East of England Ambulance Service NHS Trust

Records Management Policy and Procedures

Document Reference	POL005
Document Status	Approved
Version:	V10.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
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)
V1.0	September 2009	Approved by Trust Board

Version	Date	Comments (i.e. viewed, or reviewed, amended approved by person or committee)
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
V8.1	January 2021	Reviewed by Corporate Records Manager / FoI Officer
V8.1	21 January 2021	Recommended by IGG
V9.0	18 February 2021	Approved by CRG
V9.0	25 March 2024	Extension approved by CRG
V9.1	April/May 2024	Reviewed by Corporate Records Manager/FoI Officer and Records Management Officer
V9.1	May 2024	Recommended by IGG
V10.0	June 2024	Approved by CRG

Document Reference	Records Management Code of Practice for Health and Social Care
Recommended at Date	Information Governance Group 15/05/2024
Approved at Date	Compliance and Risk Group 03/06/2024
Valid Until Date	June 2026
Equality Analysis	Completed
Linked procedural documents	Patient Care Record Policy Confidentiality Code of Conduct
Dissemination requirements	All managers and staff via email and intranet. To be published on the Trust's public web site
Part of Trust's publication scheme	Yes

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

Appendices

1. Introduction

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 importance of sound records management is outlined in the Records Management Code of Practice for Health and Social Care. 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 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. Scope

This policy relates to all records held in any format by the Trust and applies to all those working for the Trust in any capacity.

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 and 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. This role is held by the Trust's Medical Director.

3.3 Director of Finance

The Director of Director of Finance as Senior Information Risk Owner (SIRO) for the Trust is responsible for reporting to the Board on any records management issues.

3.4 Compliance and Risk Group

The Compliance and Risk Group shall receive reports and notes of meetings from Information Governance Group as often as requested or required.

3.5 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.

3.6 Head of Information Governance and Security

The Head of Information Governance and Security is responsible for ensuring that appropriate systems are in place for the effective and secure administration, storage, archiving, retention and destruction of all records.

3.7 Data Protection Officer

The Data Protection Officer is responsible for informing and advising the Trust about its obligations to comply with the UK GDPR and other data protection laws, as well as monitoring compliance with these.

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, as well as ensuring that any local processes support national policy and processes.

3.9 Corporate Records Manager/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.

3.11 Records Management Team

The Records Management 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.

3.12 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. As well as managing those records in keeping with this policy, established information security and governance best practices, and with any further guidance subsequently produced.

3.13 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 current Records Management Code of Practice for Health and Social Care, in particular:

- The Public Records Act 1958;
- The Data Protection Act 2018;
- 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.

4. Definitions

4.1 Records

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'. An effective records management system will enable the Trust to track and trace all records.

4.2 Records Creation / Records Life Cycle

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.

4.3 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.

4.4 Information

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

4.5 Personal Information

Personal data is defined as Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.6 Sensitive Information

Special category data (formerly known as sensitive data) is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

4.7 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 the Information Governance team.

4.8 Records Retention Schedule

The Trust's Records Retention Schedule (see Section 9) states how long each group of records should be retained for and what action should be taken at the end of this retention period – secure destruction of transfer to a Place of Deposit.

4.9 Place of Deposit

Records will be transferred to an approved Place of Deposit (PoD), often a local record office, as directed in the Trust's Record Retention Schedule (see Section 9). Such a location will retain these documents as per the requirements of the Public Records Act.

4.10 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 an 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 received, held or communicated, especially information of a sensitive nature. See Section 10 for further information.

5. Document Development

The Corporate Records Manager/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 Section 9).

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.
- 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 or transferred to the Records Management team.

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 current NHS Records Management Code of Practice, this can be found here - https://eastamb.sharepoint.com/sites/RetentionSchedule

This SharePoint site also contains the NHS Retention Schedule for reference.

10. Place of Deposit

"Places of Deposit for public records are appointed to hold specific record classes in agreement with their parent authority under Section 4 (1) of the Public Records Act (1958)."

(The National Archives)

NHS guidance states that NHS Trusts must offer certain records to a Place or Deposit and consider the transfer of others, this is outlined in the Trust's Retention Schedule (see Section 9). Departments must pass any such records, once they have reached the end of the retention period, to the Records Management Team.

11. 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.

11.2 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".

A return address should be 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.

11.3 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.

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.

If being sent outside of the Trust person-identifiable or sensitive information must be either encrypted or sent to external organisations which have a suitable accredited secure email domain and end to end connector in place between the Trust and the external organisation.

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.

11.4 Telephone

Person-identifiable or sensitive information should not be disclosed via telephone, however if required and approved, the following steps must be taken.

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.

11.5 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 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.

11.6 Physical Records

Physical 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.

11.7 Notice Boards

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

11.8 Losses/Unauthorised Releases of Information

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.

12. Equality Analysis

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

13. Dissemination and Implementation

13.1 Dissemination

This document will be stored in the online Document Library for all Trust staff to access.

13.2 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 required.

14. Process for Monitoring Compliance and Effectiveness

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

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 Compliance and Risk Group.

15. Standards/Key Performance Indicators

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

16. References

Records Management: NHS Code of Practice

Public Records Act 1958

Data Protection Act 2018

Freedom of Information Act 2000

17. Associated Documents

Patient Care Records Policy

Confidentiality Code of Conduct

Appendices

Appendix A Patient Records Management Procedures

Appendix B Corporate Records Management Procedures

Appendix C Flow Chart for Archiving Records Off-site

Appendix D Flow Chart for Retrieval of PCR Stored On-site

Appendix E Flow Chart for Retrieval of PCR Stored Off-site

Appendix F Monitoring Table

Appendix G Equality Analysis

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 they came from.

Any stations submitting paper PCRs that exceed the 14 day standard will be contacted by the relevant locality office and the Records Management team notified of any outcomes. Further delays will be escalated to the Information Governance Manager

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

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

Retrieval – Single Patient Care Records

Internal archiving – To request a PCR that is stored onsite see Appendix D

Retrieval from external archiving

Only the Corporate Records Manager/FOI Officer and Information Governance Manager are authorised to request PCRs from the offsite storage provider.

To request a PCR that is stored with the offsite storage provider see Appendix E

Retrieval from external archiving – Multiple Days

When physical PCRs for an entire day or multiple days are required these must be requested through the Information Governance Manager.

Retention and Destruction of records

Archived PCRs held off-site will be retained in line with the Trust's Record Retention Schedule or until they have been retrieved and scanned. The archived PCRs will be securely destroyed in line with the Record Retention Schedule.

The destruction certificate will be retained by the Corporate Records Manager/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 Records Management Team 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

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.

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 of Records

Box Retrieval

Email: Records.Management@eastamb.nhs.uk with

- the box number of the box you require
- the barcode or the number assigned to it by the Trust can be used

File Retrieval

Email: Records.Management@eastamb.nhs.uk with

- name/number of the file
- the number of the box it is in

To receive a Scan back (electronic scanned image)

Request through SharePoint PCR Request Site

A database of all requests and retrievals is held by the Records Management Team.

Returns

To return physical records to storage please email Records.Management@eastamb.nhs.uk 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.

Review date

When a box reaches, or is close to, its review date, the head of your department 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 () then this must be outlined in an email to Records.Management@eastamb.nhs.uk

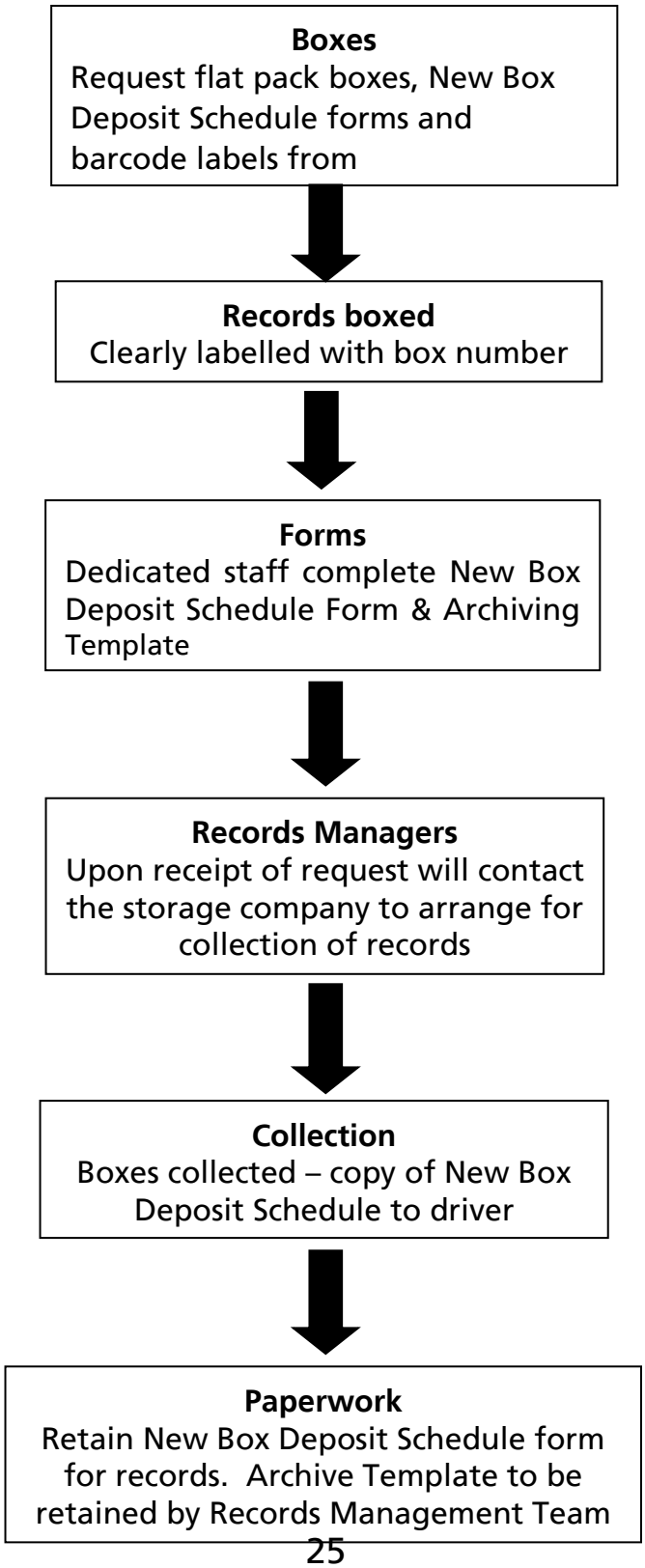
Please note: if you wish to recall the box for inspection you will incur the cost of retrieving the box and then returning it to storage for destruction.

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, Records.Management@eastamb.nhs.uk 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

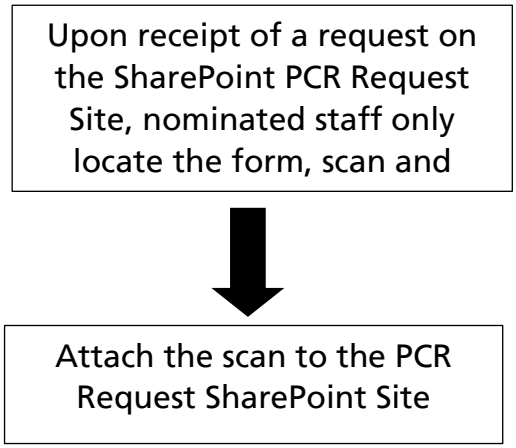
Remove and reuse all ring binders and lever arch folders; documents should be bound with filing clips (paper clips or elastic bands rust/perish).



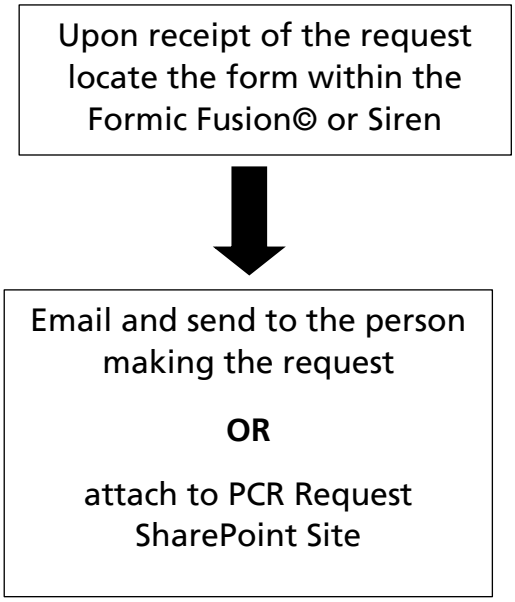
Appendix D - Flow chart for retrieval of PCR stored on-site

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

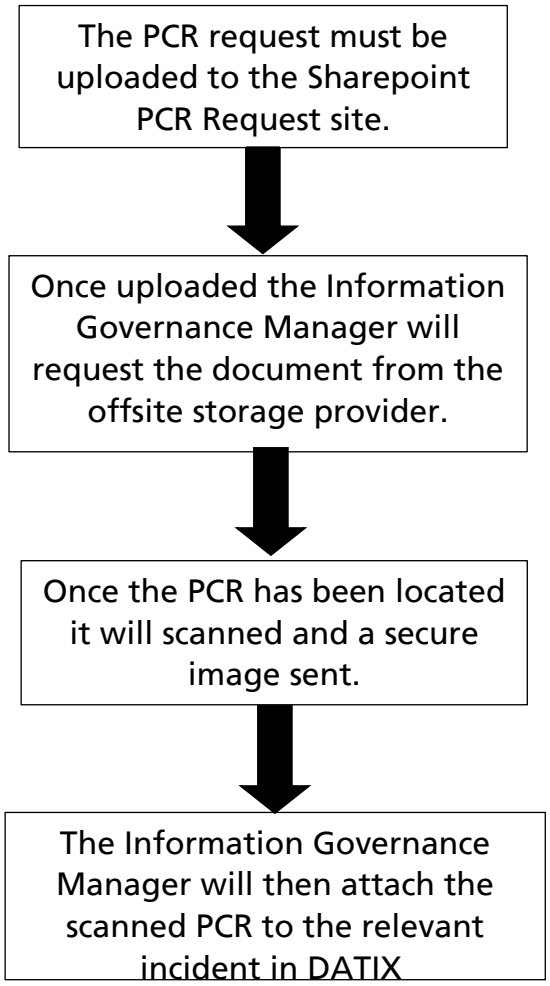
UNDER NO CIRCUMSTANCES RELEASE THE ORIGINAL PATIENT CARE RECORD



For those instances where the PCR has been scanned or ePCR used:



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



Appendix F – 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 appraisals	Annually	Appraisal forms; identified Training needs submitted to Organisational Development	The results will be reported to the Trust Board via the Audit Committee, Information Governance Group and Quality and ELB.	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	Information Governance 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 ELB.	Any required actions identified will be undertaken by the Information Governance Team within the timeframes agreed with the	The Information Governance Team will be responsible for sharing the lessons learnt and any practice changes with all the relevant stakeholders

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
	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		Information Governance Group	
Retention and disposal schedules	Corporate Records Manager/ FoI Officer	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 ELB.	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
Training	Organisational Development Trust Board	In line with requirements as defined within the current Training	Annually	Board reports Minutes of meetings, training plans	The results will be reported to the Trust Board via the Audit Committee, Information Governance Group	Any required actions identified will be undertaken by the Information Governance	The Information Governance Team will be responsible for sharing the lessons learnt and any practice

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
		Needs Analysis Training programme review			and Quality and ELB.	Team within the timeframes agreed with the Information Governance Group	changes with all the relevant stakeholders
	Organisational Development Trust Board	Training attendance	As required	Training figures	The figures will be brought to each IGG meeting as required.		
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 ELB.	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	Information Governance Group	Monitoring of Trust information flows, Datix	Bi-monthly at IGG meetings	Periodic information flow mapping exercises	The IGG will review information incidents and make recommendations/	IG Team	Changes will be disseminated to staff via the

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
sensitive information via established best practice methods		incident reports and IG updates		Datix incident reports	take action to mitigate risks, as necessary.		intranet and staff bulletins. IG training will be revised to reflect current best practice, as necessary.

Appendix G – Equality Impact Assessment

<table>
<tr><th colspan="2">EIA Cover Sheet</th></tr>
<tr><td>Name of process/policy</td><td>Records Management Policy and Procedures</td></tr>
<tr><td>Is the process new or existing? If existing, state policy reference number</td><td>POL005</td></tr>
<tr><td>Person responsible for process/policy</td><td>Corporate Records Manager / FoI Officer</td></tr>
<tr><td>Directorate and department/section</td><td>Nursing & Quality Improvement – Compliance & Standards</td></tr>
<tr><td>Name of assessment lead or EIA assessment team members</td><td>Corporate Records Manager / FoI Officer</td></tr>
<tr><td>Has consultation taken place?

Was consultation internal or external? (please state below):</td><td>Yes</td></tr>
<tr><td>Internal</td><td>Information Governance / IGG</td></tr>
<tr><td>The assessment is being made on:

Please tick whether the area being assessed is new or existing.</td><td>
<table>
<tr><td>Guidelines</td><td></td></tr>
<tr><td>Written policy involving staff and patients</td><td>X</td></tr>
<tr><td>Strategy</td><td></td></tr>
<tr><td>Changes in practice</td><td></td></tr>
<tr><td>Department changes</td><td></td></tr>
<tr><td>Project plan</td><td></td></tr>
<tr><td>Action plan</td><td></td></tr>
<tr><td colspan="2">Other (please state)

Training programme.</td></tr>
</table>
</td></tr>
</table>

Equality Analysis					
What is the aim of the policy/procedure/practice/event? To ensure staff are clear on how to manage any records they receive or create as part of their role at EEAST					
Who does the policy/procedure/practice/event impact on? All staff who create or receive records during their work for EEAST.					
Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐
Who is responsible for monitoring the policy/procedure/practice/event? Corporate Records Manager / FoI Officer					
What information is currently available on the impact of this policy/procedure/practice/event? N/A					
Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event? ~~Yes~~/No					
Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? ~~Yes/~~No, If yes please provide evidence/examples:					
Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐

Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? ~~Yes/~~No, if so please provide evidence/examples:

Race	☐	**Religion/belief**	☐	**Marriage/Civil Partnership**	☐
Gender	☐	**Disability**	☐	**Sexual orientation**	☐
Age	☐	**Gender re-assignment**	☐	**Pregnancy/maternity**	☐

Please provide evidence:

Action Plan/Plans - SMART

Specific

Measurable

Achievable

Relevant

Time Limited

Evaluation Monitoring Plan/how will this be monitored?

Who

How

By

Reported to