East of England Ambulance Service NHS Trust

Records Management Policy and Procedures

Document Reference	POL0005
Document Status	Approved
Version:	V7.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author**
Internal Audit & update of Records Management: NHS Code of Practice (Department of Health; January 2009)	October 2008	As part of recommendations forming action plan Previous joint Risk Management Strategy and Policy to be **replaced** by separate documents following audit and update of Records Management: NHS Code of Practice (updated January 2009)
	31 March 2009	Natalie Mudge and Anna Price
Version	**Date**	**Comments (i.e. viewed, or reviewed, amended approved by person or committee)**
V1.0	September 2009	Approved by Trust Board
V2.0	December 2009	Minimum changes made to retention schedule
V3.0	15 August 2011	Executive Management Team
V4.0	December 2014	Review date extension approved by EMB

V5.0	December 2015	Review date extension approved by ELB
V6.0	17 November 2016	Approved by ELB
V6.1	14 February 2017	Reviewed by IGG Manager following BDO Internal Audit
V7.0	14 March 2017	Approved by ELB

Document Reference	Records Management Code of Practice for Health and Social Care 2016
Recommended at Date	Information Governance Group 14 February 2017
Approved at Date	Executive Leadership Board 14 March 2017
Review date of approved document	13 March 2019
Equality Analysis	Completed
Linked procedural documents	Risk Management Strategy Patient Care Record Policy Records Management Framework & Guidelines
Dissemination requirements	All managers and staff via email and intranet. To be published on the Trust's public web site
Checklist completed?	Yes
Part of Trust's publication scheme	No

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

1. Introduction

The ISO standard, ISO 15489-1:2016 Information and documentation - Records management [8] defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of businesses. ISO 15489-1:2016 applies to the creation, capture and management of records regardless of structure or form, in all types of business and technological environments, over a period of time.

The importance of sound records management is outlined in The Records Management Code of Practice for Health and Social Care 2016. This document is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice and has been endorsed by the Information Governance Group as best practice and will be utilised in the development of this records management policy and procedures.

The East of England Ambulance Service NHS Trust's (EEAST) 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 EEAST 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.

The Board has adopted this Records Management Policy and Procedures document as it has determined that the organisational benefits of doing so include:

- better use of physical and server space;
- better use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduced costs.
- Improved use of environmental resources
- Improved governance arrangements around trust records

2. Purpose

This policy relates to all records held in any format by the Trust.

3. Duties

3.1 Chief Executive

The Chief Executive, as accountable officer, has overall responsibility for records management in EEAST. Records management is key to service delivery and continuity as it will ensure appropriate, accurate information is available when required.

3.2 Caldicott Guardian

The Caldicott Guardian is responsible for reflecting patients' interests regarding the use of patient identifiable information and ensuring patient identifiable information is shared in an appropriate and secure manner. At EEAST the nominated Caldicott Guardian is the Medical Director

3.3 Director of Nursing & Clinical Quality

The Director of Nursing & Clinical Quality is responsible for reporting to the Board on any records management issues.

3.5 Quality and Risk Assurance Committee (QRAC)

The Quality and Risk Assurance Committee (QRAC) has designated Trust Board responsibility, amongst others:

- To review, monitor and challenge the approved risk management framework to ensure that Trust policies, systems and processes are effective in the management of all risks within the Trust and escalate risk management issues to the Audit Committee and/or to the Trust Board as necessary.
- To ensure effective management, accountability, compliance and assurance for all aspects of Information Governance.

In order to properly to fulfil its functions and to provide the appropriate audit trail for, e.g., the NHSLA, the Committee shall receive reports and notes of meetings from organisation groups established to review and manage risk and governance issues as shown in the Risk Management strategy, this includes both the Clinical Quality and Safety Group and the Information Governance Group. Reports will be received at least at the frequency of the meetings held by the organisation groups.

3.6 Information Governance Group

The Information Governance Group (IGG) has responsibility for receiving any breaches of this policy in respect of the inappropriate release or loss of information and for monitoring any action plans implemented as a result.

3.7 Compliance & Standards Lead

The Compliance & Standards Lead is responsible for ensuring that appropriate systems are in place for the effective and secure administration, storage, archiving, retention and destruction of all records.

3.8 Information Governance Manager

The Information Governance Manager has designated responsibility for records management and to ensure that the appropriate systems are monitored and audited as required.

3.9 Corporate Records Manager/FoI Officer/FoI Officer

The Corporate Records Manager/FoI Officer is responsible for ensuring that this policy is implemented and that the records management system and processes are developed, co-ordinated and monitored.

3.10 Registration Authority (RA) Manager

EEAST must ensure access to all NHS Care Records Service compliant applications (Webviewer, ESR, SCR, etc.) and records is strictly controlled and managed in order to comply with the confidentiality requirements as detailed within the NHS Care Records Guarantee. The RA Manager is responsible, on behalf of the Trust, for ensuring that the National Registration policy and processes underpinning the NHS Care Records Guarantee are adhered to and that any local processes support the National policy and processes.

3.11 Clinical Records Manager/FoI Officer

The Clinical Records Manager/FoI Officer has responsibility for the scanning and safe destruction of paper PCRs when they are received at the locality.

3.12 Information Governance Team

The Information Governance team has responsibility for the safe archiving, retention and storage of all records and for their safe destruction in line with relevant guidance and legislation.

3.13 All Staff

All staff who create, receive and use records have records management responsibilities. In particular, ensuring that they keep appropriate records of their work at EEAST and manage those records in keeping with this policy, established information security and governance best practices, and with any further guidance subsequently produced.

3.11 Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. EEAST will take action 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 Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.

and any new legislation affecting records management as it arises.

3.12 Consultation and Communications with Stakeholders

EEAST is committed to involving staff and key stakeholders in the development, review and monitoring of key procedural documents. As such, relevant stakeholders have been consulted to ensure that their views have been taken on board in the development of this document.

4. Definitions

4.1 Records Management

The key components of records management are:

- record creation;
- record keeping (records library including file name, file category/structure, reference;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.

4.2 Records Creation / Records Life Cycle

All records are created primarily to capture information for evidence of patient and business activity. Creating a record is one of the most important processes in records management. Of equal importance is the need to Name the record and be able to reference the record for easy retrieval. The term Records Life Cycle describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation. Created records in the Trust are approved through the appropriate governance arrangements and are stored in the Trust's "Document Library" on East 24. Each record is determined by whether it is A Strategy, A Policy, or a Standing Operational Procedure. All documents are classified. This means the classification given to a particular information asset will determine how it should be protected and who should be given access to it. The Trust uses the classification codes listed in the NHS Information Governance Guidance for the classification marking of NHS Information. Refer to the Trust's Information Classification Policy for more detail. All Trust documents created should be written in a corporate records common format. The Policy for the Development of Procedural Documents will describe in detail the difference between a strategy and policy, the referencing to be applied and the version control of a document.

4.3 Record Keeping / Filing Reference

In this policy, Records are defined as 'recorded information, in any form, created or received and maintained by EEAST in the transaction of its business or conduct of affairs and kept as evidence of such activity'. The records management landscape is changing. With the rise of digital content, and our increasing reliance on it, changes to the way the Trust manages its records are inevitable. The question is how to manage these changes. Help is on its way with the newly published ISO 15489-1. ISO 15489-1 establishes the core concepts and principles for the design, implementation and management of policy, information systems and processes allowing people, organisations, governments, private enterprises and collaborative coalitions to:

- Create and capture records to meet requirements for evidence of business activity
- Take appropriate action to protect the authenticity, reliability, integrity and usability of records, as well as their business context, and to identify requirements for their management over time.

All documents stored in the document library on East 24 are filed by category. For example Human resources, Operations, Emergency Operations Control, Corporate, Clinical, Supplies, Medical Devices, Patient Transport services. For example ; the filing reference for the Emergency Operations Control is EOC01 for the Clinical documents it is CSOP01 and for the Corporate and Human Resources category it is by alphabetical order. This records management system allows to track and trace all Trust records.

4.4 Information

Information is a corporate asset. Records are important sources of administrative, evidential and historical information.

4.5 Safe Haven

The term 'Safe Haven' describes an agreed set of procedures to ensure the safe and secure handling of confidential information. It can also be considered to be a location within the organisation where confidential information is both received and stored in a secure manner. Safe haven procedures should be in place in any location where confidential information is being received, held or communicated, especially information of a sensitive nature.

4.6 Personal Information

Personal information is any information which can be used to identify a person, either on its own or in combination with other information. Example of personal information are name, address, postcode, sex, date of birth, occupation, other significant dates (e.g. dates of diagnosis), telephone numbers, email addresses, National Insurance number, NHS number, driving licence number, etc.

4.7 Sensitive Information

Sensitive information is defined as any information which an individual would not want disclosed without their prior knowledge and consent. Examples of sensitive information such as health or physical condition (e.g. PCRs and medical records), sexual orientation, ethnic origin, religious beliefs, political views, criminal convictions, trade union membership, etc.

4.8 Corporate Information

Corporate information relating to EEAST business may or may not be confidential in its nature. Some information (such as financial accounts and board minutes) are considered to be publicly-disclosable and are available via the Freedom of Information Act and the EEAST website publication scheme. Other information is more confidential in its nature and its disclosure may be restricted.

Staff should take particular care when disclosing corporate information. If in any doubt staff should check first with their line manager, the Caldicott Guardian or Head of Information Governance.

5. Document Development

5.1 Identification of Stakeholders

The stakeholders for this Policy and Procedures document are all staff who create, receive, retain, archive or dispose of records.

5.2 Responsibility for Document's Development

The Corporate Records Manager/FoI Officer/FoI Officer is responsible for the development and review of this document; recommending responsibility lies with the Information Governance Group.

6. Aims of our Records Management System

The aims of our Records Management System are to ensure that:

- **records are available when needed** - to ensure EEAST has all relevant information to hand as and when required;
- **records can be accessed** - records can be located easily, and that the current version is identified where multiple versions exist;
- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **records can be trusted** – the record's integrity and authenticity can be demonstrated;
- **records can be maintained through time** – the records is available and accessible throughout its lifecycle.

- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;

- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and

- **staff are trained** - so all staff are aware of their responsibilities for record-keeping and record management.

7. Managing Records Retained On-site

All staff must manage any records they create or receive as part of their role at EEAST. Records must be easily retrievable and securely retained for as long as required in line with the Record Retention Schedule (see Appendix G).

The following are some guidelines for effectively managing your records in-house:

- Ensure that all files are clearly labelled and organised in a manner that aids retrieval
- Regular appraisal of records ensures that only those which are used regularly and need to be retained in-house are stored onsite. Other documents can either be archived or disposed of as per the retention schedules in Appendix G.
- Duplicates should not be retained
- Documents should be retained in electronic format where possible to reduce the need for physical storage space both on and off-site.

Records should be reviewed regularly and any inactive records, unnecessary duplicates, and/or records that have reached the end of their retention period should be securely destroyed.

8. Retrieval and Archiving

For the retrieval and archiving of records, please refer to Appendices A & B.

9. Retention and Disposal Schedules

All EEAST records must be retained for a minimum period of time for legal, operational, research and safety reasons. The length of time will depend on the type of record and its importance to the business functions.

EEAST has adopted the retention periods set out in the Records Management Code of Practice for Health and Social Care 2016, please see Appendix G.

10. Safe Haven

Safe Haven procedures ensure that all confidential information that enters or leaves EEAST is handled and accessed in a controlled manner, and that the privacy and confidentiality of personal information is maintained.

Any area or department that routinely handles confidential person-identifiable information must follow the safe haven procedures below.

10.1 Safe Haven Systems

The following Safe Haven requirements should be in place for any area where physical (e.g. fax or post) confidential or sensitive information is sent or received:

- A room that is either locked or accessible via a coded key pad known only by authorised staff or an office or workspace sited in such a way that only authorised staff can enter that location.
- If sited on the ground floor any windows should be secure and have locks on them
- If a securely locked room is not available then fax machines should be kept in a lockable cupboard accessible by authorised staff only
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records containing person-identifiable information should be stored in a secure area accessible by authorised personnel only
- Fax machines must be situated in an office (not corridor) which is locked when unoccupied. Access to the fax machine must be by authorised personnel only.

10.2 Sending a Fax

Fax machines must only be used to transfer personal information where it is absolutely necessary.

Fax machines which are designated as secure Safe Havens should be accessible to approved staff only and be clearly marked as such. An example of a notice to be displayed in Safe Haven areas can be found in Appendix H

When sending a fax, the sender must ensure that it is being sent to the relevant recipient and that the correct fax number is entered.

Before sending the recipient must be made aware that a fax is being sent and they must confirm receipt.

Only the minimum amount of personal information should be sent, if possible this should be anonymised. Personal information should only be sent to a safe haven fax machine.

A Safe Haven fax header must be used which carries a clear confidentiality statement, e.g.:

'The information contained within this fax transmission is intended only for the use of the individual or entity on the transmission sheet. The documents accompanying it contain information from the East o England Ambulance Service NHS Trust that may confidential and privileged. If you are not the intended recipient, you are hereby notified that any disclosure, copying, dstribution or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this transmission in error please notify us be telephone immediately to arrange for the return of the documents.'

10.3 Receiving Faxes

No received faxes should be left unattended at the fax machine and access to the machine should be limited to authorised personnel only.

The contents must not be disclosed to any other parties without the sender's permission.

If the fax is not acknowledged by the recipient, they must be contacted as soon as possible.

10.4 Incoming and Outgoing Letter Mail

When transferring information by mail, the following procedures should be followed:

Check the name, department and address of the intended recipient.

Outgoing mail should be sealed securely and marked "Private and confidential, to be opened by addressee only".

Ensure that a return address is recorded on the outside of the envelope and a compliment slip with the sender's details is contained in the envelope to allow safe return in the event of loss or damage to the package/envelope.

Where possible, send a photocopy of the information, rather than originals.

If the information is considered to be highly sensitive consider if the item should be sent by courier or registered post.

All incoming mail containing patient or personal information should be opened away from public areas and by the addressee only.

10.5 Sending patient information electronically

Access to computers must be password protected and where personal information is displayed the screens must be positioned in such a way as to prevent anyone overlooking them.

Any personal information received must be stored appropriately on the EEAST network.

Where transferring via an email system use NHS mail (NHS.net). The NHS mail service enables person identifiable information to be securely transmitted from one NHS mail user to another NHS mail user or other secure mail exchanges e.g. pnn.police.uk

Senders must ensure emails are sent to the correct address, marked as 'confidential' where necessary and that an audit trails of those emails sent and received is retained.

Person-identifiable or sensitive information should not be sent electronically via any other route unless there is evidence that the route is secure. Advice should be sought from the Trust's IM&T or IG Teams before sending. Staff should also ensure that the recipient is a registered user of NHS mail (or equivalent secure service) and will be able to receive the information.

Email messages should also contain a corporate warning in the event that they should reach anyone other than the intended recipient e.g.

The information contained in this transmission is confidential. It is intended for the addressee (s) only. If you are not the addressee you should not disclose, copy or circulate the information used in this transmission. Such unauthorised use may be unlawful. If you have received this transmission in error, please notify the sender immediately.

10.6 Telephone

Any request for patient information made during a telephone call should not be disclosed without first confirming the identity of the person requesting the information:

Ask the caller to confirm their name, job title, department and organisation, and the reason for their request.

If in doubt, take a contact number for the requester and call them back when the validity of their request has been confirmed, and that the person has the right to receive the information.

Mobile phones should not be used to communicate personal or sensitive information as they are less secure than land lines. Personal information should not be sent by text message.

If voicemail and answering machines are used by departments, they should be set up so that messages left are recorded silently. Staff should take care when playing back messages so that they are not overheard by unauthorised personnel.

When an answering machine is receiving messages which may be confidential it should be protected by pin number access or in a locked room (when unattended) to prevent unauthorised access.

Return the call only to the person who requested the information

If you have to give patient or personal information over the telephone, be aware of others who may be able to hear your conversation and do not provide more information that is necessary.

Do not leave patient or personal information on an answer phone, unless you are sure that the answer phone is in a safe haven environment.

Ensure that you record your name, the date and time of disclosure, the reason, who authorised disclosure (if authorisation was sought) and the recipient's details in the patient's record.

10.7 Transporting Patient Information

Care should be taken to ensure that patient information is only taken off site when absolutely necessary. When selecting the most suitable delivery option for documents it is important to pay strict attention to the information classification level and to any possible security risk. See the Trust's Confidentiality Code of Conduct and Information Classification Policy for further information.
If information is taken off site:

Record what information is being taken off site, the reason why, and where or to whom it is being taken.

The information must be transported in a secure manner.

The information should not be left unattended or be made available to any unauthorised person.

The information should be returned as soon as possible and the return should be recorded.

Where the bulk transfer of personally identifiable information is required, special precautions should be agreed by the IM&T and IG Teams prior to transfer. All portable media must be encrypted to approved NHS standards and sent by secure courier.

Where the transfer is internal (i.e. between different sites and departments) then transport should be via an individual member of staff where possible. Containers should be 'tamper evidenced', i.e. it should be possible to tell if a seal has been broken in transit.

All transfers of personally identifiable information should be marked confidential and should have a return address on the outside in the event of non-delivery. They should be clearly addressed, preferably to a named person.

10.8 Manual Records

Manual Records containing patient or personal information must be kept in a secure environment and securely locked away when unattended.

Patient records must be kept face-down when in public areas, and not left unattended.

10.9 Notice Boards

Patient and personal information should not be displayed on notice boards.

10.10 Record Keeping

All losses or unauthorised releases of information must be recorded on the Datix Risk Management System in line with the Trust's risk management procedures.

11. Equality Analysis

An Equality Analysis has been undertaken for this document, see Appendix L.

12. Dissemination and Implementation

12.1 Dissemination

This document will be stored in the online Document Library for all Trust staff to access; it will also be publicised using relevant EEAST internal publications.

12.2 Implementation

All staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance as defined within the Training Needs Analysis contained within the EEAST Learning & Development policy.

13. Process for Monitoring Compliance and Effectiveness

EEAST will monitor this policy for compliance through various streams (see Appendix K).

EEAST will also consider the risks of Records Management within its Internal Audit Programme and if appropriate will add to the annual programme for auditing.

The results of any audits undertaken in relation to Records Management will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and Risk Assurance Committee. Any areas of high risk will be identified to the Risk Management Committee.

14. Standards/Key Performance Indicators

Details of the standards and KPIs are included in Appendix K.

15. References

Records Management: NHS Code of Practice (updated January 2009)

Public Records Act 1958

Data Protection Act 1998

Freedom of Information Act 2000

16. Associated Documents

Records Management Framework and Guidelines

Appendices

Appendix A – Patient Records Management Procedures

Archiving

Locality offices

Upon receipt of paper Patient Care Records (PCRs) from stations, the nominated staff at the three locality offices will:

- record the date PCRs are received,
- the ambulance base or officer they came from.

Any stations submitting paper PCRs that exceed the 14 day standard will be contacted by the relevant locality office and the Clinical Records Manager/FoI Officer notified of any outcomes.

Operational management should receive reports from Area Offices of any weeks PCRs have not been received and of any re-occurring late or inappropriate arrivals.

The records will be prepared and scanned within the relevant locality secure storage area. This area must be kept locked at all times and is restricted to nominated staff only.

The originals of scanned PCRs will be held within the secure area for one week post scanning before being placed in the blue 'confidential waste' shredding bins. These bins will be emptied by the contracted secure waste disposal company.

It is extremely important to note that each box of records sent to offsite storage has cost implications, for processing the record/collection, storage for the agreed retention period, and retrieval (if necessary).

Retrieval – Single Patient Care Records

Internal archiving

For those instances when the PCR is currently stored at the locality office:

- Upon receipt of the request form (as contained within the Release of Information Policy) locate the form, photocopy and return it to storage.
- Forward the photocopy to the person making the request.

Under no circumstances should the original be sent.

For those instances where the PCR has been scanned:

- Upon receipt of the request locate the form within the Formic Fusion© database
- Either, email via secure nhs.net or print a hard copy and send to the person making the request

External archiving

Only staff members within the Patient Services team are authorised to request PCRs from the offsite storage provider.

To request a PCR that is stored with the offsite storage provider, the following process must be followed:

- The PCR Request Form (Appendix F) must be completed and emailed to eastsales@boxit.co.uk copying in the Corporate Records Manager/FoI Officer.
- Once the PCR has been located it will scanned to a secure server and a link sent to the requestor. All requestors must have a user name and password from the offsite storage provider in order to be able to view their records on the secure system.
- The requestor will then attach the scanned PCR to the relevant incident in DATIX and will delete the email.

Retrieval from external archiving – Multiple Days

When physical PCRs for an entire day or multiple days are required these must be requested through the Corporate Records Manager/FoI Officer/FoI Officer.

Retention and Destruction of records

Archived PCRs held off-site will be retained for 10 years from the date of the incident in line with the NHS Retention Schedule defined in Appendix G or until they have been retrieved and scanned.

All on-site PCRs and archived PCRs retrieved for back scanning will be retained for one calendar month post scanning and then destroyed by an externally contracted secure company. A central database of all archived documents will be held by Clinical Records.

At the start of each calendar year, the Corporate Records Manager/FoI Officer/FoI Officer will contact both the Medical Director and Director of Nursing & Clinical Quality by email for their agreement for destruction of those patient care records that have reached the end of their retention period.

The destruction certificate will be retained by the Corporate Records Manager/FoI Officer/FoI Officer.

Mitigating Risk

If for any reason there is an identified or suspected incident relating to the archiving, retrieval or destruction of patient care records including: loss, damage or theft, the Corporate Records Manager/ FoI Officer and the Clinical Records Manager/FoI Officer must be contacted immediately. This will also be reported and investigated through the Trust's DATIX Risk Management system.

Appendix B – Corporate Records Management Procedures

New Archive Box Deposits

This section details the process for sending new boxes to archive.

Preparation

- Request flat pack boxes, New Box Deposit Schedule forms and barcode labels from the Corporate Records Manager/FoI Officer
- Ideally only inactive records should be archived; records which are required on a regular basis should be retained in-house for as long as possible.
- Remove and reuse all ring binders and lever arch folders; documents should be bound with filing clips (not paper clips or elastic bands as these rust/perish).
- If file retrieval is required then each file must have an identifying name or number clearly written on it to aid retrieval.

Packing

- All records within a single box must have the same or a similar review date (date of the record plus the retention period for the record type as laid down in the Retention Schedule, Appendix F)
- Only boxes supplied by Box-It should be used to archive records
- Boxes must not be over packed; heavy boxes or those where the lid does not sit flat will not be collected.
- Each new box must have a complete inventory of its contents; this should be entered into the Archive Template (to be requested from the Corporate Records Manager/FoI Officer). A review date **must** be included for each box.
- Each new box must have a unique reference number starting with the department/location code, these codes will be assigned by the Corporate Records Manager/FoI Officer. A central list of numbers for each department in each location must be kept to avoid duplication.
- The unique reference number must be written clearly on the box and nothing else; all other information/details written on the box must be crossed out.
- The number assigned to the box and its review date should be entered into the appropriate fields on the New Box Deposit Schedule form.
- A barcode should then be assigned to each of these new box numbers, and the large barcode label attached to the relevant box. The large barcode must be placed in the top right hand corner on the small side of the box (ensuring that it will not be obscured by the lid). The small barcode label is to be placed next to the appropriate box number on the New Box Deposit Schedule form.

Collection

- A copy of the Archive Template (contents list) should be sent to the Corporate Records Manager/FoI Officer with an email requesting collection.
- The New Box Deposit Schedule should then be copied as the driver will need to take the original with him – both copies must be signed
- The work order supplied by the driver and the signed New Box Deposit Schedule form should then be scanned and sent to the Corporate Records Manager/FoI Officer.
- The Corporate Records Manager/FoI Officer will retain copies of all New Box Deposit Schedules and any work orders, as well as a complete set of the Archiving Templates to show exactly what records we have sent to offsite storage.

It is extremely important to note that each box of records sent to offsite storage has cost implications, for processing the record/collection, storage for the agreed retention period, and retrieval (if necessary).

Retrievals

To request a record from storage:

- To retrieve a **box** of records from storage please email the Corporate Records Manager/FoI Officer with the box number of the box you require; the Box-it barcode or the number assigned to it by the Trust can be used.
- To retrieve a **file** of records from storage please email the Corporate Records Manager/FoI Officer with the name/number of the file and the number of the box it is in.
- To receive a **scan back** (an electronic scanned image) of a document held in offsite storage, please email the Corporate Records Manager/FoI Officer.

The work order supplied by the driver should then be scanned and sent to the Corporate Records Manager/FoI Officer.

A database of all requests and retrievals is held by the Corporate Records Manager/FoI Officer.

Returns

To return physical records to storage please email the Corporate Records Manager/FoI Officer stating:

- the number of boxes or files you wish to have collected with either the relevant barcode(s) or unique number(s) and
- that these are returns and not new boxes.

Following collection the workorder must be scanned and emailed to the Corporate Records Manager/FoI Officer.

Review date

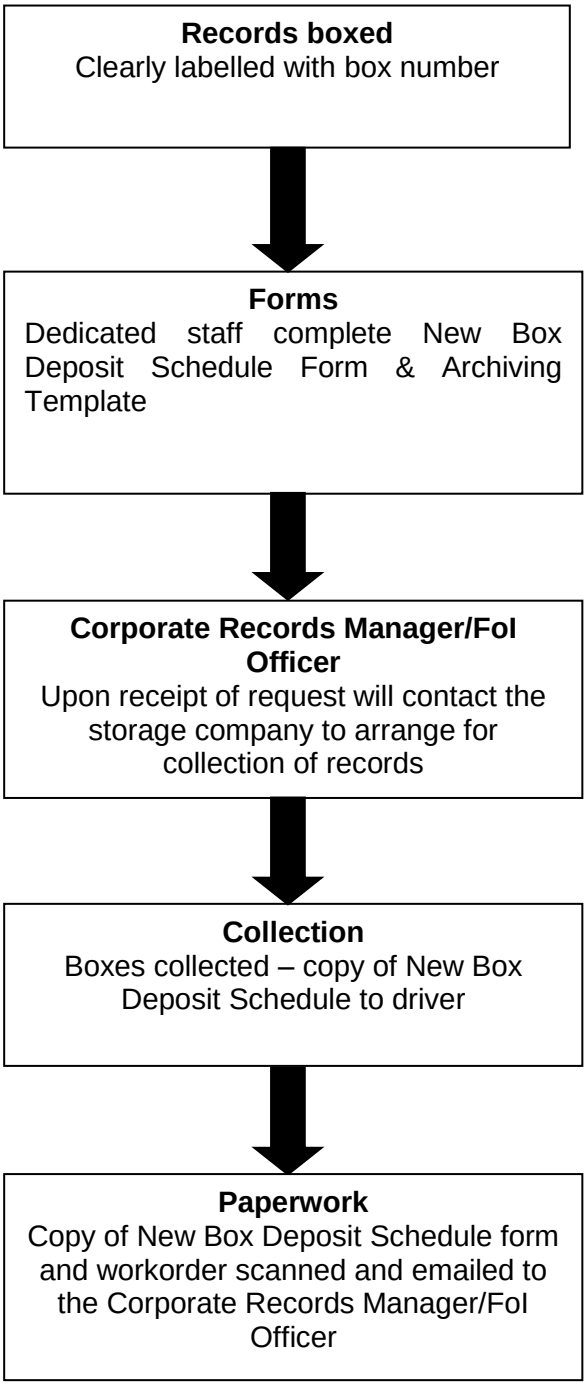
When a box reaches, or is close to, its review date, you will be contacted to ask if you would like to review the box contents and/or approve destruction of the contents. If the contents are to be retained beyond the retention period as laid out in the Retention Schedule (Appendix G) then this must be outlined in an email to the Corporate Records Manager/FoI Officer.

Please note: if you wish to recall the box for inspection you will incur the cost of retrieving the box and then returning it to storage for destruction.

Mitigating Risk

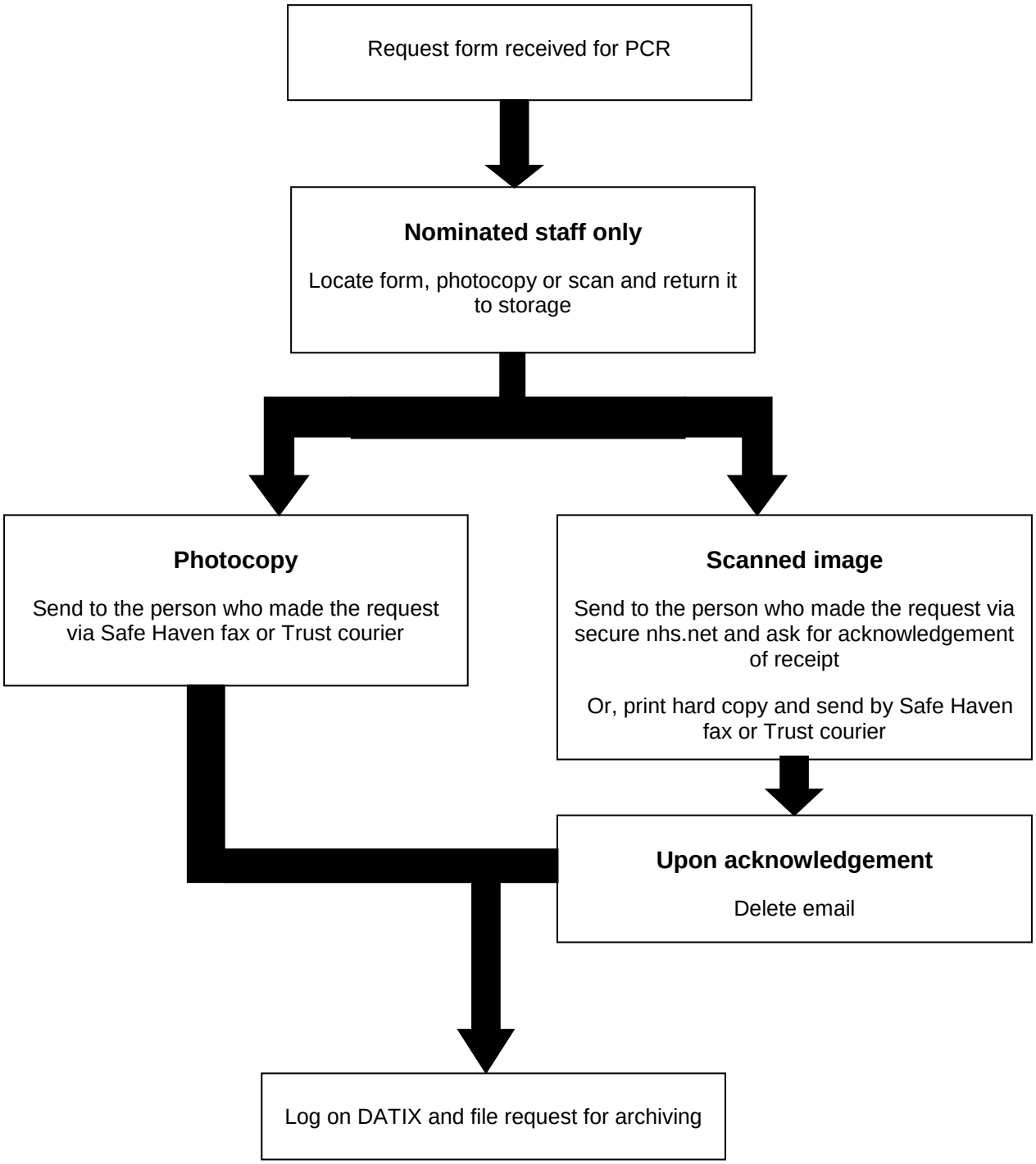
If for any reason there is an identified or suspected incident relating to the archiving, retrieval or destruction of records including: loss, damage or theft, the Corporate Records Manager/FoI Officer must be contacted immediately. This will also be reported and investigated through the Trust's DATIX Risk Management system.

Appendix C - Flow chart for archiving records off-site

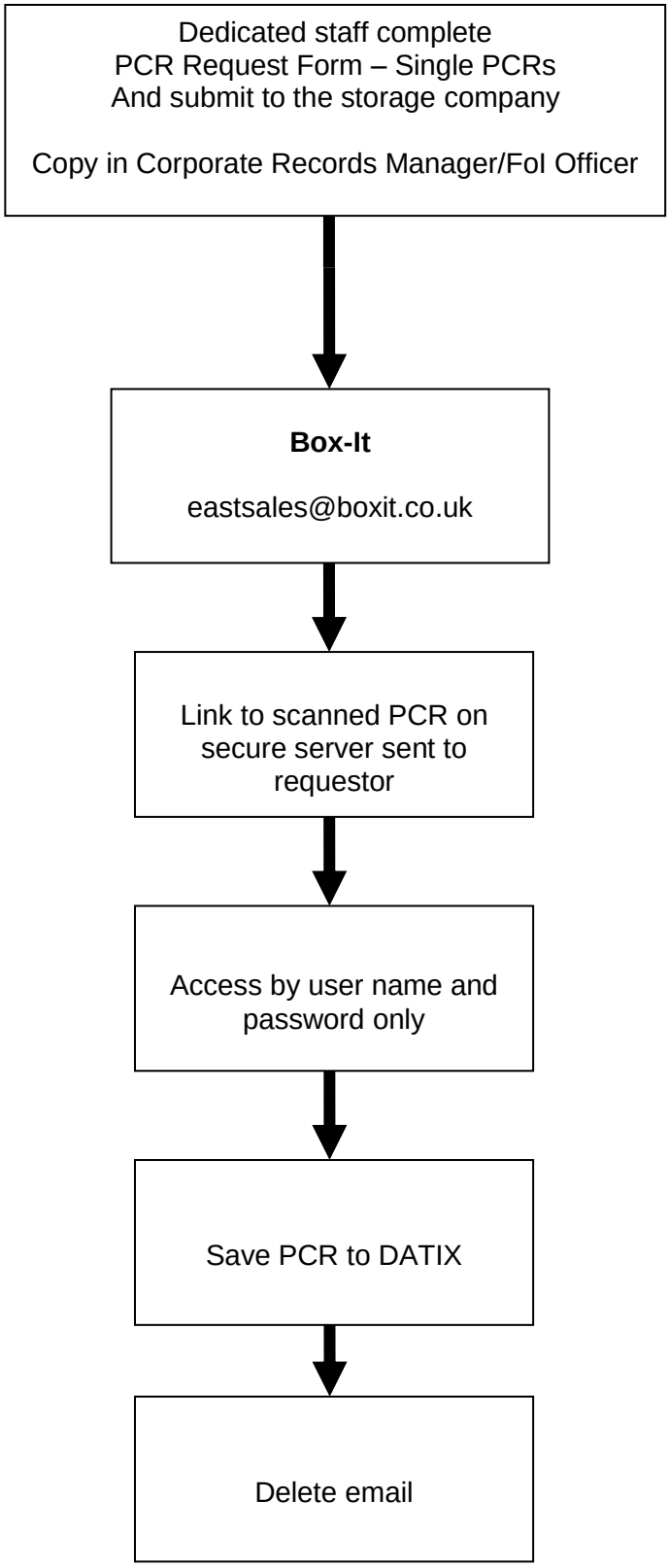


Appendix D - Flow chart for retrieval of PCR stored on-site

UNDER NO CIRUMSTANCES RELEASE THE ORIGINAL PATIENT CARE RECORD



Appendix E - Flow chart for retrieval of single PCR from off-site



Appendix F – PCR Request Form

To be emailed to eastsales@boxit.co.uk

Please ensure you complete the form fully and do not include any patient-identifiable information

Bedford		**Chelmsford**		**Norwich**	

Person making the request	
Position	
Date requested	
Contact number	

DELIVERY Request Form

This form is to be completed for SINGLE RECORDS only

For incidents concerning multiple patients please ensure that you record each patient as a separate request to ensure that all PCRs are located.

Incident number	Date & time of incident	Vehicle / crew details	Location (This must not identify a single residential address – street name and town/city only)

Appendix G Retention Schedule

Care Records with standard retention periods

Record Type	Retention Start	Retention period	Action at end of retention period	Notes
Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review and if no longer needed destroy	Basic health and social care retention period - check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Adult social care records	End of care or client last seen	8 years	Review and if no longer needed destroy	
Children's records including midwifery, health visiting and school nursing	Discharge or patient last seen	25th or 26th birthday (see Notes)	Review and if no longer needed destroy	Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as X-rays and scans as well as video and other formats.
Electronic Patient Records System	See Notes	See Notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.

GP Patient records	Death of Patient	10 years after death see Notes for exceptions	Review and if no longer needed destroy	If a new provider requests the records, these are transferred to the new provider to continue care. If no request to transfer: 1. Where the patient does not come back to the practice and the records are not transferred to a new provider the record must be retained for 100 years unless it is known that they have emigrated 2. Where a patient is known to have emigrated, records may be reviewed and destroyed after 10 years 3. If the patient comes back within the 100 years, the retention reverts to 10 years after death.
Mental Health records	Discharge or patient last seen	20 years or 8 years after the patient has died	Review and if no longer needed destroy	Covers records made where the person has been cared for under the Mental Health Act 1983 as amended by the Mental Health Act 2007. This includes psychology records. Retention solely for any persons who have been sectioned under the Mental Health Act 1983 must be considerably longer than 20 years where the case may be ongoing. Very mild forms of adult mental health treated in a community setting where a full recovery is made may consider treating as an adult records and keep for 8 years after discharge. All must be reviewed prior to destruction taking into account any serious incident retentions.
Obstetric records, maternity records and antenatal and post natal records	Discharge or patient last seen	25 years	Review and if no longer needed destroy	For the purposes of record keeping these records are to be considered as much a record of the child as that of the mother.
Cancer/Oncology - the oncology records of any patient	Diagnosis of Cancer	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of any cancer must be retained in case of future reoccurrence. Where the oncology records are in a main patient file the entire file must be retained. Retention is applicable to primary acute patient record of the cancer diagnosis and treatment only. If this is part of a wider patient record then the entire record may be retained. Any oncology records must be reviewed prior to destruction taking into account any potential long term research value which may require consent or anonymisation of the record.
Medical record of a patient with Creutzfeldt-Jakob Disease (CJD)	Diagnosis	30 Years or 8 years after the patient has died	Review and consider transfer to a Place of Deposit	For the purposes of clinical care the diagnosis records of CJD must be retained. Where the CJD records are in a main patient file the entire file must be retained. All must be reviewed prior to destruction taking into account any serious incident retentions.

Record of long term illness or an illness that may reoccur	Discharge or patient last seen	30 Years or 8 years after the patient has died	Review and if no longer needed destroy	Necessary for continuity of clinical care.The primary record of the illness and course of treatment must be kept of a patient where the illness may reoccur or is a life long illness.
Pharmacy				
Information relating to controlled drugs	Creation	See Notes	Review and if no longer needed destroy	NHS England and NHS BSA guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf The Medicines, Ethics and Practice (MEP) 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/
Event & Transaction Logs				
Clinical Audit	Creation	5 years	Review and if no longer needed destroy	
Chaplaincy records	Creation	2 years	Review and consider transfer to a Place of Deposit	See also Corporate Retention
Clinical Diaries	End of the year to which they relate	2 years	Review and if no longer needed destroy	Diaries of clinical activity & visits must be written up and transferred to the main patient file. If the information is not transferred the diary must be kept for 8 years.
Clinical Protocols	Creation	25 years	Review and consider transfer to a Place of Deposit	Clinical protocols may have archival value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (see Corporate Records).
Datasets released by HSCIC under a data sharing agreement	Date specified in the data sharing agreement	Delete with immediate effect	Delete according to HSCIC instruction	http://www.hscic.gov.uk/media/15729/DARS-Data-Sharing-Agreement/pdf/Data_Sharing_Agreement_2015v2%28restricted_editing%29.pdf

Destruction Certificates or Electronic Metadata destruction stub or record of clinical information held on destroyed physical media	Destruction of record or information	20 Years	Review and consider transfer to a Place of Deposit	Destruction certificates created by public bodies are not covered by an instrument of retention and if a Place of Deposit or the National Archives do not class them as a record of archival importance they are to be destroyed after 20 years.
Equipment maintenance logs	Decommissioning of the equipment	11 years	Review and consider transfer to a Place of Deposit	
Inspection of equipment records	Decommissioning of equipment	11 Years	Review and if no longer needed destroy	
Notifiable disease book	Creation	6 years	Review and if no longer needed destroy	
Telephony Systems & Services (999 phone numbers,111 phone numbers, ambulance, out of hours, single point of contact call centres).				
Recorded conversation which may later be needed for clinical negligence purpose	Creation	3 Years	Review and if no longer needed destroy	The period of time cited by the NHS Litigation Authority is 3 years
Recorded conversation which forms part of the health record	Creation	Store as a health record	Review and if no longer needed destroy	It is advisable to transfer any relevant information into the main record through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record the recording must be considered as part of the record and be retained accordingly.
The telephony systems record(not recorded conversations)	Creation	1 year	Review and if no longer needed destroy	This is the absolute minimum specified to meet the NHS contractual requirement.
Clinical Trials & Research				
Research data sets	End of research	Not more than 20 years	Review and consider transfer to a Place of Deposit	http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf
Corporate Governance				
Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.

Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.
Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings
Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Public Records Act 1958. If records are not excluded by such an instrument they must either be transferred to a place of deposit as a public record or destroyed 20 years after the record has been closed.
Incidents (serious)	Date of Incident	20 Years	Review and consider transfer to a Place of Deposit	
Incidents (not serious)	Date of Incident	10 Years	Review and if no longer needed destroy	
Non-Clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed destroy	
Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	
Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to a Place of Deposit	
Communications				
Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	
Website	Creation	6 years	Review and consider transfer to a Place of Deposit	

Staff Records & Occupational Health				
Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	
Occupational Health Report of Staff member under health surveillance	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	
Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file.	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75th birthday, whichever is sooner, if a summary has been made.
Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see page 36 for an example of a Staff Record Summary used by an organisation.
Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	
Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer2 Statutory and mandatory training records - to be kept for ten years after training completed3Other training records - keep for six years after training completed.

Procurement				
Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Contracts - financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	
Estates				
Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
CCTV		See ICO Code of Practice	Review and if no longer needed destroy	ICO Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.
Equipment monitoring and testing and maintenance work where asbestos is a factor	Completion of monitoring or test	40 years	Review and if no longer needed destroy	
Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed destroy	
Inspection reports	End of lifetime of installation	Lifetime of installation	Review	
Leases	Termination of lease	12 years	Review and if no longer needed destroy	
Minor building works	Completion of work	retain for 6 years	Review and if no longer needed destroy	
Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.

Radioactive Waste	Creation	30 years	Review and if no longer needed destroy	
Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Nynhydrin Test	Date of test	11 years	Review and if no longer needed destroy	
Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to Place of Deposit	
Finance				
Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. Where benefactions endowment trust fund/legacies - permanent retention.
Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	
Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Expenses	Close of financial year	6 years	Review and if no longer needed destroy	
Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible
Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	

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

Appendix H – Example of the notice to be displayed in Safe Havens

This is a Safe Haven Fax - Fax no:

You may send or receive personally identifiable information from here. Please take the following precautions:

Do's

- Do check and double check that you have typed the recipients number correctly.
- Do use pre-programmed numbers where possible.
- Do use an EEAST cover sheet with instructions on it should the fax be received by the wrong person.
- Do print a confirmation sheet for the transmission.
- Do follow Caldicott principles when sending person identifiable information.
- Do use an identifying number instead of personal details if possible.
- Do separate clinical and personal/demographic details if possible.

Do Not's

- Don't send person identifiable information unless you can justify that it is necessary.
- Don't include person identifiable information details on the Cover sheet.

Appendix I – Fax Cover Sheet Template

East of England Ambulance Service NHS Trust

Safe Haven Fax

CONFIDENTIAL

To:	**From:**
Fax:	**Pages:**
Phone:	**Date:**
Re:	**CC:**

☐ **Urgent** ☐ **For Review** ☐ **Please Comment** ☐ **Please Reply** ☐ **Please Recycle**

Message:

The information contained within this fax transmission is intended only for the use of the individual or entity on the transmission sheet. The documents accompanying it contain information from the East o England Ambulance Service NHS Trust that may confidential and privileged. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited. If you have received this transmission in error please notify us be telephone immediately to arrange for the return of the documents.

Appendix J – Checklist

	Title of document being reviewed:	Yes/No/ N/A	Comments
1.	**Purpose**		
	Are the reasons for the development of the Document stated?	Yes	
2.	**Definitions**		
	Have all key terms been clearly defined?	Yes	
3.	**Consultation**		
	Have relevant stakeholders and/or users been consulted with?	Yes	
4.	**Equality Impact Assessment**		
	Has the Trust Equality Impact Assessment Screening Form been completed and attached by the author and approved by the responsible Executive Director?	Yes	
5.	**Monitoring**		
	Has the Monitoring Table been fully completed and attached?	Yes	
6.	**References/Associated Documents**		
	Are key references cited?	Yes	
	Are linked documents identified where appropriate?	Yes	
6.	**Approval**		
	Does the Document identify which committee/group will approve it?	Yes	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Review Date**		
	Is the review date identified?	Yes	

Information Governance Lead (or delegated authority)			
This Procedural Document complies with the Policy for the Development of Procedural Documents			
Name		Date	
Clinical Quality Team			
The Procedural Documents complies with the relevant NHSLA standards			
Name		Date	
Please attach to the procedural document and forward to the relevant committee for approval			

Appendix K – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Duties **Legal and professional obligations**	**Line Managers including Trust Board level**	**Monitored through PDRs**	**Annually**	**PDR forms; identified Training needs submitted to LDU**	**The results will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and Risk Assurance Committee. Any areas of high risk will be identified to the Risk Management Committee.**	**Any required actions identified will be undertaken by the Information Governance Team within the timeframes agreed with the Information Governance Group**	**The Information Governance Team will be responsible for sharing the lessons learnt and any practice changes with all the relevant stakeholders**
	Line Managers including Trust Board level	**As a result of concerns raised following an investigation of a complaint or incident**	**As required**	**Documentation included on Datix Risk Management System**			
Retrieval and archiving	**Corporate Services Manager** **Clinical Quality Manager**	**Monitoring of Release of Information requests** **Monitoring of PCR requests to Archiving company**	**Monthly** **Monthly**	**Documentation included on Datix Risk Management System**	**The results will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and Risk Assurance Committee. Any areas of high risk will be identified to the Risk Management Committee.**	**Any required actions identified will be undertaken by the Information Governance Team within the timeframes agreed with the Information Governance Group**	**The Information Governance Team will be responsible for sharing the lessons learnt and any practice changes with all the relevant stakeholders**
	Line Managers including Trust Board level	**As a result of concerns raised following an investigation of a complaint or incident**	**As required**	**Documentation included on Datix Risk Management System**			
Retention and disposal schedules	**Clinical Quality Manager (Patient Care Records)** **Information Governance Team**	**Review of archiving databases**	**Annually**	**Emails** **Minutes: Meetings** **Destruction certificates**	**The results will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and Risk Assurance Committee. Any areas of high risk will be**	**Any required actions identified will be undertaken by the Information Governance Team within the timeframes agreed with the Information Governance**	**The Information Governance Team will be responsible for sharing the lessons learnt and any practice changes with all the relevant stakeholders**

	(Corporate Records)				**identified to the Risk Management Committee.**	**Group**	
Training	**LDU** **Trust Board**	**In line with requirements as defined within the current Training Needs Analysis** **Training programme review**	**Annually**	**Board reports** **Minutes of meetings, training plans**	**The results will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and Risk Assurance Committee. Any areas of high risk will be identified to the Risk Management Committee.**	**Any required actions identified will be undertaken by the Information Governance Team within the timeframes agreed with the Information Governance Group**	**The Information Governance Team will be responsible for sharing the lessons learnt and any practice changes with all the relevant stakeholders**
	LDU **Trust Board**	**Training attendance**	**Monthly**	**Corporate Dashboard**			
Records Management systems	**Trust's contracted Internal Auditors**	**Through internal audit**	**As appropriate**	**Audit Report Minutes: Audit Committee and Trust Board**	**The results will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and Risk Assurance Committee. Any areas of high risk will be identified to the Risk Management Committee.**	**Any required actions identified will be undertaken by the Information Governance Team within the timeframes agreed with the Information Governance Group**	**The Information Governance Team will be responsible for sharing the lessons learnt and any practice changes with all the relevant stakeholders**
Secure transfer of confidential and sensitive information via established best practice methods	**Information Governance Group**	**Monitoring of Trust information flows, Datix incident reports and IG updates**	**Bi-monthly at IGG meetings**	**Periodic information flow mapping exercises** **Datix incident reports**	**The IGG will review information incidents and make recommendations/ take action to mitigate risks, as necessary.**	**IG Team**	**Changes will be disseminated to staff via the intranet and staff bulletins.** **IG training will be revised to reflect current best practice, as necessary.**

Appendix L – Equality Analysis

Title: Records Management Policy and Procedures

What are the intended outcomes of this work? *Include outline of objectives and function aims* To ensure that all documents produced or received by the Trust are managed appropriately.
Who will be affected? *e.g. staff, patients, service users, general population etc* All staff and third party contractors who produce and/or receive documents.

Evidence *The Government's commitment to transparency requires public bodies to be open about the information on which they base their decisions and the results.* [1]
What evidence have you considered? *List the main sources of data, research and other sources of evidence (including full references) reviewed to determine impact on each equality group (protected characteristic). This can include national research, surveys, reports, research interviews, focus groups, pilot activity evaluations etc. If there are gaps in evidence, state what you will do to close them in the Action Plan on the last page of this template.*
Disability The policy can be made available in different formats if required.
Gender No evidence found to highlight any differences/ allowances required
Race The policy can be made available in different formats if required.
Age The policy can be made available in different formats if required.
Gender reassignment (including transgender) No evidence found to highlight any differences/ allowances required

[1] EEAS Being Open Policy

Sexual orientation

No evidence found to highlight any differences/ allowances required

Religion or belief

No evidence found to highlight any differences/ allowances required

Pregnancy and maternity

No evidence found to highlight any differences/ allowances required

Carers

No evidence found to highlight any differences/ allowances required

Other identified groups

No evidence found to highlight any differences/ allowances required

Engagement and involvement

Was this work subject to the requirements for public engagement/consultation?

How have you engaged stakeholders in gathering evidence or testing the evidence available?

How have you engaged stakeholders in testing the policy/strategy or programme proposals?

For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:

Summary of Analysis

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Eliminate discrimination, harassment and victimisation

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Advance equality of opportunity

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Promote good relations between groups

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

What is the overall impact?

No evidence to suggest that there is any potential differential impact for any of the protected characteristics.

Addressing the impact on equalities

No actions required

Action planning for improvement

Please give an outline of the key actions based on any gaps, challenges and opportunities you have identified. Actions to improve the policy/programmes need to be summarised (An action plan template is appended for specific action planning). Include here any general action to address specific equality issues and data gaps that need to be addressed through consultation or further research.

Please give an outline of your next steps based on the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of EEAS strategic equality objectives.*

For the record

Name of person who carried out this assessment:

Gail Butler (Corporate Records Manager)

Date assessment completed:

28th September 2016

Name of responsible Director:

Sandy Brown (Director of Nursing and Clinical Quality)

Date assessment was signed: 8th December 2016