Freedom of Information Request

Reference Number: EPUT.FOI.19.1304
Date Received: 31 October 2019

Information Requested:

Can I also get the below IG doc's please?

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Attached</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPG9(c) Storage, Retention and Destruction Procedure</td>
<td>Please see attached</td>
</tr>
<tr>
<td>CPG9(d) Electronic Records Procedure</td>
<td>Please see attached</td>
</tr>
<tr>
<td>RMPG13(d) Secure Handling and Disposal of Confidential Waste Procedure</td>
<td>Please see attached</td>
</tr>
</tbody>
</table>

Publication Scheme:

As part of the Freedom of Information Act all public organisations are required to proactively publish certain classes of information on a Publication Scheme. A publication scheme is a guide to the information that is held by the organisation. EPUT’s Publication Scheme is located on its Website at the following link: [https://eput.nhs.uk](https://eput.nhs.uk)
STORAGE, RETENTION AND DESTRUCTION OF RECORDS PROCEDURE

POLICY REFERENCE NUMBER
VERSION NUMBER
REPLACES SEPT DOCUMENT
REPLACES NEP DOCUMENT
KEY CHANGES FROM PREVIOUS VERSION
Incorporated new General Data Protection Regulations
Updated processes

AUTHOR
Consultation
Information Governance Steering Committee
Quality Committee
Paris Project Board
Mobius Project Board

IMPLEMENTATION DATE
August 2017
AMENDMENT DATE(S)
August 2018
LAST REVIEW DATE
August 2018
NEXT REVIEW DATE
August 2021
APPROVAL BY INFORMATION GOVERNANCE STEERING SUB-COMMITTEE
24th September 2018
RATIFIED BY QUALITY COMMITTEE
12th October 2018

COPYRIGHT
© EPUT 2018
All rights reserved. Not to be reproduced in whole or part without the permission of the copyright owner

OPERATIONAL POLICY SUMMARY
The purpose of this procedure is to ensure that the destruction of health and corporate records is compliant with the Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016, Public Records Act 18

The Trust monitors the implementation of and compliance with this operational policy in the following ways;
This process is monitored via the Information Governance Toolkit and assurance reports are submitted to the Information Governance Steering Committee

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

STORAGE, RETENTION AND DESTRUCTION OF RECORDS PROCEDURE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE. BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THAT SECTION.

1.0 INTRODUCTION
2.0 PURPOSE
3.0 LEGAL POSITION
4.0 RESPONSIBILITY
5.0 RECORD CLOSURE
6.0 RECORD STORAGE FACILITIES
7.0 PERMANENT PRESERVATION OF RECORDS
8.0 RECORDS TO BE RETAINED
9.0 RETRIEVAL OF RECORDS
10.0 DESTRUCTION OF RECORDS
11.0 DESTRUCTION OF ELECTRONIC RECORDS
12.0 REFERENCE TO OTHER POLICIES AND PROCEDURES

APPENDICES

APPENDIX 1 – RECORDS MANAGEMENT CODE OF PRACTICE: SECTION 4
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

STORAGE, RETENTION AND DESTRUCTION OF RECORDS PROCEDURE

Assurance Statement
The purpose of this procedure is to ensure that the destruction of health and corporate records is compliant with the Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016, Public Records Act 1958

The implementation of these guidelines will ensure that the Trust stores, retains and disposes of records in accordance with current legal requirements and best practice.

1.0 INTRODUCTION

1.1 Records are a valuable source of information, and the intelligence they contain is vital to the quality of patient care and treatment, and provides evidence of the Trust’s business decisions made.

1.2 Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016 states that “records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time”.

1.3 The Trust may decide to keep records longer than the recommended minimum period, according to the reasoning behind its own retention schedules. However records should not be destroyed earlier than the recommended minimum period.

1.4 In 2013 the government confirmed that historical records (the Trust will decide if any records are considered to be of historical value to the public), are to be stored at The National Archives, (TNA) or Local Place of Deposit, (LPoD) after 20 years instead of 30 years. The move to a ‘20-year rule’ represents a major change for public records and replaces the ‘30-year rule’.

2.0 PURPOSE

2.1 These guidelines refer to the minimum retention periods for all health and corporate records and details the minimum standards for record storage facilities in line with the relevant legislation and guidance.

3.0 LEGAL POSITION

3.1 All NHS records are public records under the Public Record Act 1958/1967, under the terms of guidance issued by the Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016

3.2 The Trust has reviewed this guidance and agreed minimum retention periods for all Trust records in line with Section 4 of the Code of Practice.
3.3 All NHS organisations have a legal responsibility to maintain records safely and securely under Article 5 of the Data Protection Act 2018.

3.4 The preservation of Trust records can be divided into two distinct categories:

- Records requiring permanent preservation
- Records to be retained for minimum periods

3.5 These guidelines refer to NHS records of all types regardless of the media on which they are held, including:

- Patients health / medical records (electronic, digital, paper based) across all specialties
- Administrative records (personnel, estates, financial and accounting, notes associated with complaint handling, etc.)
- X-ray, imaging reports, photographs, slides and other images
- Microfilm, microfiche
- Audio and video tapes, cassettes, CD-ROM, etc.
- E-mails
- Digital records
- Computerised records

3.6 The use of health and corporate records as a legal document places specific requirements upon the Trust to meet minimum periods of retention. The length of retention depends upon the type of record and its importance to the business of the organisation. For further details staff should refer to the Records Management Code of Practice: Section 4 (Appendix 1 of this Procedure).

4.0 **ROLES AND RESPONSIBILITIES**

4.1 All Trust staff have a responsibility for records management, and should refer to the Trust Records Management Policy (CP9) for full details of how to manage the Trust’s records.

4.2 The Director with responsibility for records (the Executive Chief Finance and Resourcing Officer) is responsible for Trust wide and strategic management of records. In addition the Trust has nominated officers (Head of Electronic Systems & Records / Records Manager) – responsible for ensuring compliance with the Trust’s policy on the retention / preservation of records. These officers also have the responsibility to ensure that records are stored and destroyed in line with Trust policy / procedure.

4.3 All staff are responsible for the storage and confidentiality of records within their area of activity. Existing records must be stored securely and appropriately referenced, and quality assurance standards should be maintained for digitally scanned records in line with the Trust’s best practice.
4.4 The Head of Electronic Systems & Records / Records Manager is responsible for co-ordinating any archiving with the local records managers / service managers / administration staff with responsibility for records and the Trust's nominated supplier / storage facility.

4.5 The Head of Electronic Systems & Records and the Director with responsibility for records will be responsible for liaising, where required, with the Public Records Office.

4.6 The Information Governance Manager will be responsible for ensuring that all information breaches in relation to the storage, retention and destruction of records are investigated and reported in line with Trust procedures to the Caldicott Guardian \ Senior Information Risk Owner.

5.0 RECORDS CLOSURE

5.1 Records must be closed as soon as they have ceased to be in active use other than for reference purposes i.e. (Dormant flag can be used) An indication that a file of paper records or folder of electronic records has been closed must be shown on the record itself as well as noted in the index, database of the file folders / Trust information systems.

5.2 Wherever possible, information on the intended disposal of electronic records must be included in the metadata when the record is created.

5.3 The storage of closed or non-current records awaiting disposal must follow accepted standards relating to environment, security and physical organisation of the files. In any event, public records must not ordinarily be kept for more than 20 years (calculated from the last entry date on the file), without being transferred to a local place of deposit. If the Trust has reason to retain the records for more than 20 years (other than for statutory or active administrative purposes) it must contact the National Archive (or the LPoD) for advice. Records chosen for archive must be dealt with by following the Trust's Records Management Policies and Procedures.

5.4 All staff are responsible for the safety and security of any person identifiable, confidential and/or sensitive information that is to be transported. Records must be in secure tamper proof bags, and in vehicles out of sight from the public, placed in the boot, if in a car. External contractor transportation must always meet the same Trust standards. Once transported to a LPoD the security of the records becomes the responsibility of the new keeper.

6.0 RECORD STORAGE FACILITIES

6.1 The following guidelines, based on BS5454: 2000, ‘Recommendations for Storage and Exhibition of Archival Documents’, must be applied to all record storage areas (archive and central ‘active’ records) across the Trust or held within external storage facilities on behalf of the Trust.
The LPoD for Essex records is the Essex Records Office at Essex County Council and for Bedford records it is Bedfordshire Archives Services in Bedford.

6.2 Central Record libraries (Archive)

Situation/Construction
6.2.1 The siting must not be subject to any hazard from external sources including neighbouring buildings or properties.

6.2.2 The store must be of robust construction of brick, stone or concrete, with protection against unauthorised entry, fire, flood, damp or pest.

6.2.3 The floor should be capable of bearing the weight of the records stored and the type of shelving chosen.

6.2.4 Plumbing and drains in or above or adjacent to the storage room should be avoided. There must be no pipe work containing water or other liquids positioned above the storage.

6.2.5 Any materials used should be a minimum of flammable finishes and fixtures.

6.3 Security
6.3.1 The perimeter of the storage room must be secure against unauthorised entry and vandalism.

6.3.2 The doors must be strong and fitted with mortise deadlocks or security locks and keys must be strictly controlled by archival staff.

6.3.3 Windows should be protected by bars or mesh especially on ground floors.

6.3.4 Alarms should be used to protect against intruders out of normal working hours. All alarms including fire alarms must be connected to the appropriate emergency services.

6.3.5 Access should be restricted to records staff and other authorised staff employed by the organisation.

6.3.6 A suitable CCTV system must be in place.

6.3.7 All storage transport vehicles must be unmarked in terms of contents (e.g. not say confidential storage items being transported) and must be locked and secured when not in use.

6.4 Fire Protection
6.4.1 Automatic smoke detectors and fire alarms should be fitted throughout the stores.
6.4.2 Fire extinguishers must be provided with advice from the fire prevention officer.

6.4.3 Lighting should be by fluorescent tube fitted with diffusers.

6.4.4 Smoking should be prohibited.

6.5 Environment & Storage

6.5.1 Constant temperatures should be maintained in line with the Records Management Code of Practice Parts I and II.

6.5.2 Shelving should possess sufficient load bearing strength for the items to be stored.

6.5.3 Films should be stored in dust free metal cabinets.

6.5.4 Tapes should be stored in metal, cardboard or inert plastic containers, placed vertically on metal shelving.

6.6 Local Record Libraries

6.6.1 Department and service / team managers will be responsible for the implementation and compliance of these procedures, and will be answerable for ensuring that their teams manage the local libraries for both paper and electronic records.

6.6.2 Records in constant use should be securely kept at the service or unit. Cabinets / drawers / local record libraries / rooms containing medical or other confidential records must be kept locked or electronically stored where available.

6.6.3 Electronic records must be stored on shared drives (e.g. G:\, S:\, T:\, H:\ etc.) and not on local C:\ drives (this includes Desktop, My Documents, etc.).

6.6.4 Access to local records libraries should be by authorised personnel only.

6.7 Electronic Records

6.7.1 All records stored on the Trust’s electronic records systems will need to follow both system / manufacturer guidance and also trust policies and be in line with BS: 100008 Legal Admissibility

7.0 PERMANENT PRESERVATION OF RECORDS

7.1 Documents detailing major changes within the provision of health care, research and those of specific organisational historical data, may be of public interest and therefore suitable for permanent preservation.
7.2 Examples of records requiring permanent preservation are as follows:- (List is not exhaustive)

- Documents detailing history of the Trust
- Major events/notable events. (e.g. major incidents, including pandemics, or substantial changes in the provision of local healthcare)
- Major projects and plans (e.g. opening of new buildings; healthcare plans/strategies)
- Industrial Relations documents
- Documents detailing research work / development (these may include health records)

7.3 The appropriate directorate Director will be responsible for identifying to the Head of Electronic Systems & Records, those records that may require permanent preservation at the point they are to be archived.

7.4 Those records identified for permanent preservation should not be included in an ‘ordinary’ archive box of records but should be passed to the Head of Electronic Systems & Records as individual items.

7.5 The Head of Electronic Systems & Records Manager will be responsible for identifying records for permanent preservation and securely storing this in the central records libraries. Only when a full box of permanent preservation records is completed will the box be sent to the external archive store.

7.6 Once identified and selected the Trust Executive Team will be required to authorise final preservation in line with the national Information Governance Records Management Code of Practice.

7.7 Local county councils already possess many of the original documents relating to important changes in the provision of local healthcare. Close cooperation is required between the nominated officers and the LPoD to ensure samples of records are transferred at the appropriate time to the Public Records Offices, Chelmsford and Bedford. The Public Records Office must be advised, by the nominated officer, of the type and nature of any record held by the Trust in excess of 20 years of age.

8.0 RECORDS TO BE RETAINED

8.1 Records Not Requiring Permanent Preservation
The Trust’s agreed minimum retention time for non-permanent records is shown in the summary guidance at Appendix 1, to ensure that the Trust meets its statutory duties and may provide evidence in case of future litigation.

8.2 The agreed time-scales balance the need to retain records and the resources available to meet the costs of storage. It is also recognised both nationally and locally that some documents may be destroyed before notification of a legal claim has been registered.
8.3 General correspondence, memos, emails etc. not directly related to any of the categories identified should be retained for a maximum of three years. Local judgement should be used to determine the minimum retention period, particularly where storage space is limited.

9.0 RETRIEVAL OF RECORDS

9.1 Active Records
9.1.1 Only authorised staff have permission to retrieve active records. These may be administration staff, health professionals involved with the patient, medical secretaries and the Head of Electronic Systems & Records / Records Manager.

9.1.2 Whenever a record is taken from the records library (central or local) the authorised person removing the record must ensure that the record is tracked using the Trust's tracking processes.

9.1.3 All records must be replaced in their original place of deposit when no longer required and the tracking card / system updated.

9.2 Archive Records – see below for supplier specifics
9.2.1 Suppliers / external storage companies will be reviewed for suitability by the Head of Electronic Systems & Records, and Trust’s Records Manager with the Contracts Department, decide on the approved supplier for archiving services in line with Trust policy for tendering / contracts.

9.2.2 Only authorised staff have permission to retrieve archive records. These may be the Head of Electronic Systems & Records or the designated person(s) at the external record library. Teams / individuals requiring the return of archived records must, in writing to epunft.essex.records@nhs.net request retrieval through the local processes as agreed with the Head of Electronic Systems & Records.

9.2.3 All requests for record retrieval must be via email to epunft.essex.records@nhs.net and must include details of the archived box number and / or file barcode number (not individual file name), budget code and address for delivery. This information will be obtained from the original archive record sheet, which will be held locally by individual teams / services.

9.3 Returning Records to Archive
9.3.1 All requests for returns to the archive facility must be via email to epunft.essex.records@nhs.net and contain the information as in 9.2.2 above.
9.4 **Records Requests for Restore/Stephens/Oasis**

9.4.1 All requests for records to be archived via the Trust’s offsite storage providers, Restore, Oasis and Stephens, are administered by the dedicated records staff and records e-mail address. These are, epunft.essex.records@nhs.net for all South and North localities and for all Bedfordshire Community.

Local procedures are available from the dedicated records staff.

9.4.2 As instructed in the local procedure, barcodes will need to be used to both identify the boxes and the individual health files. Corporate files do not require file barcodes. A list should be maintained of the records contained in each box on the specific templates. This applies to both corporate records and health records.

9.4.3 The lists of records are password protected and are sent to the epunft.essex.records@nhs.net e-mail address where the dedicated records staff then transfers this information onto a main catalogue of stored records.

9.5 **Records Requests from Restore/Oasis/Stephens – Retrieval from Archive**

9.5.1 All requests for records to be retrieved from archive via the Trust’s offsite storage provider, Restore / Oasis / Stephens, are administered by the dedicated records staff and records e-mail address epunft.essex.records@nhs.net

9.5.2 Using the designated templates, and completing as instructed this form is sent via password protected e-mail to epunft.essex.records@nhs.net where the dedicated records staff will request the relevant records directly from the offsite storage provider via encrypted e-mail.

10.0 **DESTRUCTION OF PAPER BASED RECORDS**

10.1 This section of the procedure should be read in conjunction with the Trust’s Confidential Waste Procedure.

10.2 The Head of Electronic Systems & Records / Records Manager will be responsible for ensuring that the destruction of scanned and or paper records is carried out once all quality assurance checks have been validated and the Director with responsibility for records has authorised such destruction.

10.3 The Trust retains responsibility for ensuring confidentiality throughout all stages of the destruction process and any contractor employed to remove records must demonstrate satisfactory safeguards against accidental loss or disclosure.
10.4 At all stages during the destruction process confidentiality must be fully maintained. The Trust’s preferred method of destruction, therefore, will be by incineration or shredding only.

10.5 Following destruction of any health records, all Certificates of Destruction must be forwarded to the Head of Electronic Systems & Records / Records Manager who will be responsible for maintaining the records of destruction, in line with the Information Governance Alliance Code of Practice, Section 4, permanently.

10.6 The Head of Electronic Systems & Records / Records Manager or their representative will provide confirmation of destruction at the Information Governance Steering Committee. This information will be in the form of number of boxes / records destroyed (paper), and not by individual file name. For electronically held records destruction will be maintained within the specified parameters in the Trust's electronic system as determined by this procedure.

10.7 If a record due for destruction is known to be the subject of a request for information, destruction must be delayed until disclosure has taken place or if the authority has decided not to disclose the information until the complaint and appeal provisions of the Freedom of Information Act 2000 have been exhausted.

11.0 DESTRUCTION OF ELECTRONIC RECORDS

11.1 This section of the procedure must be read in conjunction with the Trust’s Scanned Records Quality Control to Disposal Procedures. Electronic records due for deletion from the Trust’s electronic scanning system are strictly controlled by technical restrictions for access, controlled by passwords and smart cards, with different access levels according to the status of the user.

11.2 A log of electronic records destroyed must always be maintained, showing the reference number, description and reason for deletion.

12.0 REFERENCE TO OTHER POLICIES AND PROCEDURES

12.1 When processing records in any capacity reference should be made to any Trust policies relating to records as well as to local and professional guidance.

12.2 Other documentation will include:
- Records Management Policy (CP9)
- Data Protection Act 2018 and Confidentiality Policy / Procedure
- Information Sharing and Consent Procedure
- Secure Handling and Disposal of Confidential Waste Procedure
- Scanned Records Quality Control to Disposal Procedures

END
### SUMMARY OF DESTRUCTION PERIODS FOR RECORDS WHICH ARE NOT FOR PERMANENT PRESERVATION

(AS DETAILED IN RECORDS MANAGEMENT CODE OF PRACTICE: SECTION 4)

<table>
<thead>
<tr>
<th>NUMBER AND CLASS OF DOCUMENTS</th>
<th>PERIOD AFTER WHICH DOCUMENTS MAY BE DESTROYED</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Salaries and wages records, i.e. employees pay cards and personal pay records (except those for part-time doctors and dentists employed by RHA’s and HA’s which should not be destroyed)</td>
<td>Ten years after the termination of employment</td>
</tr>
<tr>
<td>2. Copies of forms SD55 (ADP) and AD55J (originals are sent to Health Services Superannuation Branch of the Department)</td>
<td>Ten years after the end of the financial year to which they relate</td>
</tr>
<tr>
<td>3. Principal Ledger Records: including such documents as cash books, ledgers, income and expenditure journals, etc.</td>
<td>Six years after the end of the financial year to which they relate</td>
</tr>
<tr>
<td>4. Bills, receipts and cleared cheques</td>
<td>Six years after the end of the financial year to which they relate</td>
</tr>
<tr>
<td>5. Documents, other than those of permanent relevance in relation to trust funds and the terms of any trusts administered by health authorities</td>
<td>Six years after the end of the financial year to which the trust monies became finally spent, or the gift in kind was accepted</td>
</tr>
<tr>
<td>6. Major establishments records: including personal files, letters of appointment, contracts references and related correspondence and records of sick leave (except for those part-time doctors and dentists employed by RHA’s and HA’s which should not be destroyed)</td>
<td>Six years after the officer leaves the service of the hospital or on the date on which the officer would reach the age of 70, whichever is the later, provided that if an adequate summary of the personal and health record is kept for this period the main records may be destroyed ten years after the officer leaves the service of the hospital</td>
</tr>
<tr>
<td>7. Wages / salary records</td>
<td>10 years after termination of employment</td>
</tr>
<tr>
<td>8. Estimates: including supporting calculations and statistics</td>
<td>Three years after the end of the financial year to which they relate</td>
</tr>
<tr>
<td></td>
<td>NUMBER AND CLASS OF DOCUMENTS</td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>9.</td>
<td>Cost accounts prepared in accordance with the directions of the Secretary of State or at the request of the Department</td>
</tr>
<tr>
<td>10.</td>
<td>Audit records (e.g. organisational audits, records audits, system audits) – internal and external in any format (paper, electronic, etc.)</td>
</tr>
<tr>
<td>11.</td>
<td>Accounts – minor records (pass books, paying-in slips, cheque counterfoils, cancelled/ discharged cheques [for cheques bearing printed receipts, see Receipts], accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt books, income records, laundry lists and receipts) Stores, equipment and buildings</td>
</tr>
<tr>
<td>12.</td>
<td>Engineers inspection reports on boilers, lifts, etc.</td>
</tr>
<tr>
<td>13.</td>
<td>Major stores records; stores ledgers and equivalents</td>
</tr>
<tr>
<td>14.</td>
<td>Minor Supplies Records: including invitations to tender and inadmissible tenders, routine papers relating to catering and demands for furniture, equipment, stationery and other supplies</td>
</tr>
<tr>
<td>15.</td>
<td>Records (other than those of permanent value) relating to capital and other building works or improvements, including plans and specifications prepared for temporary purposes and papers relating to them</td>
</tr>
<tr>
<td>16.</td>
<td>Inventories of furniture, medical and surgical equipments not held on store charge and with a minimum life of 5 years</td>
</tr>
<tr>
<td>17.</td>
<td>Activity records, input documents which supplement but do not replace health records</td>
</tr>
<tr>
<td>18.</td>
<td>Health and Safety Records including RIDDOR, COSHH, Accident Reports and Notifications to staff on Health and Safety issues</td>
</tr>
<tr>
<td>No.</td>
<td>Type of Record</td>
</tr>
<tr>
<td>-----</td>
<td>----------------</td>
</tr>
<tr>
<td>19</td>
<td>Diaries</td>
</tr>
<tr>
<td>20</td>
<td>Ward Report Book</td>
</tr>
<tr>
<td>21</td>
<td>Obstetric records Maternity (all obstetric and midwifery records, including those of episodes of maternity care that end in stillbirth or where the child later dies)</td>
</tr>
<tr>
<td>22</td>
<td>Records relating to children and young people</td>
</tr>
<tr>
<td>23</td>
<td>Records relating to mentally disordered people within the meaning of the Mental Health Act 1959</td>
</tr>
<tr>
<td>24</td>
<td>Records relating to interuterine coil devices  Contraception and Sexual health records</td>
</tr>
<tr>
<td>25</td>
<td>All other personal health records</td>
</tr>
</tbody>
</table>
# Scanning Front Sheet

**Date:**

<table>
<thead>
<tr>
<th>Team / Ward</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scanner Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date Scanned:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QA date:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Quality Assurance Record - Documents Scanned

**Essex Partnership University NHS Foundation Trust**

**Updated: 19/07/2016**

<table>
<thead>
<tr>
<th>Hospital No</th>
<th>No of Pages</th>
<th>OK or</th>
<th>Error Code</th>
<th>Action Required</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Error Code: A** Date Error / Case Recipient error
- **Count: 1**

- **Error Code: B** Cover Selector / Case Recipient error
- **Count: 2**

- **Error Code: C** Wrong document type
- **Count: 1**

- **Error Code: D** Test or barcode covered (not fit, folded, creased)
- **Count: 2**

- **Error Code: E** Bar Code Data being scanned (inside blank, Failed)
- **Count: 1**

- **Error Code: F** 2-3-4 sheets scanned together
- **Count: 3**

- **Error Code: G** 2 scanner failure (VTM) & recycled paper used
- **Count: 1**

- **Error Code: H** Other
- **Count: 1**

- **Error Code: I** Printing issues (Low Ink, Leaking Ink), Bar Code Failed
- **Count: 2**

- **Error Code: J** Other printing issues
- **Count: 1**

- **Error Code: K** Document partly scanned
- **Count: 1**

- **Error Code: L** Document Not found, Re-scanned
- **Count: 1**

- **Error Code: M** Document Not Scanned to Scanning Folder
- **Count: 1**

- **Error Code: N** 2 or more different documents for the same patient scanned together
- **Count: 1**

- **Error Code: O** Wrong Bar coded Coversheet printed and scanned for the wrong patient
- **Count: 1**

- **Error Code: P** Scanning failures (Barcodes damaged, torn, double imaged, punched, angled, glass dirty)
- **Count: 1**

- **Error Code: Q** Scanned Single Sided, Re-scanned
- **Count: 1**

- **Error Code: R** Documents In Failed Folder
- **Count: 1**
NOTICE

THE FOLLOWING PAGE(S) ARE TORN OR DAMAGED THEY HAVE BEEN SCANNED AS PER THE ORIGINAL(S)
NOTICE

THE FOLLOWING PAGE(S) ARE PHOTOCOPIES. THEY HAVE BEEN SCANNED AS PER THE ORIGINAL(S)
PLEASE NOTE:-

This patient’s file has had one or more documents removed from it.

These may have been:

X-Rays
Samples or any
Other unscannable media

Removed By     Name:

Date:-
PAGE____________
PART____________
WAS / WERE MISSING AT TIME OF SCANNING

Thank you
SECURE HANDLING AND DISPOSAL OF CONFIDENTIAL WASTE PROCEDURE

Procedure No: RMPG13d

RETRIEVAL FORM

Site: ........................................................................................................

Requestor (print name): .................................................................

Signature: ........................................................................................

Date of Retrieval: ..........................................................................

Authorised Person: (Witness) ....................................................
(Print name)

Signature: ........................................................................................

Date of Retrieval: ..........................................................................

Reason for retrieval:

Please copy this form. Original to be retained by Requestor
Copy to be sent Information Governance Department
SECURE HANDLING AND DISPOSAL OF CONFIDENTIAL WASTE PROCEDURE

PROCEDURE NUMBER: RMPG13d
VERSION NUMBER: 5
REPLACES SEPT DOCUMENT
REPLACES NEP DOCUMENT
KEY CHANGES FROM PREVIOUS VERSION: Merger of NEP & SEPT Policies
AUTHOR: Head of Estates and Facilities
CONSULTATION GROUPS: N/A
IMPLEMENTATION DATE: April 2017
AMENDMENT DATE(S): March 2018

LAST REVIEW DATE: November 2019
NEXT REVIEW DATE: November 2022
APPROVAL BY HEALTH SAFETY AND SECURITY COMMITTEE: October 2019
RATIFICATION BY QUALITY COMMITTEE: November 2019
COPYRIGHT: 2017

PROCEDURE SUMMARY

The Trust has a responsibility to ensure that all documents and records of a confidential nature are destroyed and also to ensure that prior to the destruction process that these documents / records are stored securely. Non-compliance has very serious implications for both the Trust and individuals. As such every member of staff must take responsibility for ensuring that when and where they are required to dispose of documents etc. that are of a confidential nature, that these actions are carried out appropriately, so as not to compromise confidentiality.

THE TRUST MONITORS THE IMPLEMENTATION OF AND COMPLIANCE WITH THIS PROCEDURE IN THE FOLLOWING WAYS:
Reporting of any incidents via Datix. Regular monitoring and reports to relevant committee. Contractual review meeting, Auditing and Monitoring

SCOPE

<table>
<thead>
<tr>
<th>Services</th>
<th>Applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustwide</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

The Director responsible for monitoring and reviewing this policy is Executive Chief Finance Officer

Page 1 of 5
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

PROCEDURAL GUIDELINES FOR THE SECURE HANDLING, AND DISPOSAL OF CONFIDENTIAL WASTE

CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

1.0 INTRODUCTION
2.0 CONFIDENTIAL WASTE
3.0 STORAGE CONFIDENTIAL WASTE
4.0 RETRIEVAL OF INCORRECTLY CONSIGNED CONFIDENTIAL MATERIAL
5.0 DESTRUCTION OF CONFIDENTIAL WASTE

APPENDICES

APPENDIX 1 - RETRIEVAL FORM
1.0 INTRODUCTION

1.1 The Trust has a responsibility to ensure that all documents and records of a confidential nature are destroyed and also to ensure that prior to the destruction process that these documents / records are stored securely. Non-compliance has very serious implications for both the Trust and individuals. As such every member of staff must take responsibility for ensuring that when and where they are required to dispose of documents etc. that are of a confidential nature, that these actions are carried out appropriately, so as not to compromise confidentiality.

1.2 The procedure should be read in conjunction with the Storage Retention and Destruction of Records Procedure, CPG9C.

Please Note: both documents have been written to ensure that the Trust complies with the guidance issued in the Data Security and Protection Toolkit.

2.0 CONFIDENTIAL WASTE

2.1 Confidential waste is anything that contains:

- Patient and/or Person Identifiable Information
- Personal Information
- Corporately Sensitive Information

2.1.1 Person Identifiable Information is information about a person which would enable that person’s identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode which could allow the person to be identified.

2.1.2 Personal Information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community. For e.g. where the personal information contains details of the individual’s:

- Health or physical condition
- Sexual life
- Religious beliefs
- Trade union
- Political opinions
- Criminal convictions
- Personal Details
- Payroll data
2.1.3 Corporately Sensitive Information is that which if disclosed may, adversely affect the Trust’s reputation.

### 3.0 STORAGE CONFIDENTIAL WASTE

3.1 Confidential waste must be stored securely either in locked consoles or bins or in a secure room or compound prior to destruction.

3.1.1 An approved contractor will supply confidential waste containers which will be serviced on a regular basis and any documentation etc. contained with will be destroyed. Departments etc. requiring this service must contact their relevant Estates and Facilities Department:

South Essex- 01268 407814  
North Essex- 01206 334500  
Bedford and Luton-01234 310070  
West Essex- 01279 827626  

Please state the approximate quantities of waste they anticipate generating and agree a frequency for service and destruction.

Containers will include:
- Blue Wheelie bins
- Grey consoles
- Blue or white plastic sacks

**Please note:**
- Wards and departments must not make their own arrangements with external contractors to dispose of their confidential waste.

3.2 All bins are to remain locked at all times & bags must be stored securely to prevent unauthorised access. Responsibility for secure storage lies with the producers of the waste.

3.3 Keys to confidential waste storage containers and compounds must be kept secure at all times by a nominated authorised person(s) on individual sites.

### 4.0 RETRIEVAL OF INCORRECTLY CONSIGNED CONFIDENTIAL MATERIAL

4.1 In the event that confidential waste /data/material is mistakenly or accidently placed in a secure confidential waste container, a request can be made to an authorised person (Typically a Building Administrator or Team Manager) to open the container or compound.

4.1.1 If keys are not available the authorised person should place a ‘Do not remove notice’ on the lid of the waste container. The Estates and Facilities Department must be informed so that they can postpone the scheduled collections of the waste containers and to arrange for the bin to be opened with duplicate keys.
4.2 The authorised person(s) will act as a witness to the opening, retrieval of the ‘confidential data’ and relocking of the confidential waste container to maintain the secure handling and disposal of confidential waste process.

4.3 After the event the authorised person(s) and the requestor must sign a Retrieval Form (see appendix 1) to record and evidence the event. The original requestor must also inform the Information Governance department of the event by sending a copy of the Retrieval Form.

5.0 DESTRUCTION OF CONFIDENTIAL WASTE

5.1 Confidential waste must be destroyed, either by using a dedicated, approved service arranged by the Estates and Facilities Department or by shredding the unwanted data using a cross cut shredder.

5.2 Charges for the confidential waste destruction service will be paid for by the wards, department etc. producing the waste.

5.3 Where appropriate, i.e. designated areas only producing small quantities of confidential documents, it is permissible to shred waste using a cross cut shredder.

5.3.1 Shredded confidential waste can be placed in a clear recycling bag before being placed in the recycling bin.

5.4 In the event of a ward/department having a large quantity of confidential waste to be destroyed, the Estates and Facilities Department will make the necessary arrangements for the most cost effective method of destroying the waste.

5.5 Any queries regarding the storage and destruction of confidential waste should be directed to either the Estates Facilities Department (see 3.2) or one of the Information Governance Leads:
   - Associate Director of Electronic Systems and Information Governance
   - Head of Performance and Information
   - Head of IT Service Delivery and Customer Services
   - Information Governance Manager

END