equality Act (2010), Transgender people share the protected characteristic of 'gender reassignment'. To be protected from gender reassignment discrimination, an individual does not need to have undergone any specific treatment or surgery to change from their birth sex to their preferred gender. This is because changing physiological or other gender attributes is a personal process rather than a medical one. An individual can be at any stage in the transition process – from proposing to reassign their gender, to undergoing a process to reassign their gender, or having completed it.

Protected persons health records

Where a record is that of someone known to be under a protected person scheme, the record must be subject to greater security and confidentiality. It may become apparent (via accidental disclosure) that the records are those of a person under the protection of the courts for the purposes of identity. The right to anonymity extends to health and care records. For people under certain types of protection, the individual will be given a new name and NHS Number, so the records may appear to be that of a different person.

Youth offending service records

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

Bring your own device (BYOD) created records

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

When an individual staff member no longer works for the employing organisation, any information that staff take away could be a risk to the organisation. If this includes personal data or confidential patient information, it is reportable to the ICO and may be a breach of confidentiality. For this reason, personal/confidential patient information should not be stored on the device unless absolutely necessary and appropriate security is in place. Local health and care organisations should have a policy on the use of BYOD by staff. Also refer to guidance on BYOD.

Cloud-based records

Use of cloud-based solutions for health and care is increasingly being considered and used as an alternative to manage large networks and infrastructure.
NHS and care services have been given approval to use cloud-based solution, provided they follow published guidance from NHS Digital and information on GOV.UK.

Before any cloud-based solution is implemented there are a number of records considerations that must be addressed as set out by The National Archives. The ICO has issued guidance on cloud storage. Organisations must complete a DPIA when considering using cloud solutions.

Another important consideration is that at some point the service provider or solution will change and it will be necessary to migrate all of the records,
including all the formats, onto another solution. Whilst this may be technically challenging, it must be done, and contract provisions should be in place to do this.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever-increasing storage instead of good records management will not meet the records management recommendations of this Code. For example, if digital health and care records are uploaded to cloud storage for the duration of their retention

period, then they must contain enough metadata to be able to be retrieved and a retention date applied so it can be reviewed and actioned in good time.

Personal data that is stored in the cloud, and then left, risks breaching UK GDPR by being kept longer than necessary. This information would also be subject to Subject Access process, and if not found or left unfound, would be a breach of the patient or service user's rights

Email and record keeping implications

Email is widely accepted as the primary communication tool used every day by all levels of staff in organisations. They often contain business (or in some cases clinical) information that is not captured elsewhere and so need to be
managed just like other records. The National Archives has produced guidance on managing emails.

Email has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record. However, a common problem with email is that it is rarely saved in the business context.

The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Solutions such as email archiving and ever-larger mailbox quotas do not encourage staff to meet the standard of storing email in the correct business context and to declare the email as a record.

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

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

- undertake periodic audits of working practice to identify poor practice
- have a policy in place that covers email management - including the appraisal, archiving and disposal of

emails

- take remedial action where poor practice or compliance is found

Automatic deletion of email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information, even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation. Legal holds can take many forms and records cannot be destroyed if there is a known process or a reasonable expectation that records will be needed for a future legal process such as:

- local inquiries into health or care issues
- national inquiries
- public inquiries
- criminal or civil investigations
- cases where litigation may be reasonably expected, for example, a patient has indicated they will take the organisation to court
- a SAR (known or reasonably expected)
- a FOI request (submitted or reasonably expected)

This means that no record can be destroyed by a purely automated process without some form of review whether at aggregated or individual level for continued retention or transfer to a PoD.

The NHSmail 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 to another NHS organisation, they must ensure that no sensitive data relating to the former organisation is transferred. It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of classified information. This is facilitated by staff storing only emails that need to be retained on an ongoing basis.

Emails that are the sole record of an event or issue, for example, an exchange between a clinician and a patient, should be copied into the relevant health and care record rather than being kept on the email system or deleted.

Instant messaging records

Health and care services are increasingly using instant messaging apps or platforms to share patient and service user information between health and care professionals or to contact patients or services users in a transactional way, such as appointment reminders. NHSX has published guidance on this issue.

Instant messaging apps or platforms should not be used as the main, or primary, record for a person. Where possible, information shared in this way also needs to have a place in the health or care record of that person. This could be a printout of the exchange; contents transcribed into the record; or a progress note accurately covering the exchange entered into the record. If the app or platform is the only place that information is stored, then it must be managed in line with this Code.

Transactional messages, such as GP appointment reminders or pharmacy notifications that your prescription is ready for collection, have a short shelf-life and will no longer be needed once the appointment is attended or prescriptions collected. Organisations that use these systems should keep a record of messages sent to a person, in case they are needed later (such as proof that the patient was reminded of their appointment), but once it is clear that the purpose of the message has been fulfilled, there is no requirement to keep these messages.

Integrated viewing technology and record keeping

Many record keeping systems pool records to create a view or portal of information, which can then be used to inform decisions. This in effect creates a single digital instance of a record, which is only correct at the time of viewing. This may lead to legacy issues, especially in determining the authenticity of a record at any given point in the past. When deciding to use systems that pool records from different sources, organisations must be assured that the system can recreate a record at a given point in time, and not just be able to provide a view at the time of access. This will enable a health or care provider to show what information was available at the time a decision was made.

Consideration should also be given to the authenticity and veracity of the record, particularly if there is conflicting information presented by two or more contributors to the record. Some conflicts may be easier to resolve than others (for example, a person has a different address with two systems), however more complex conflicts would require organisations to have a process or procedure to agree how to resolve these.

Scanned records

This section applies to health and care records as much as it does to corporate records. When looking to scan records, organisations need to consider the following:

- the scanned image can perform equally as well as the original paper
- scanned images can be challenged in court (just as paper can)
- ability to demonstrate authenticity of the scanned image
- ensure technical and organisational measures are in place to protect the integrity, usability and authenticity of the record, over its period of use and retention
- discussions need to take place with the local PoD over records that may be permanently accessioned - they will need input into the format of the transferring record
- where the hard copy is retained, this will be legally preferable to the scanned image

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or digital, can be admissible as evidence.

The Archives and Records Association has produced a flow chart to support scanning processes. The British Standards Institution has published a standard that specifies the method of ensuring that electronic information remains authentic. The standard deals with both 'born digital' and scanned records. The best way to ensure that records are scanned in accordance with the standard is to use a supplier or service that meets the standard following a comprehensive procurement exercise, which complies with NHS due diligence. Using an BSI10008 accredited supplier, or an in-house accredited service would be seen as best practice.

For local scanning requirements or for those records where there is a low risk of being required to prove their authenticity, organisations may decide to do their own scanning following due diligence and internal compliance processes. This may require a business case to be drawn up and approved, and procurement rules followed to purchase the necessary equipment.
Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original, unless the format of the original has historical value, in which case consideration should be given to keeping it with a view to permanent transfer. Where paper is disposed of post-scanning, this decision must be made by the appropriate group or committee. A scan of not less than 300 dots per inch (or 118

dots per centimetre) as a minimum is recommended for most records although this may drop if clear printed text is being scanned. Methods used to ensure that scanned records can be considered authentic are:

- board or committee level approval to scan records
- a written procedure outlining the process to scan, quality check and any destruction process for the paper record
- evidence that the process has been followed
- technical evidence to show the scanning system used was operating correctly at the time of scanning
- an audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- fix the scan into a file format that cannot be edited

Some common mistakes occur in scanning by:

- only scanning one side and not both sides, including blank pages - to preserve authenticity, both sides of the paper record, even if they are both blank, must be scanned (this ensures the scanned record is an exact replica of the paper original)
- scanning a copy of a copy - leading to a degraded image
- not using a method that can show that the scanned record has not been altered after it has been scanned – questions could be raised regarding process and authenticity
- no long-term plan to enable the digitised records to be stored or accessed over the period of their retention

Once you have identified digital records that are suitable for accessioning to your local PoD or The National Archives (for national bodies, it is recommended to follow published The National Archives guidance on the accessioning of digital records.

Social media

Organisations must have approved policies and guidance when using social media platforms. It is acknowledged that social media will mainly be used for promoting activities of the organisation, rather than as a way of communicating care issues or interventions with patients or service users. Information posted on social media may also be classed as a corporate record and appropriate retention periods set where applicable.

Information posted on social media (such as details of upcoming meetings, or published policies) will usually be captured elsewhere in an organisation's corporate records' function, and where this is the case, there is no value in retaining the information held in the social media platform, as it will be a duplication of the corporate records management function.

The National Archives have begun to capture social media content of NHS bodies that have a national focus, such as NHS England and Improvement. Where requested, this can also be extended to local NHS bodies, but this would be the exception not the rule.

Website as a business record

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

For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate or there must be some other method to recreate what the website or intranet visitor viewed. It may be possible
to arrange regular crawls of the site with the relevant PoD 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 (part of The National Archives) 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.

National NHS organisations have their websites regularly captured by The National Archives and can (upon request) capture local organisation's websites, where regional information would be captured that would not necessarily go to the local PoD (such as a CCG closing down). Local Authorities' websites are not routinely

captured by the WebArchive Team at The National Archives but they can do so in exceptional circumstances and if requested by the Authority.

Annex 1: Records at contract change

Characteristic of new service provider	Fair processing required	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 campaigns 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. All records must be transferred by the former provider to the new provider.	Individual communications may not be possible so obtaining consent, from the holder of the current caseload, may need to be sought by the old provider before transfer. It may not be possible to transfer the record without consent (to satisfy confidentiality) so in some cases no records will be transferred.

Non-NHS provider from different premises but with same staff.	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload.	
Non-NHS 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.	