NHS
Yorkshire
Ambulance Service
NHS Trust

Records Management Policy

Document Author: Information Governance Manager

Date Approved: May 2018

Document Reference	PO – Records Management Policy
Version	9.1
Responsible Committee	Trust Management Group
Responsible Director (title)	Executive Director of Quality, Governance and Performance Assurance
Document Author (title)	Information Governance Manager
Approved by	Trust Management Group
Date Approved	May 2018
Review Date	March 2021
Equality Impact Assessed (EIA)	Yes - Screening
Protective Marking	Not protectively marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
2.0	Sept 2008	David Johnson	A	Revisions to format and content.
3.0	Feb 2010	David Johnson	A	Revisions to format and content.
4.0	Feb 2011	David Johnson	A	Revisions to format and content. Amended staff details in table, section 14.10.
5.0	Dec 2011	Julie Barber	A	Revisions to format and content. Updated to reflect minor changes in processes/procedures and policy over the last 12 months.
5.1	Feb 2013	Caroline Squires	D	Significant revisions to existing procedural document in relation to content and format.
5.2	April 2013	Caroline Squires	D	Minor amendments following consultation with Information Governance Working Group members.
5.3	May 2013	Caroline Squires	D	Amendments to content and format following Senior Management Group meeting.
6.0	June 2013	Caroline Squires	A	Minor amendments. Approval by Senior Management Group.
6.1	Nov 2015	Caroline Squires	D	Amendments to reflect latest policy format and minor accuracy changes.
7.0	Dec 2015	Caroline Squires	A	Approval by Trust Management Group in December 2015.
7.1	Dec 2016	Leon Kaplan	D	Amendments to reflect Records Management Code of Practice 2016
8.0	Feb 2017	Leon Kaplan	A	Approved by TMG
8.1	Sept	Allan Darby	A	Extension agreed at TMG in

	2017			preparedness for the launch of General Data Protection Regulations which come in to force May 2018. IG policies remain best practice up to this date.
8.2	Apr 2018	Allan Darby	D	Amended to reflect GDPR and Data Security and Protection Toolkit requirements.
8.3	April 2018	Risk Team	D	New Visual Identity – Document Formatted
	April 2018	IG Working Group		Review by IG Working group – agreed
9.0	May 2018		A	TMG – approved subject to adding a paragraph regarding loss of paper PCRs – completed at 3.5
9.1	August 2020	Ruth Parker	D	Date agreed by TMG for review date extension

A = Approved D = Draft

Document Lead =Information Governance Manager

Associated Documentation:

- Health Record-Keeping Standards Guideline
- Information Governance Policy
- Information Governance Strategy
- Data Protection Policy and Associated Procedures
- Freedom of Information Policy
- ICT Security Policy and Associated Procedures
- Internet Policy and Procedure
- Email Policy
- Data Quality Policy

Staff Summary

The use of standardised file names and version control methods should be applied consistently throughout all record lifecycles.
File records in a logical manner to aid future retrieval and avoid making unnecessary duplications to help reduce the risk of data being lost, or unlawfully disclosed.
Where possible avoid printing copies of records.
Paper records that are sensitive or hold confidential information should be placed in a secure storage area when not in use.
Electronic records must be protected at all times from unauthorised disclosure, access and corruption. All electronic corporate/business records should be stored on shared drives or servers, which are regularly backed up.
No record should be destroyed until the retention period for that particular record type has expired.
Records believed to be ready for destruction should be documented onto the form "Authorisation for the Destruction of YAS Records", a copy of which can be found on the Trust intranet within the 'Records Management Resource Zone'. The relevant Executive Director / Associate Director must authorise the destruction.
All staff are personally responsible for making themselves aware of and complying with this policy

1.0 Introduction

1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format (paper or digital) or media type (see 1.3 below), from their creation, all the way through their lifecycle to their disposal or permanent archive.

1.2 The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. Records are required for a number of reasons and are essential to the organisation. Some examples of why records are needed are detailed below:

- To support patient care and continuity of care
- To support the day to day business and the delivery of care
- To support evidence based clinical practice
- To support sound administrative and managerial decision making, as part of the knowledge base for NHS services

- To meet legal requirements, including requests from patients under subject access provisions of the General Data Protection Regulations, Data Protection Act and/or the Freedom of Information Act
- To assist clinical and other types of audits
- To support improvements in clinical effectiveness through research and also to support archival functions by taking account of the historical importance of material and the needs of future research
- To support patient choice and control over treatment and services designed around patients.

1.3 Examples of types of record and media covered by this policy include:

- Patient clinical records (electronic or paper based)
- Integrated health and social care records
- Data processed for secondary use purposes. Secondary use is any use of person level or aggregate level data that is for direct care purposes. This can include data for service management, research or support for commissioning.
- Corporate records (such as HR, estates, financial, complaint-handling)
- Photographs, slides and other images
- Microform (i.e. microfiche/microfilm)
- Audio and video tapes, cassettes, CD-ROM etc
- E-mails
- Staff diaries
- Computerised records
- Scanned records
- SMS text messages (both outgoing from the NHS and incoming responses)
- Computer database outputs, disks and all other electronic records
- Material intended for short term or transitory use, including notes and copies of documents.
- Websites and intranets sites that provide key information for patients and staff.

1.4 The Trust is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- better use of physical and digital space
- clear standards for record keeping, tracking and destruction
- better use of staff time and more efficient workflows
- improved control, access, and retrieval of valuable information assets
- compliance with legislation and professional standards
- reduced business costs resulting from poor records management
- reduced volume of lost or duplicated information
- a better understanding of the types of records held
- an informed and educated workforce, able effectively to carry out records management responsibilities.

2.0 Purpose/Scope

2.1 The purpose of this policy is to provide clear guidance to all staff in the handling and management of all records both corporate and clinical, regardless of the media on which they are stored. Additionally, this policy sets out a framework within which staff responsible for managing the Trust's records can develop specific local procedures to ensure that records are managed and controlled effectively commensurate with legal, operational and information needs.

2.2 This policy supports at a local level the legal and best practice requirements set out with the Records Management Code of Practicefor Health and Social Care 2016 for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice. This has been published by the Information Governance Alliance (Department of Health, NHS England, NHS Digital, and Public Health England).

2.3 **All staff are personally responsible for making themselves aware of and complying with this policy.**

3.0 Process

3.1 Legal and Regulatory Obligations

3.1.1 All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the Records Management Code of Practice for Health and Social Care 2016, in particular:

- The Public Records Acts 1958 and 1967
- General Data Protection Regulations 2016
- Data Protection Act 2018
- The Freedom of Information Act 2000
- Lord Chancellor's Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000 which directs public organisations to have records management systems which will help them perform their statutory function
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice

and any new legislation affecting records management as it arises.

3.1.2 All records (manual or electronic) containing personal data are covered by the General Data Protection Regulations 2016 and the Data Protection Act 2018 and consequently the provisions of the Act apply to all of the Trust's records containing person identifiable information including patient records and staff identifiable records.

3.1.3 For most health professionals, there are relevant codes of practice issued by the registration bodies and membership organisations of staff. That guidance

is designed to guard against professional misconduct and to provide high quality care in line with the professional bodies.

3.1.4 The Academy of Medical Royal Colleges (AoMRC) has 12 generic medical record keeping standards.

3.1.5 There is professional guidance on the structure and content of the clinical records of ambulance patients, hosted by the Royal College of Physicians.

3.2 Records Creation, Capture, Maintenance and Quality

3.2.1 Record Creation

When creating information in the first instance, these principles apply:

- ***Available when needed*** - to enable a reconstruction of activities or events that have taken place.
- ***Accessible to all members of staff that require access in order to enable them to carry out their day to day work*** - the information must be located and displayed in a way consistent with its initial use and that the current version is clearly identified where multiple versions exist.
- ***Interpretable, clear and concise*** - the context of the information must be clear and be able to be interpreted appropriately, i.e. who created or added to the record and when, during which business process and how the record is related to other records. This is especially important for managing emails.[1]
- ***Trusted, accurate and relevant*** - the information must reliably represent the initial data that was actually used in, or created by, the business process whilst maintaining its integrity. The authenticity must be demonstrable and the content relevant.
- ***Secure*** - the information must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled and audit trails used to track all use and changes. The information must be held in a robust format which remains readable for as long as the information is required or retained.

Employees should also consider the following when creating information for the first time:

- What is being recorded and how it should be recorded
- Why is it being recorded
- How to validate the information (and against what) in order to ensure that what is being recorded is the correct data
- How to identify errors and how to report errors and correct them accordingly

[1] Email fixes information in time and assigns an 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, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system of the activity to which it relates. If an 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, e.g., an email approving a business case must be saved with the business case file.

- The intended use of the information, understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important)
- How to update the information and how to add in information from other sources

A step by step guide to creating clinical records can be found in Appendix D and a step by step guide to creating corporate records can be found in Appendix E.

3.2.2 **Record Capture**

For reasons of business efficiency or, in order to address problems with storage, consideration should be given to the option of scanning paper format records into electronic format. Where this is proposed, the factors to be taken into account include the:

- Costs of the initial (and any later) media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept.
- Need to consult in advance with the local Place of Deposit or The National Archives with regard to records which may have archival value, as the value may include the format in which it was created.
- Need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the 'BS 10008 Electronic Information Management – Ensuring the authenticity and integrity of electronic information'.
- In order to fully realise the benefits of reduced storage requirements and business efficiency, the Information Asset Owners (IAOs) should dispose of any paper records that have been copied into electronic format and stored in accordance with appropriate standards. Where the record constitutes confidential information it must be securely destroyed.

3.2.3 **Record Maintenance**

All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed (perhaps permanently) despite changes in the format.

3.2.4 **Quality**

All staff must ensure that high standards of data quality are applied at every phase of the records lifecycle, for further detailed guidance please refer to the Data Quality Policy on the Trust's intranet.

For details of the procedures and quality standards which must be used by all Trust staff with patient contact, when completing the clinical records, please refer to the following:

- The Health Record-Keeping Standards Guideline which can be found on the Trust intranet in the Policy, Procedure and Strategy Document Library.

- Patient Care Record (PCR) Completion Guides - There are a number of different PCR forms currently used by Trust clinicians to record the details of the treatment provided to a patient and all other relevant details surrounding the incident attended. There are comprehensive Completion Guides to assist clinicians in the completion of the various forms which can be found on the Trust's intranet at the following link: http://pulse.yas.nhs.uk/apps/ClinicalPathways/Pages/Patient-Care-Record-Completion-Guides.aspx

3.3 Records Use - Control, Tracking, Security and Storage

3.3.1 Record Control

The use of standardised filenames and version control methods should be applied consistently throughout all record lifecycles. Please refer to the table below for guidance on how to version control a document from the point of its creation, on-going maintenance and throughout its use.

How to Version Control a Document

Stage	**Version Number**	**Filename**
Initial creation	0.1	APolicyDocument_v0.1 - draft
Second draft to include some feedback	0.2	APolicyDocument_v0.2 - draft
Third draft to include changes from stakeholders	0.3	APolicyDocument_v0.3 - draft
All changes included, ready for approval	0.4	APolicyDocument_v0.4 - draft
Approved version – now ready for release	1.0	APolicyDocument_v1.0 - FINAL
DOCUMENT PUBLISHED AND RELEASED	**1.0**	APolicyDocument_v**1.0** - **FINAL**
Review now due		
Make amendments on the draft as applicable	1.1	APolicyDocument_v1.1 - draft
Incorporate feedback from stakeholders	1.2	APolicyDocument_v1.2 - draft
Issue for approval	1.3	APolicyDocument_v1.3 - draft
Incorporate feedback from the approvers	1.4	APolicyDocument_v1.4 - draft
Re-issue for final approval	1.5	APolicyDocument_v1.5 - draft
Approved version – now ready for release	2.0	APolicyDocument_v2.0 - FINAL
DOCUMENT RE-PUBLISHED AND RE-RELEASED	**2.0**	APolicyDocument_v**2.0** - **FINAL**

Where possible all staff must avoid duplication and printing copies of records. This increases risks of breaches of confidentiality and needlessly increases administrative and paper costs felt by the Trust. Where the creation of copies

is unavoidable, they must be destroyed as soon as they are no longer required.

3.3.2 Record Tracking

Version Number	Date of Change	Time of Change	Full Name	Reason for / Type of Change
1.0	31/01/2010	14.30	John Smith	To include staff mobile contact numbers.
1.1	28/02/2010	10.00	Joanne Smith	Add additional data to include full postal address.

Example of a Manual Audit Trail for Electronic and/or Paper Records

The process flow for tracking both electronic and paper based records can be found in Appendix F.

3.3.3 Tracking Electronic Records

The tracking of electronic records is held automatically in the audit trails of the systems that hold the data. Where this type of audit trail does not exist for some systems, staff must enter a manual audit trail in the record itself that details the full name of the person to last update the record and the date and time the amendment was carried out (please refer to the example above).

Depending on the nature of the record, this level of detail may not always be applicable, however best practice is to ensure version control is always applied as a minimum. If a particular record cannot be version controlled, has no automatic system audit trail and a manual audit trail cannot be easily applied directly to the record itself, consideration should be given to a separate document that details the audit of amendments to that particular record.

Records should be closed (i.e. made inactive and transferred to a secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records, or folder of electronic records, has been closed, together with the date of closure, should be shown on the record itself, as well as noted in the index, manual audit trail or database of the files/folders.

Where possible, information on the intended disposal of electronic records is included in the metadata when the information is created. The storage of closed records follows accepted standards relating to environment, security and physical organisation of the files. This is handled by the organisation's third party storage contractor which is used for archiving closed paper records and also the secure destruction of the records once the relevant retention period has expired.

The above table can be less detailed where applicable, for example the time of the change may only be required if a particular record is being updated numerous times during the same working day. Likewise additional columns can be added if further details about the type of change are required. The above manual audit trail can be used for both electronic and paper records.

3.3.4 Tracking Paper Records

Paper records do not have the facility of an automatic audit trail that electronic systems offer and so staff must enter a manual audit trail in the record itself that details the full name of the person to last update the record and the date and time the amendment was carried out (please refer to the example above). Depending on the nature of the record, this level of detail may not always be applicable, however best practice is to ensure version control is always applied as a minimum. If a particular record cannot be version controlled and a manual audit trail cannot be easily applied directly to the record itself, consideration should be given to a separate document that details the audit of amendments to that particular record.

Whilst the organisation is continually making changes to help reduce the amount of paper records produced in the first instance and to also convert some existing paper based records into electronic format using scanning, there is always likely to be the need for some paper based records within the organisation. In the first instance, staff must always look for alternative methods of creating, storing and maintaining records that do not involve the paper based means being the primary source. However, where a suitable electronic alternative is not readily available, staff must always seek to be as efficient as possible, file records in a logical manner to aid future retrieval and avoid making unnecessary duplications to help reduce the risk of data being lost, or unlawfully disclosed.

Staff must apply clear version control as described in section 3.3.1 and manual audit trail in the record itself, as described in the table above.

3.3.5 Tracking Paper Patient Care Record Forms (PCRs)

The Trust is currently implementing an electronic system for capturing clinical information when treating patients. The paper based versions of the various PCR Forms should continue to be used in areas where the electronic record has not yet been implemented. Since February 2010 all paper PCR forms across the whole organisation have been scanned and verified by the Healthcare Records team. The paper forms once scanned are retained for one week and then securely destroyed using a confidential waste contractor.

All staff must adhere to the Trust's procedures for handling and managing all the different types of PCRs. Each type of PCR has its own Completion Guide which can be found on the intranet:
http://pulse.yas.nhs.uk/apps/ClinicalPathways/Pages/Patient-Care-Record-Completion-Guides.aspx

There are a number of teams within the organisation that require access to these forms for various reasons. Specific individuals have direct access to the database (Onbase), where the scanned copies are held, which has a detailed

audit trail automatically generated each time an individual file/record is accessed or printed.

Please refer to the process flow for Tracking Paper Patient Care Record Forms which can be found in Appendix H.

Where completed PCRs are lost, every effort should be made to locate these by re-tracing steps where possible. An incident should be reported immediately, providing details of the lost PCR, including CAD 'job' number and patient details (where these are available). An information governance breach including loss of personal or special categories of data will be considered in line with national policy and proportionate level of escalation and investigation will be undertaken. This may include reporting to the Information Commissioners Office. It is essential that staff should cooperate with the investigation by providing any additional information requested.

3.4 Record Security and Storage

The security of all Trust records is critical, as records provide evidence of business transactions, support management decisions and ensure public accountability requirements are met. Records in all formats should be stored securely to prevent unauthorised access, destruction, alteration or removal. Trust staff are responsible for the safe custody of all files and documents.

No paper records can be taken off Trust premises, e.g., home, except for a temporary period (i.e., overnight or at most a weekend) where a member of staff's travel to a meeting requires this. In all cases, only the minimum number of records relevant to that meeting is permitted. The member of staff must ensure the safe storage of those records whilst in their personal possession. The records must be returned to Trust premises by the next working day.

Paper records that are sensitive or hold confidential information should be placed in a secure storage area when not in use. Paper records must be stored in secure and preferably alarmed facilities with strict access controls in place. Electronic records must be protected at all times from unauthorised disclosure, access and corruption.

Storage of records in offices must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. Records held in offices are generally those that are in current use with cupboards and convenient storage areas utilised to store any archived records. These records must be securely stored to prevent theft or unauthorised access.

Offsite storage areas must conform to all current relevant legislation and guidance regarding Health and Safety, namely the Health & Safety at Work Act 1974 and Workplace (Health, Safety and Welfare) Regulations 1992. The Trust has a contract with external suppliers to provide secure storage of records. All records stored off site must still comply with retention periods.

The Trust follows the protective marking scheme for patient information as being 'NHS Confidential', which corresponds to the classification of "Official Sensitive" under the Cabinet Office Government Security Classifications (2014).

3.5 Records Retention, Appraisal and Disposal

3.5.1 Records Retention

The table in Appendix C details the minimum retention period for each type of record[2]. Records (whatever the media) may be retained for longer than the minimum period, however, records should not ordinarily be retained for more than 30 years (this excludes a number of Human Resources record types, which should be retained until the individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time). The National Archives should be consulted where a longer retention period than 30 years is required, or for any records that pre date 1948.

The retention period varies dependent on the type of information being stored, clinical records should not ordinarily be retained for more than 30 years. The information being recorded and retained must be relevant, fit for the purpose it was intended and only retained for as long as it is genuinely required.

Please refer to the process flow for Retaining Records which can be found in Appendix I. Refer to Appendix C for the table detailing the retention periods for each record type.

36 Records Appraisal

The process of deciding what to do with records when their business use has ceased is called appraisal. The three outcomes of appraisal are: destroy/delete (see 3.5.3 below); keep for a longer period (see 3.5.1 above) or transfer to a place of deposit appointed under the Public Records Act 1958 (see 3.6 below).

3.7 Records Disposal

Disposal is defined as the point in the records lifecycle when it is either transferred to an archive, or securely destroyed. It is particularly important under the Freedom of Information legislation that the disposal of records is undertaken in accordance with this policy and in accordance with the retention requirements of any local and national inquiries such as the Independent Inquiry into Child Sex Abuse (IICSA) which has requested large parts of the Health and Social Care sector do not destroy any records that are, or may fail into, the remit of the inquiry. This includes children's records and any instances of allegations or investigations or any records of an institution where abuse has, or may have occurred. Local guidance should be followed in relation to record retention instructions issued by inquiries.

[2] The table does not contain all record types, only those records that are used or referred to most frequently in the organisation have been extracted for guidance. If information is required regarding another type of record, not listed in the table, please refer to the Records Management Code of Practice for Health and Social Care 2016 at: https://digital.nhs.uk/article/402/Information-Governance

No record should be destroyed until the retention period for that particular record type has expired. The retention periods for the most frequently used record types are listed in the table in Appendix C.

Records believed to be ready for destruction should be documented onto the form "**Authorisation for the Destruction of YAS Records**", a copy of which can be found on the Trust intranet within the 'Records Management Resource Zone'.

Once all the details of the records that need destroying have been listed, the relevant Executive Director / Associate Director must authorise the destruction. At no point should any member of staff request destruction of any records without the signed permission of a Director / Associate Director. This authorisation process should be used for records held locally on YAS premises as well as records held by the Trust's records storage contractor, and the authorisation process should be used irrespective of whether the record is of a confidential nature or not.

The same authorisation form must be used for electronic records that require destruction/deletion. Contact the ICT department for details of how to ensure that all copies/instances of the records are deleted from any temporary cache or mirrored databases/systems.

The authorisation form listing the records that were destroyed, must be retained indefinitely in accordance with the retention period described in the table in Appendix C.

The destruction exercise relating to records held by the records storage contractor will be co-ordinated on a yearly basis by the Information Governance Manager on behalf of the relevant Information Asset Owners.

Confidential paper based records held locally on YAS premises must be securely disposed of as soon as possible after they are eligible.

Please refer to the 'Step by Step Guide to Disposing of Records' process flow chart which can be found in Appendix J.

3.7.1 **Records Archiving**

Records of the NHS and its predecessor bodies are subject to the Public Records Act 1958, which imposes a statutory duty of care directly upon all individuals who have direct responsibility for any such records. If the records have no on-going administrative value but have or may have long-term historical or research value, or they have some administrative value but are more appropriately held as archives. Records with such value must be transferred to the organisation's approved Place of Deposit. Where the organisation has no existing relationship with a Place of Deposit, The National Archives should be contacted in the first instance. Where the Trust is unsure whether records may have archival value, The National Archives or the Place of Deposit with which the organisation has an existing working relationship should be consulted.

Contact National Advisory Services at TNA (nas@nationalarchives.gov.uk, 020 8392 5330 x 2620). National Advisory Services are also able to advise on any other queries regarding the working of the Public Records Act in respect of NHS records. A list of all the current appointed Places of Deposit is available on The National Archives website:
http://www.nationalarchives.gov.uk/archives/deposit.htm

It is a legal requirement that NHS records which have been selected as archives should be held in a repository that has been approved for the purpose by The National Archives. Where an organisation is already in regular contact with its Place of Deposit, it should consult with it over decisions regarding selection and transfer of records. Where this is not the case, The National Archives should be contacted in the first instance.

The Government is reducing this timeframe for transfer from 30 to 20 years. In 2013, central government records were transferred to the National Archives for 1983 and 1984. Two years' worth of records are now being transferred each year, so that by 2022, the records will relate to 2001 and 2002.

There is an annual survey to monitor the progress of record transfers for all public sector organisations affected by the 20 year rule.

3.7.2 Records Transfer

The mechanisms for transferring records from one organisation to another should be tailored to the sensitivity of the material contained within the records and the media on which they are held. Before transferring any information that may be of a confidential nature you must have approval from the relevant Information Asset Owner for the business area concerned.

Ensure that all transfers of confidential records are handled in accordance with the Trust's:

- Data Protection Policy and Associated Procedures
- ICT Security Policy and Associated Procedures
- Email Policy

4 Records Access, Retrieval and Disclosure

4.1 Records Access

Records must be available to all authorised staff who require access to them for business purposes.

Records held in electronic format are often easier to access and maintain, however staff must always ensure that records are not being accessed unnecessarily, or kept for any longer than reasonably required just because it is easier to do so. If the records contain information that is person identifiable, personal or of a sensitive nature the principles of the General Data Protection Regulations 2016 and the Data Protection Act 2018 as well as the Caldicott Principles must be adhered to.

Records held in paper format are less easy to access, maintain and control than electronic records due to the very nature of them. Paper based records

often only have the one master copy and are difficult to back up easily and cost effectively. Therefore, staff must take additional precautions when safeguarding and filing paper records to ensure that retrievals will be possible, when required at some point in the future. Where possible the filing and archiving of paper based records should provide sufficient information to allow the identification of the records needed and wherever possible should be filed in accordance with the intended future destruction date, i.e. all records due to be destroyed on the same date should be filed together. This makes the secure destruction of these records much more straight forward.

4.2 **Records Retrieval**

All electronic corporate/business records should be stored on shared drives or servers, which are regularly backed up, and not on the C drives of Trust computers, laptops or peripheral devices. This enables the retrieval of information by staff other than the author where appropriate and necessary. It also greatly reduces the risk of loss due to the failure of laptop or desktop PC hard drives or theft.

The retrieval of electronic records is also easier to control due to the rights and restrictions that can automatically be applied to individual staff logins for the various systems that hold records. Managers are responsible for authorising and requesting the appropriate user rights for individual members of staff, however all staff continue to be responsible for security and integrity of the records and information which they record, handle, store, or otherwise come across during their day to day duties.

All information must be used consistently, only for purposes for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from the Information Governance Manager in the first instance, who will inform the relevant IAO for the business area concerned.

The Trust is committed to effective record keeping systems in logical filing systems and the application of metadata or 'context' to assist retrieval.

4.3 **Retrieving Archived Paper Records held in Storage with External Storage Contractor**

To retrieve archived paper records that have been boxed and stored with the organisation's external storage contractor, please contact the relevant authorised Filetrak user for your department. For details of the authorised users in each department and their levels of permissions, please refer to the 'Records Management Resource Zone' on the Trust's Intranet.

The storage contractor holds the same list of authorised Filetrak users that can make requests for boxes to be retrieved from store and delivered to designated addresses across the organisation.

Please refer to the process flow for retrieving archived paper records in storage which can be found in Appendix G.

4.4 **Records Disclosure**

Person identifiable information held on corporate/business records must be treated as strictly confidential and may only be disclosed to individuals authorised as part of their day-to-day work to have access to it, or with the written consent of the person in question. There are exceptions where disclosure may be permitted, please refer to the Trust's Data Protection Policy and Associated Procedures for further advice.

4.5 **Requests for Information by External Third Parties**

Should members of staff be approached by a third party organisation for copies of any information they must refer the request to the appropriate team within the organisation. Under no circumstances should staff divulge any information, however small, to anyone external to the organisation.

Staff must direct all such requests immediately to the teams trained to handle and process these requests or, alternatively, seek advice and support from their line manager in the appropriate direction of the request. The Legal Services Team and Freedom of Information team take ownership of the request and ensure that it is handled in a consistent manner, whilst also ensuring that any disclosures of person identifiable information, when carried out, are in strict accordance with the Data Protection Act 2018 and Common Law Duty of Confidentiality.

The requests may be, but are not limited to, Subject Access Requests, Police and Coroners' requests or any other type of request where staff are asked for copies of paper PCR forms, copies of calls placed with the Emergency Operational Centre and any other documentation held by the organisation. Regardless of what is being requested and who the third party making the request is, staff must refer the requestor to the teams listed in the 'Contact Details of the Staff that handle all Requests for the Release of Trust Information' which can be found on the Trust intranet within the 'Records Management Resource Zone'.

4.6 **Requests for Information by Internal Trust Staff**

Should staff be approached to provide copies of records, divulge information verbally or confirm specific details of records to internal Trust staff, this is acceptable providing the member of staff being approached is confident that the person requesting the information is actually a member of Trust staff and the Caldicott Principles are followed at all times, including the 'need to know'. Should the staff member be in any doubt, it is acceptable to ask for the request to be emailed in order to verify the requesting staff member's identity and legitimacy of the request. If there is any doubt following the email request then staff should discuss the request with their line manager or another appropriate manager before disclosing any information.

For full details on the procedures for handling requests for information by external third parties and/or internal Trust staff, please refer to the "Data Protection Policy and Associated Procedures" available on the Trust's intranet: http://pulse.yas.nhs.uk/apps/Library/PoliciesandProceduralDocuments/Data%20Protection%20Policy_V5.0.pdf

Also refer to the process flow for Retrieving Paper Clinical Records in the form of PCRs which can be found in Appendix H.

4.7 **Digital Records, Digital Continuity Digital Preservation and Forensic Readiness**

4.8 The National Data Guardian's (Dame Fiona Caldicott) Review of Data Security, Consent and Opt-Outs introduces a new standard for unsupported software systems. The Trust will review its legacy systems and the future-proofing of its digital clinical record keeping systems to maintain the authenticity, reliability, integrity and usability of records within, as digital technology advances.

4.9 The Trust is adopting a Forensic Readiness Policy to be able to collect, preserve, protect and analyse digital evidence so that this evidence can be used in legal matters, in security investigations, and in disciplinary matters.

5 Dealing with specific records

5.1 Records at contract change

The Trust acknowledges the guidance in the Records Management Code of Practice for Health and Social Care 2016, at the end of a contract for service provision with regard to:

- Retaining records after the contract has ended until the time period for their liability has expired, or making arrangements by which the records can be obtained again.
- Transferring a copy or summary of the entire record of the current caseload to a new provider for continuity of service.
- Informing service users about the change of contract and depending on the circumstances seeking consent and offering the opportunity to object or talk to someone about the transfer.

5.2 **Integrated Records**

The Trust is party to or going to be party to integrated or joint care records. The Trust is mindful that the ownership of and access to those records must be attributed. The arrangements for doing so will depend on the record, and the Trust commits to the principle of patient consent; as well as an information sharing agreement as a mechanism for providing clarity and transparency on the standards that all participants must meet.

5.3 **Controlled Drugs Regime**

The Trust follows the procedures for handling information relating to controlled drugs, by NHS England and the NHS Business Services Authority, which includes the conditions for storage, retention and destruction of information.

5.4 **Records created via social media**

The Trust will be mindful that where social media is used as means of communicating business information to clients, a record of the activity may

need to be captured through transcription or periodic storage and this information may need to be retained.

5.5 **Website as a Business Record**
The Trust will be mindful that as the internet replaces posters, publications and leaflets to interact with service users, websites form part of the record keeping system and must be preserved.

5.6 **Cloud based records**
The Trust will follow guidance on cloud storage from the Information Commissioner's Office where records might be stored, rather than on discs or networks (e.g., CCTV images.)

6.0 Training Expectations for Staff

Training is delivered as specified within the Trust Training Needs Analysis (TNA).

7.0 Implementation Plan

The latest approved version of this policy will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this policy and associated procedures during Trust Induction.

8.0 Monitoring Compliance with this Policy

A variety of methods will be used for monitoring compliance against the Records Management Policy including:

- Audit of the quality of information entered on the Restore Ltd Filetrak database and accuracy of the destruction dates set against records.
- Annual Confidentiality Audits carried out by IAOs.
- IAO risk review meetings
- Annual review of user access to the Filetrak system including a review of access rights.
- Annual audit of health records which includes record creation, record tracking, record retrieval and record retention, disposal and destruction.

9.0 References

9.1 Legislation

- Great Britain. 2018. Data Protection Act 2018. London: HMSO. Available at: www.legislation.gov.uk
- European Union. 2016. EU General Data Protection Regulations 2016. Available at: www.eugdpr.org
- Great Britain. 2000. Freedom of Information Act 2000. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2004. *Environmental Information Regulations 2004.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Computer Misuse Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1990. *Access to Health Records Act 1990. Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1958 and 1967. *Public Records Act 1958 and 1967.* London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 1998. *Crime and Disorder Act 1998*. *Chapter*. London: HMSO. Available at: www.legislation.gov.uk
- Great Britain. 2000. *Electronic Communications Act 2000.* London: HMSO. Available at: www.legislation.gov.uk

9.2 Guidance

- Information Governance Alliance, 2016: Records Management Code of Practice for Health and Social Care 2016. Available at: https://digital.nhs.uk/article/402/Information-Governance
- NHS Digital: Data Security and Protection Toolkit. Available at: www.dsptoolkit.nhs.uk/
- Department of Health, 2003. Confidentiality: NHS Code of Practice Available at: https://digital.nhs.uk/article/402/Information-Governance
- Academy of Royal Colleges, 2013: Standards for the clinical structure and content of patient records. Available at: https://www.rcplondon.ac.uk/projects/outputs/standards-clinical-structure-and-content-patient-records
- Royal College of Physicians, 2015: Professional guidance on the structure and content of ambulance records
  Available at: https://www.rcplondon.ac.uk/projects/professional-guidance-structure-and-content-ambulance-records

10.0 Appendices

Appendix A Definitions

The definitions or explanation of terms relating to this policy are:-

Record	Records are defined as 'information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. (ISO 15489:2016) Traditionally records were held on paper, or microfiche, but are now predominantly created and held in electronic format or within electronic systems. The Data Protection Bill Part 7 defines a health record as: A "health record" means a record which— (a) consists of data concerning health, and (b) has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates;
Corporate Records	Records (other than health records) that are of, or relating to, an organisation's business activities covering all the functions, processes, activities and transactions of the organisation and of its employees. Examples of corporate information are policies and procedures, strategies and action plans, minutes and agendas, reports (e.g. annual, accounting, Board), Financial Standing Orders, invoices, public consultations, contracts.
Clinical Records / Health Records	A single record with a unique identifier containing information relating to the physical or mental health of a given patient who can be identified from that information and which has been recorded by, or on behalf of, a health professional, in connection with the care of that patient. This may comprise text, sound, image and/or paper and must contain sufficient information to support the diagnosis, justify the treatment and facilitate the on-going care of the patient to whom it refers.
(Records) Information Lifecycle	The five distinct phases that all records will follow are: creation, use, retention, appraisal and disposal. For further details on each phase please refer to section 3.0.
Person Identifiable Information	Information (or data) relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental,

	economic, cultural or social identity. Information that can be used to uniquely identify, contact, or locate a single person, or can be used with other sources to uniquely identify a single individual, this includes both patients and Trust staff.

Appendix B Roles and Responsibilities

Trust Board
The Trust Board has overall responsibility for records management within the organisation with the Chief Executive being ultimately accountable for the proper management of all records within the organisation. The Executive Directors are accountable for the quality of records management within each of their Directorates.

Trust Management Group (TMG)
The Trust Management Group consists of Executive Directors and Associate Directors and is chaired by the Chief Executive. The Group carries delegated responsibility from the Trust Executive Group for approving this policy.

Executive Director of Quality, Governance and Performance Assurance
The Executive Director of Quality, Governance and Performance Assurance has strategic responsibility for Information Governance including records management. The Executive Director of Quality, Governance and Performance Assurance is also the Trust's Senior Information Risk Owner (SIRO) and as such is the executive responsible for managing information risk.

Information Asset Owners
Information Asset Owners have direct responsibility for the records held in their work area, including the integrity, secure storage and quality of those records. IAOs are responsible for taking a pro-active role in championing good records management within their areas of responsibility as well as ensuring the appropriate use of the Trust's external document storage contractor.

The IAOs provide direct support to the Senior Information Risk Owner and are also responsible for identifying, managing and mitigating information risks in relation to records they are responsible for.

Information Governance Manager
The Information Governance Manager is responsible for providing general guidance and advice on the management and retention of records and the application of this policy.

Line Manager and Supervisors
All line managers and supervisors are responsible for ensuring that their staff are adequately trained and apply the appropriate guidelines on a day to day basis.

All Staff
All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. This responsibility is established at, and defined by, the law (the Public Records Act). In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with associated guidance. Individuals are also bound by their own professional Codes of Conduct.

Appendix C

Retention Periods for each Record Type

The retention periods listed in the column “YAS Retention Period” in the following table are the retention periods that staff should refer to and adhere to at all times, the Information Governance Alliance ’Notes’ column is for additional information and reference only. The table below has been updated from the Records Management Code of Practice for Health and Social Care 2016, published by the Information Governance Alliance.

The table does not contain all record types, only those records that are used or referred to most frequently in the organisation have been extracted for guidance. If information is required regarding another type of record not listed in the table, please refer to the Code of Practice at: https://digital.nhs.uk/article/402/Information-Governance:

The main source of patient identifiable records, produced by the organisation, are the paper based PCR forms completed by ambulance crews. Due to the operational constraints regarding the collation, retention, archiving and subsequent retrieval of those paper PCR forms, the organisation cannot segregate records pertaining to different patient types. Therefore, all the organisation’s paper PCR forms fall under the record type “ambulance records” and from February 2010 onwards, were scanned into electronic format, verified and the paper copies securely destroyed after one week using the Trust’s document storage contractor.

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Clinical Records / Operations:			
Ambulance records (patient identifiable component)	Main A3 PCR Form Computer Aided Dispatch Record	**Adult - 8 years** (applies to ALL Ambulance Clinical Records) **Children and young people - Retain until the patient's 25th birthday** or 26th if young person was 17 at conclusion of treatment, or 8 years after death.	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats. Where a patient is transferred to the care of another NHS organisation all relevant clinical information must be transferred to the patients' health record held at that organisation. Staff must always pass the yellow (bottom) copy of the patient form(s) to the hospital.

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Audio tapes of calls requesting care	A&R calls	**3 years** and/or **Adult - 8years** - see notes. **Children and young people - Retain until the patient's 25th birthday** or 26th if young person was 17 at conclusion of treatment, or 8 years after death.	Retain taped calls for 3 years providing all relevant clinical information has been transferred to the appropriate patient record. Where the information is NOT transferred into a health record, the tapes should be retained for 8 years (adult) and until the patient's 25th birthday or 26th if young person was 17 at conclusion of treatment, or 8 years after death (Children and young people).
Audit Trails of electronic health records	ePCR audit trail	**Indefinitely**	NHS organisations are advised to retain all audit trails until further notice.
Children and young people (all types of records relating to children and young people)		**Retain until the patient's 25th birthday** or 26th if young person was 17 at conclusion of treatment, or 8 years after death.	If the illness or death could have potential relevance to adult conditions or have genetic implications, the advice of clinicians should be sought as to whether to retain the records for a longer period.
Clinical audit records	Clinical Performance Indicators reports	**5 years**	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Controlled drug documentation	Drug books	Requisitions – **2 years.** Registers and CDRBs – **2 years from last entry**	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) guidance can be found at the link (subscription required) http://www.rpharms.com/support/mep.asp#new Guidance from NHS England is that locally held controlled drugs information should be retained for 7 years. NHS BSA will hold primary data for 20 years and then review. NHS East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see:http://www.medicinesresources.nhs.uk/en/Communities/NHS/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Destruction records of individual health records, case notes and other health-related records - paper and/or elec format. (refer to 'destruction of records (other than health records)' for corporate record destructions)		**Indefinitely**	
Electrocardiogram (ECG) records	ECG strips	**8 years**	Each chart should be labelled with the patient's name and unique identifier (the incident date and number). Any over-sized charts can be stored separately where a report is written into the health records (this must be noted on the main A3 PCR).
Homicide / Serious Untoward Incident records		**20 years**	
Litigation - records/documents related to any litigation		**Dependent on the case** – see notes	As advised by the organisation's legal advisor. All records to be reviewed. Normal review period is 10 years after the file is closed.
Occupational health records (staff)		**6 years** after termination of employment, unless litigation ensues	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Occupationally Related Diseases (e.g. asbestosis, pneumoconiosis, byssinosos)		**40 years/5 years** after date of last entry in the record	For full details on Occupational Related Diseases, please go to: http://www.hse.gov.uk/riddor/occupational-diseases.htm 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.
(General) Operating Policies and Procedures		**3 years** retain the current version and previous version for 3 years Life of organisation plus 6 years (IGA)	From CQC outcome 21
Paediatric records		See Children and young people above	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Scanned records (relating to patient care)	Electronic scanned copy of a PCR form (originally on paper)	**Adult - 8 years** (applies to ALL Ambulance Clinical Records) **Children and young people - Retain until the patient's 25th birthday** or 26th if young person was 17 at conclusion of treatment, or 8 years after death.	
Risk Assessments		Retain the latest risk assessment until a new one replaces it	
Voice recordings, video records relating to patient care, video conferencing records related to patient care, DVD records related to patient care (includes Telemedicine records, Out of hour's records, GP cover and NHS 111 records).		**8 years**	
Vulnerable Adults		See 'Ambulance records'	

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Corporate Records (administrative and organisational):			
Accident forms	Datix	**10 years**	
Accident register (reporting of injuries, diseases and dangerous occurrences register)	Datix	**10 years**	
Agendas of board meetings, committees, sub-committees (master copies including associated papers)		**20 years**	
Agendas (other)		**2 years**	

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Agreements / Contracts Financial contracts: Approval files Approved suppliers lists Non-sealed (property) contracts on termination Non-sealed (other) contracts on termination Sealed contracts (and associated records) Maintenance contracts (routine) Contractual arrangements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract (e.g. waiting list initiative, private finance initiative)		 **15 years** **11 years** **6 years** after termination of contract **6 years** after termination of contract **15 years** (min) **6 years** from end of contract **6 years** after end of financial year to which they relate	 Retain for a minimum of 15 years, after which they should be reviewed.
Ambulance Records – Administrative (records containing non-clinical details only, eg records of journeys)	PTS journey sheets	**2 years** from the end of the year to which they relate	
Annual / corporate reports		**3 years**	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Assembly / Parliamentary questions, MP enquiries		**10 years**	
Audit Records, Internal & External in any format paper, electronic etc	Organisational Audits, Records Audits, Systems Audits	**2 years** from the date of completion of the audit	
Business plans, including local delivery plans		**20 years**	
Catering forms		**6 years**	
Close circuit TV images		**31 days** and erase permanently	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Commissioning decisions, appeal documentation, decision documentation		**6 years** from date of appeal and/or decision	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Complaints (see also litigation & litigation dossiers) Correspondence, investigation and outcomes Returns made to DH		**10 years** from completion of action Files closed annually and kept for **6 years** following closure	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Computer programmes written in-house, related documentation		Lifetime of software	
Contracts		See 'Agreements / Contracts'	
Copyright declaration forms (Library Service)		**6 years**	
Data Input Forms where the data/information has been input to a computer system	Address notifications from local Councils	**2 years**	

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Destruction of records (other than health records), records documenting the archiving, transfer to public records archive. (refer to 'destruction records of individual health-related records' for health record destructions)		**20 years**	
Diaries (office)		**1 year** after the end of the calendar year to which they refer	
Flexi working hours (personal record of hours actually worked)		**6 months**	
Freedom of Information requests		**3 years** after full disclosure	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical, to keep a summary of the redactions.
Health and safety documentation		**3 years**	
History of the organisation or predecessors, its organisation and procedures	Establishment order	**20 years**	
Incident forms	Datix	**10 years**	
Indices (records management) registry lists of public records marked for permanent preservation, or containing the record of management of public records. File lists and document lists where public records or their management are not covered.		**20 years**	

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Laundry lists and receipts		**2 years** from completion of audit	
Litigation dossiers (complaints including accident/incident reports) Records/documents relating to any form of litigation	Coroners' requests	**10 years**	Where a legal action has commenced, keep as advised by legal representatives
Manuals – policy and procedure (administrative and clinical, strategy documents)		**10 years** after life of the system (or superseded) to which the policies or procedures refer	Policy documents may have archival value.
Meetings and minutes papers of major committees and sub-committees (master copies)		**20 years**	
Meetings and minutes papers (other, including reference copies of major committees)		**2 years**	
Papers of minor or short-lived importance not covered elsewhere, eg advertising matter, covering letters, reminders, letters making appointments, anonymous or unintelligible letters, drafts, duplicates of documents known to be preserved elsewhere (unless they have important minutes on them) indices and registers compiled for temporary purposes, routine reports, punched cards, other documents that have ceased to be of value on settlement of the matter involved.		**2 years** after the settlement of the matter to which they relate	

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Patient Advice & Liaison Service (PALS) records		**10 years** after closure of the case	
Patient information leaflets		**6 years** after the leaflet has been superseded	
Patient Surveys re access to services etc		**2 years**	
Police Statements (made in the context of Accident and Emergency episodes. Statements are requested by the Police to the A&E staff in relation to alleged injuries of, or by, patients coming through A&E)		**10 years** (congruent retention period as Incident Forms)	
Press cuttings		**1 year**	Where bound volumes exist, these may have archival value.
Press releases and important internal communications		**6 years**	
Project files (including abandoned or deferred projects): Over £100,000 on termination Less than £100,000 on termination Project team files (summary retained)		 **6 years** **2 years** **3 years**	
Public Consultations eg about future provision of services		**5 years**	
Quality control records: External Internal (relating to products)		 **2 years** **10 years**	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Quality assurance records eg Healthcare Commission, Audit Commission, King's Fund Organisational Audit, Investors in People		**12 years**	
Receipts for registered and recorded mail		**2 years** following the end of the financial year to which they relate	
Reports (major)		**30 years**	
Requests for access to records (other than Freedom of Information or subject access requests)		**6 years** after last action	
Requisitions		**18 months**	
Serious incident files		**20 years**	
Software licences		Lifetime of software	
Specifications eg equipment, services		**6 years**	
Statistics including Korner returns, contract minimum data set, statistical returns to DOH, patient activity		**3 years** from date of submission	
Subject access requests (Data Protection Act 2018 and AHR) records of requests		**3 years** after last action	
Time sheets (relating to a Group or Department where the timesheets are kept as a tool to manage resources/staffing levels)		**6 months**	

Record Type ***(in alphabetical order)***	**Example(s)**	**YAS Retention Period** ***(from the date of creation unless otherwise stated)***	**Notes**
Estates / Procurement / Supplies records:			
Approval files (contracts and purchase orders)		**6 years** after end of the year the contract expired	
Approved suppliers lists		**11 years**	
Buildings, papers relating to occupation of the building (but not health and safety information)		**3 years** after occupation ceases	
Deeds of title		While the organisation has ownership of the building	Retain while the organisation has ownership of the building unless a Land Registry certificate has been issued, in which case the deeds should be placed in an archive. If there is no Land Registry certificate, the deeds should pass on with the sale of the building.
Delivery notes		**2 years** after end of financial year to which they relate	
Drawings, plans and buildings (architect signed, not copies)		Lifetime of the building to which they relate	
Engineering works, plans and building records		Lifetime of the building to which they relate	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Equipment records of non-fixed equipment, including specification, test records, maintenance records and logs		**11 years**	If the records relate to vehicles (ambulances, responder cars, fleet vehicles etc) and where the vehicle no longer exists, providing there is a record that it was scrapped, the records can be destroyed.
Inspection reports eg boilers, lifts		Lifetime of installation	If there is any measurable risk of a liability in respect of installations beyond their operational lives, the records should be retained indefinitely.
Inventories of furniture, medical and surgical equipment not held on store charge and with a minimum life of 5 years Inventories of plant and permanent or fixed equipment		Keep until next inventory **5 years** after date of inventory	
Leases, the grant of leases, licences and other rights over property		Period of the lease plus 12 years	
Photographs of buildings		**30 years**	
Plans, building (as built)		Lifetime of building	May have historical value.
Purchase Orders – see 'Approval Files' above			
Stock control reports -		18 months	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Stores records: Major (eg stores ledgers) Minor eg requisitions, issue notes, transfer vouchers, goods received books		**6 years** **18 months**	
Structure plans, organisational charts i.e. the structure of the building plans		Lifetime of building	
Supplies records eg invitations to tender and inadmissible tenders, routine papers relating to catering and demands for furniture, equipment, stationery and other supplies		**18 months**	
Surveys, building and engineering works		Lifetime of building or installation	
Tenders / Purchase Orders / Quotations: Successful Unsuccessful		 Tender period plus 6 year limitation period **6 years**	
Financial / Accounting records:			
Accounts, annual (final, one set only)		**30 years**	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Accounts, minor records; pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques, accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt books, income records, laundry lists and receipts		**2 years** from completion of audit	
Accounts, working papers		**3 years** from completion of audit	
Advice notes, payment		**18 months**	
Audit reports, internal and external including management letters, value for money reports and system/final accounts memoranda		**2 years** after formal completion by statutory auditor	
Bank statements		**2 years** from completion of audit	
Banks Automated Clearing System (BACS) records		**6 years** after year end	
Bills, receipts and cleared cheques		**6 years**	
Budgets including working papers, reports, virements and journals		**2 years** from completion of audit	
Cash sheets		**6 years** after end of financial year to which they relate	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Estimates, including supporting calculations and statistics		**3 years** after end of financial year to which they relate	
Expense claims, including travel and subsistence claims, and claims and authorisations		**6 years** after end of financial year to which they relate	
Fraud case files/investigations		**6 years**	
Fraud national proactive exercises		**3 years**	
Invoices, capital paid invoices, cash books		**6 years** after end of financial year to which they relate	
PAYE records		**6 years** after termination of employment	
Payments		**6 years** after year end	
Payroll list of staff in the pay of the organisation		**6 years** after termination of employment	Destroy under confidential conditions. For superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age.
Receipts		**6 years** after end of financial year to which they relate	

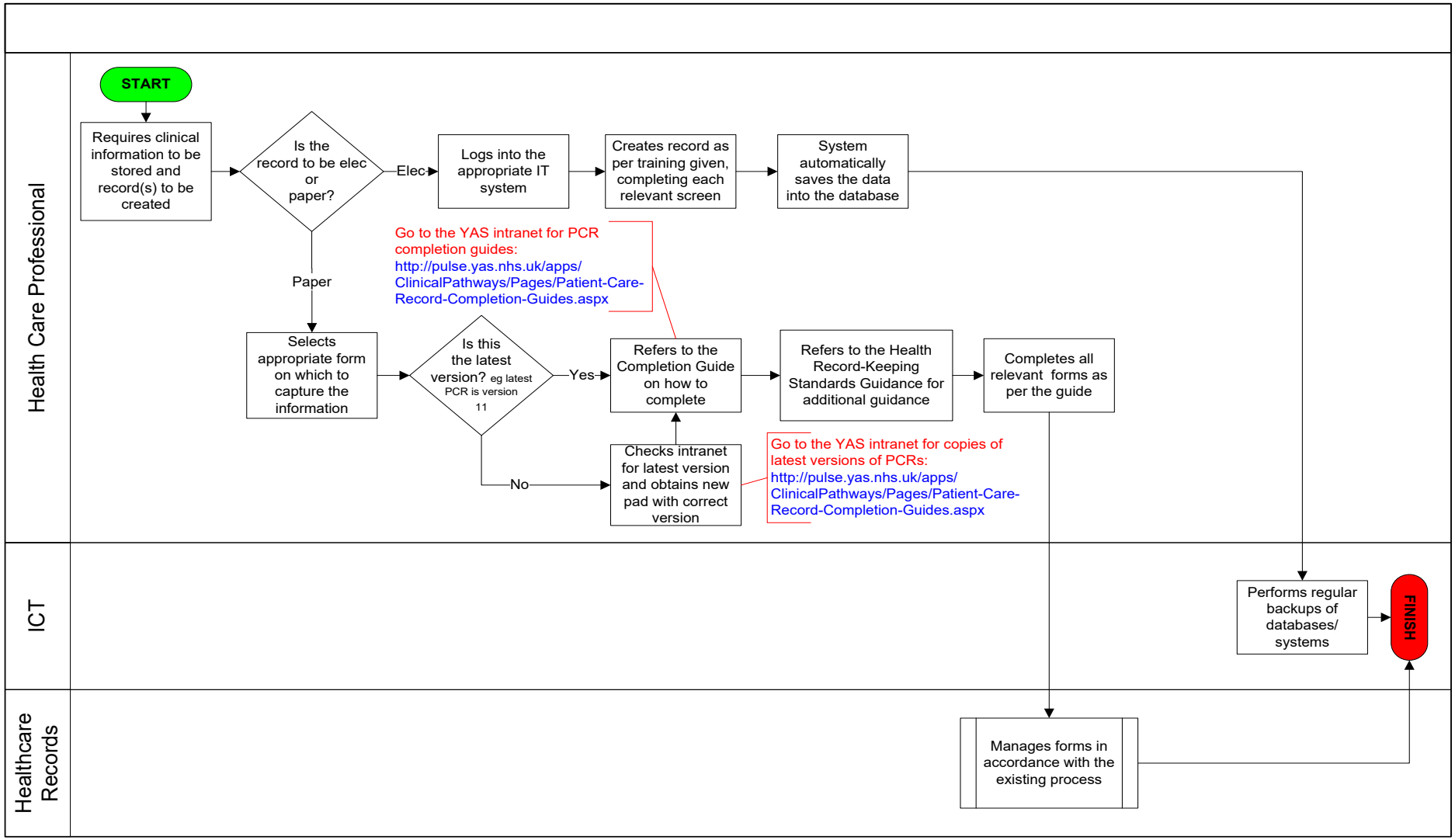
Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Salaries		See 'Wages / salaries'	
Superannuation accounts and registers		**10 years**	
Tax forms		**6 years**	
Transport (staff pool car documentation)		**3 years** unless litigation ensues	
VAT records		**6 years** after end of financial year to which they relate	
Wages / salaries		**10 years**	
Human Resources / Personnel records:			
CVs for non-executive directors: Successful applicants Unsuccessful applicants		 **5 years** following term of office **2 years**	
Industrial relations, not routine staff matters, including industrial tribunals		**10 years**	
Job advertisements - 1 year		**1 year**	
Job applications: Successful Unsuccessful		 **3 years** following termination of employment **1 year**	
Job descriptions		**3 years**	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Leavers' dossiers		**6 years** after individual has left **Summary to be retained until individual's 75th birthday** (or until 6 years after cessation of employment if aged over 70 years at the time) – see notes.	The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training Plans. The 6 year retention period is to take into account any ET claims, or EL claims that may arise after the employee leaves NHS employment, requests for information from the NHS pensions agency etc. Claims of this nature can include periods of up to 6 years or more, prior to the claim and where evidence could be needed from a number of sources, it is appropriate to retain as much as possible from the original file.
Letters of appointment		**6 years** after employment has terminated or until 70th birthday, whichever is later.	
Pension Forms (all)		**7 years**	

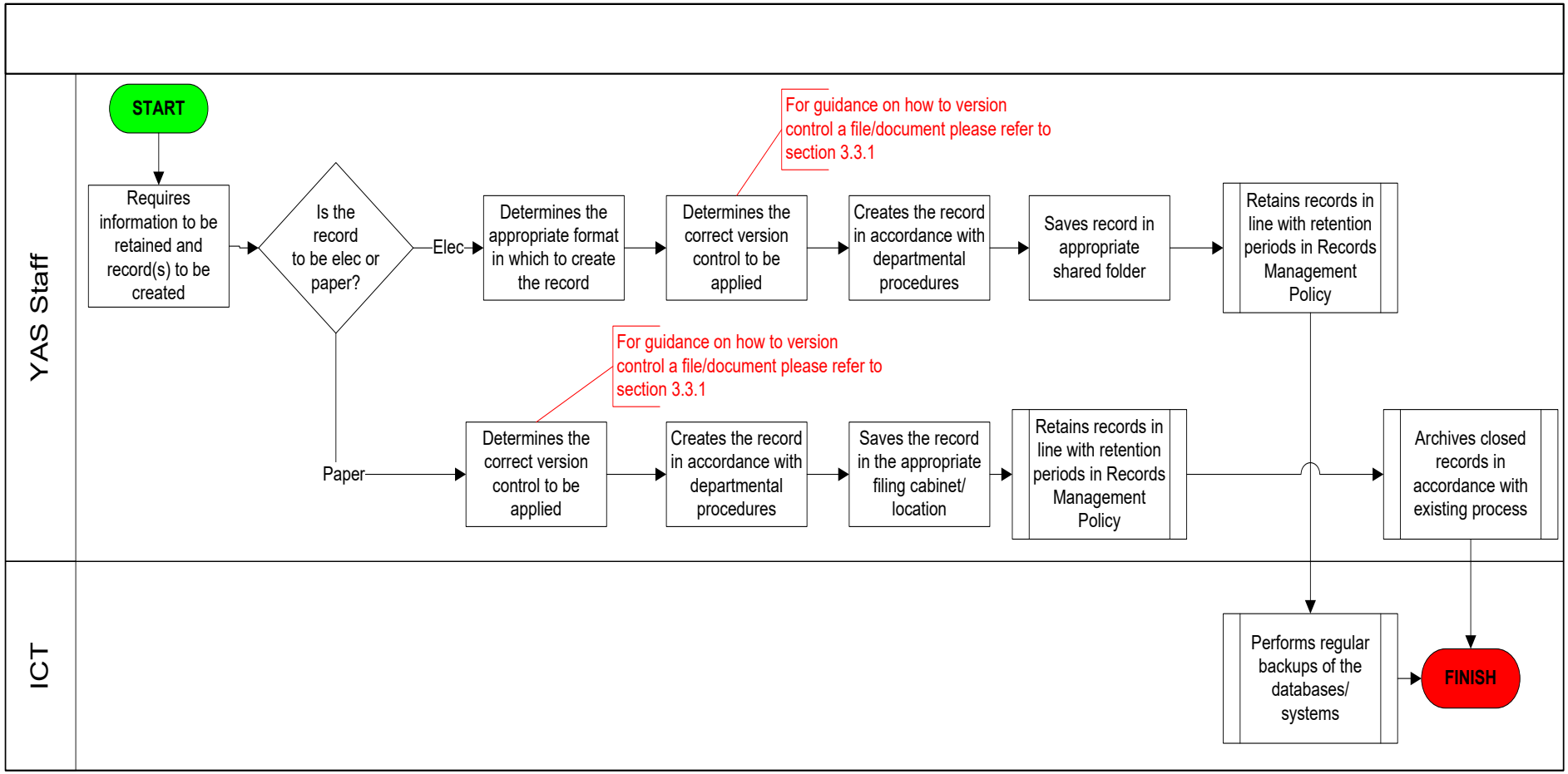
Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Personnel / human resources records, major, eg personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained))		**6 years** after individual has left **Summary to be retained until individual's 75th birthday** (or until 6 years after cessation of employment if aged over 70 years at the time) – see notes in the DOH guidance column	The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training Plans. The 6 year retention period is to take into account any ET claims, or EL claims that may arise after the employee leaves NHS employment, requests for information from the NHS pensions agency etc. Claims of this nature can include periods of up to 6 years or more, prior to the claim and where evidence could be needed from a number of sources, it is appropriate to retain as much as possible from the original file.
Personnel / human resources, minor, eg attendance books, annual leave records, duty rosters i.e. duty rosters held on the individual's record not the organisation or departmental rosters, clock cards, timesheets (relating to individual staff members)		**2 years** after the year to which they relate	
Staff car parking permits		**3 years**	
Study leave applications		**5 years**	
Timesheets (for individual members of staff)		**2 years** after the year to which they relate	

Record Type *(in alphabetical order)*	**Example(s)**	**YAS Retention Period** *(from the date of creation unless otherwise stated)*	**Notes**
Training plans		**2 years**	

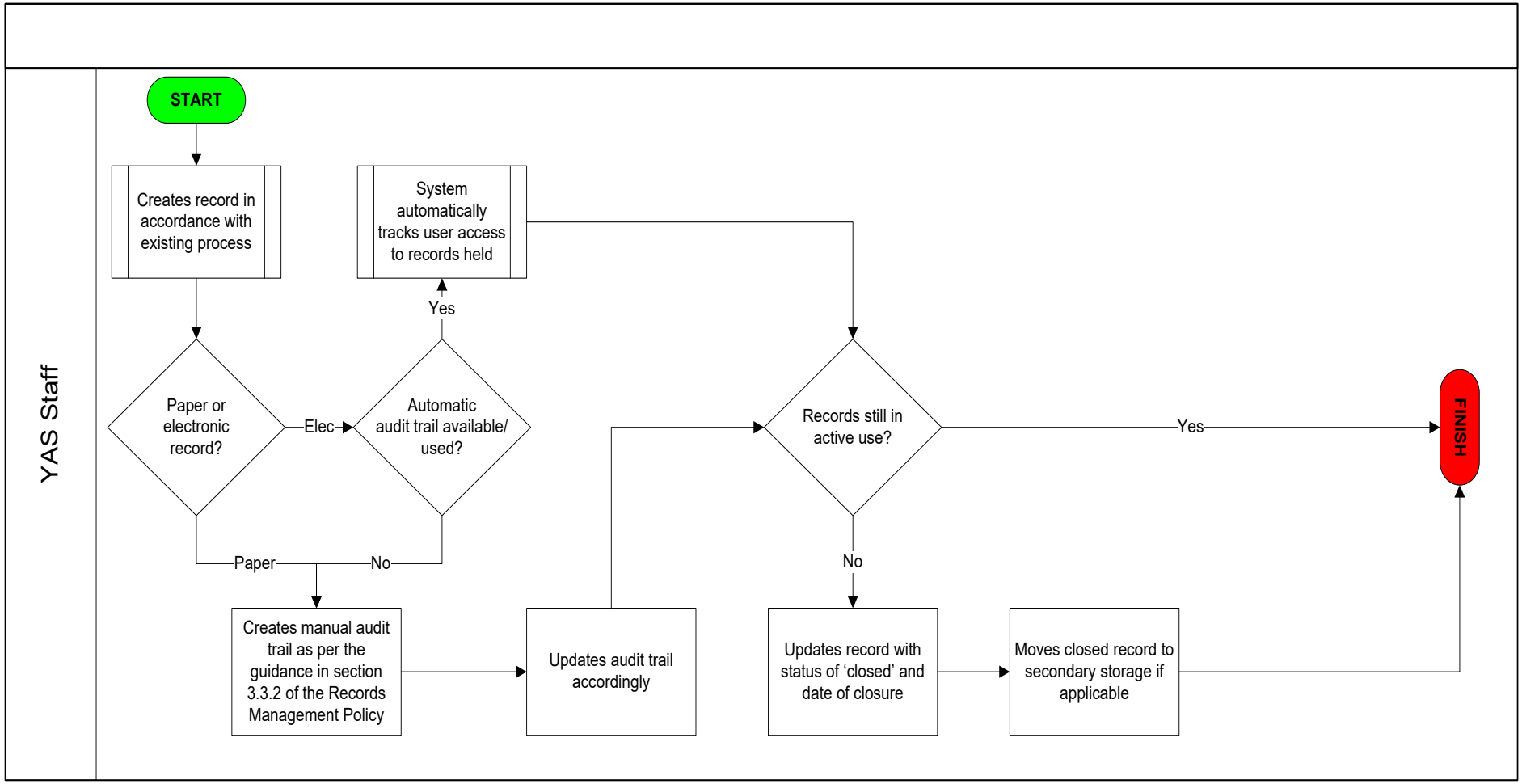
Appendix D Process Flow: Step by Step Guide to Creating Clinical Records



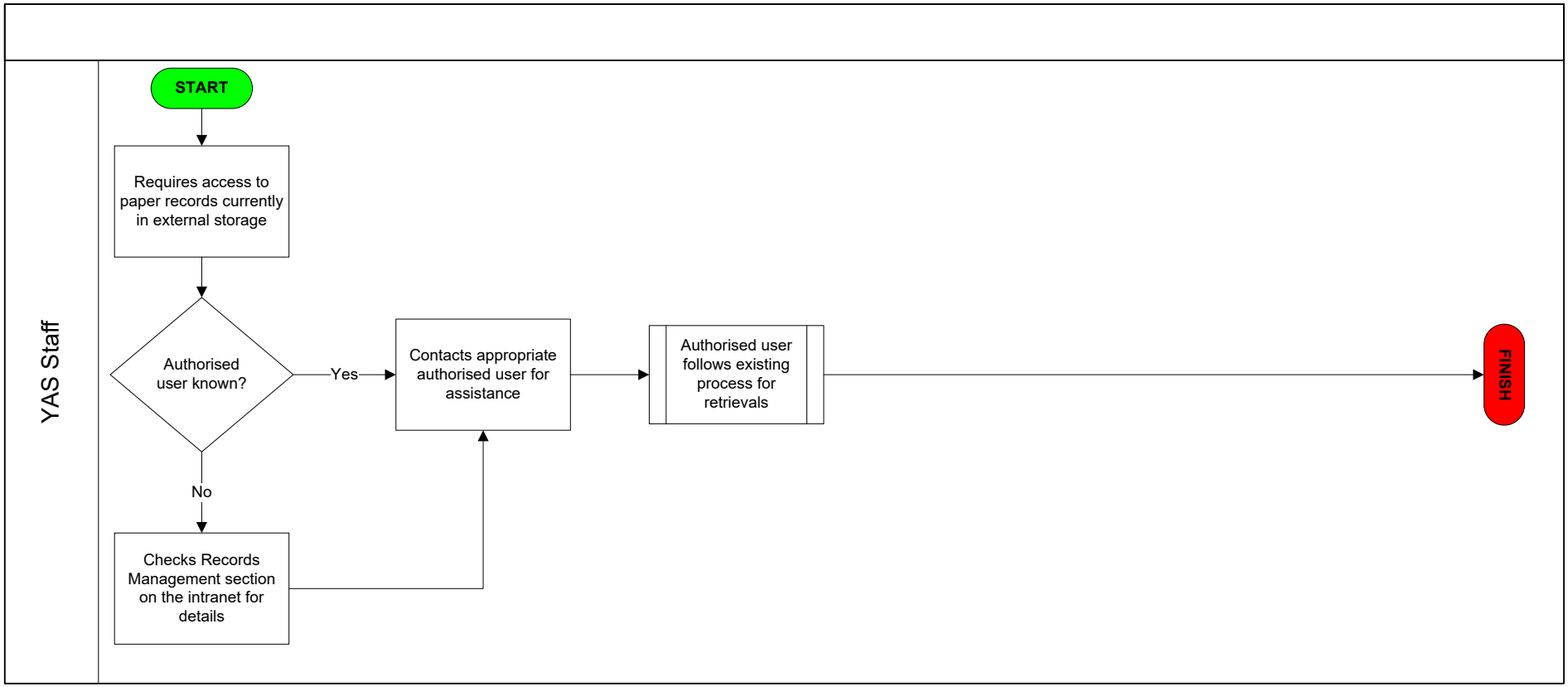
Appendix E Process Flow: Step by Step Guide to Creating Corporate Records



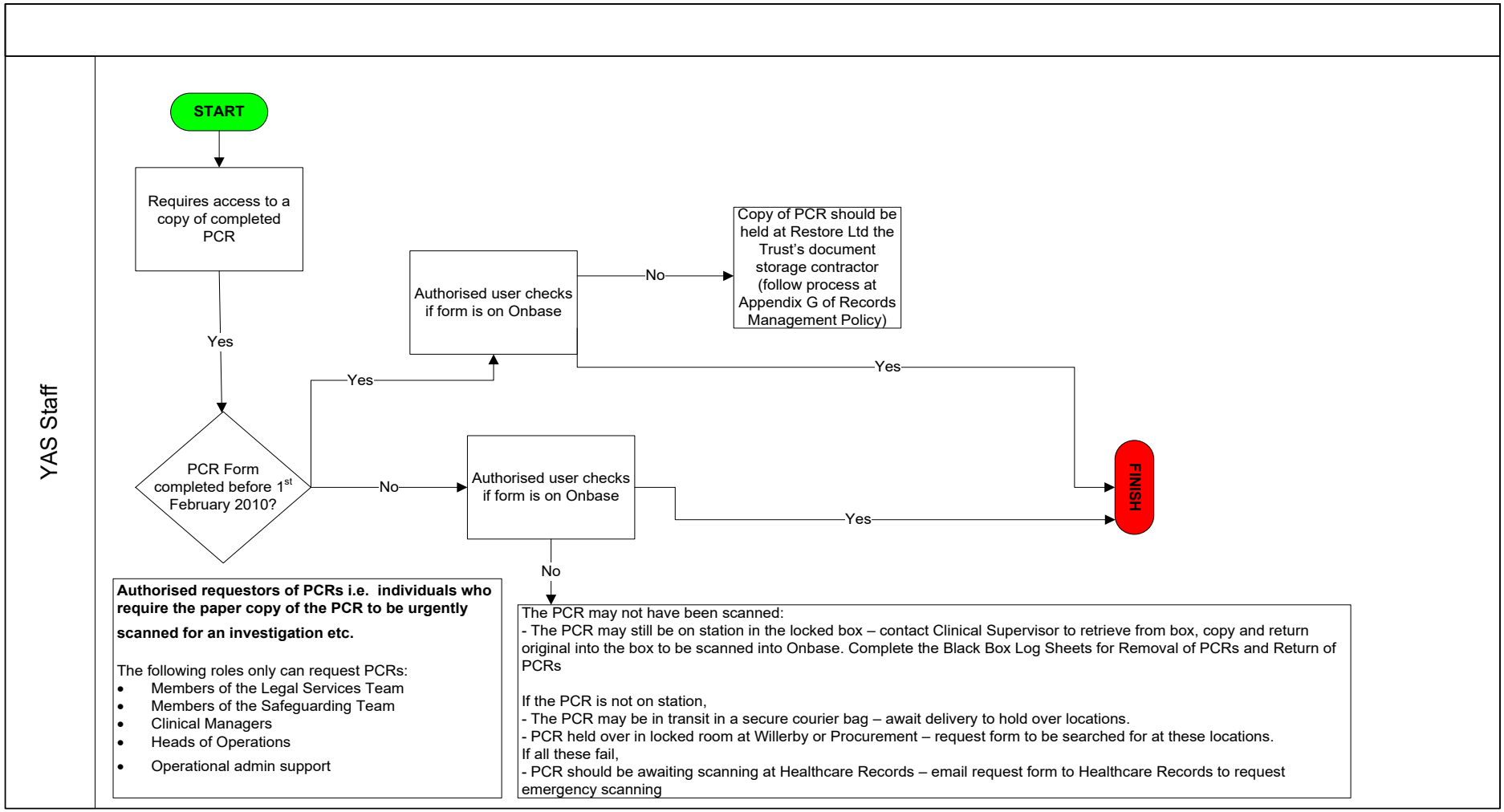
Appendix F Process Flow: Tracking Records



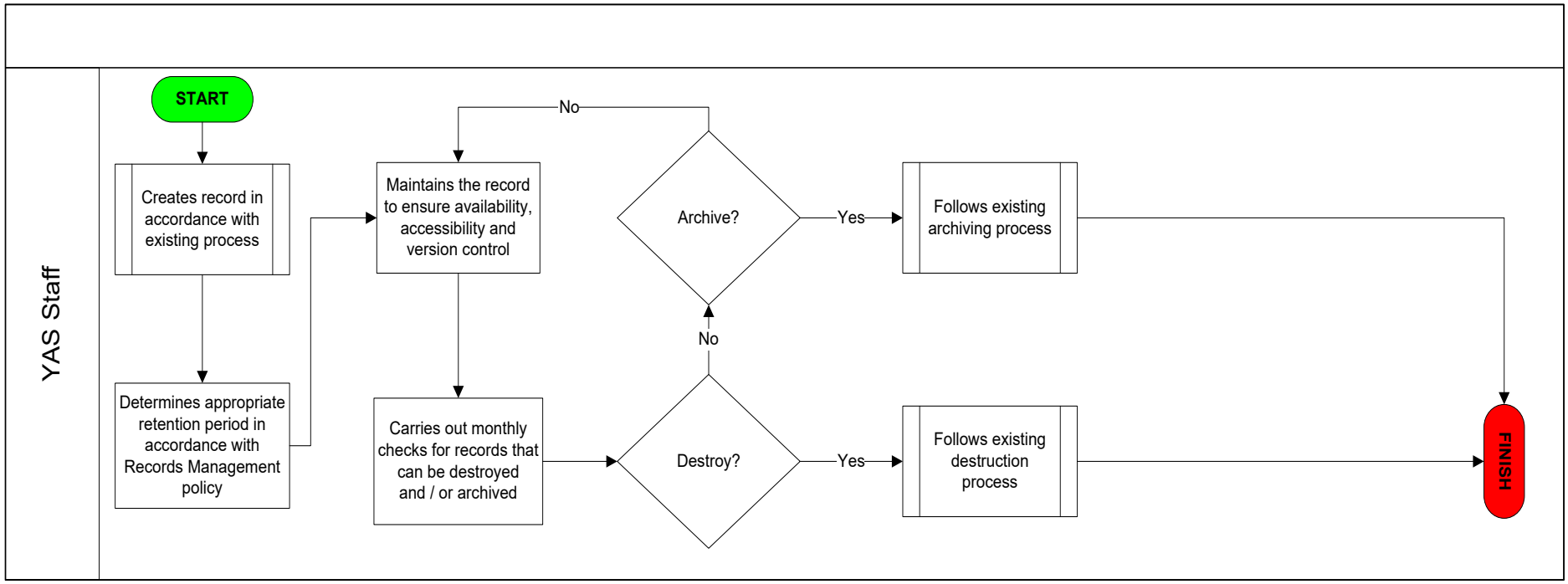
Appendix G Process Flow: Retrieving Archived Paper Records in Storage



Appendix H Process Flow: Retrieving Paper Patient Care Record Forms



Appendix I Process Flow: Retaining Records



Appendix J Process Flow: Step by Step Guide to Disposing of Records