



## Records Management Policy

Document Profile Box	
Document Category / Ref	QSSD 1315
Version:	0003.1
Ratified by:	Governance & Risk Committee
Date ratified:	5 <sup>th</sup> January 2011
Name of originator / author:	Information Governance Manager
Name of responsible committee / individual:	Information Governance Working Group
Date issued:	January 2011
Review date:	January 2012
Target audience:	All staff
Document owner:	Director of Strategy & Business Development
Approved by:	

## Version Control

Version	Release Date	Author	Status	Comments
0001	Feb 2008	Mark Glencorse	Approved	
0002	Sept 2008	Rahima Hoque	Draft	Reviewed to ensure the policy follows the structure identified in the Organisational-wide Policy for the Development and Management of Procedural Documents and the CNST requirements.
0003	Feb 2009	Rahima Hoque	Draft	Amendments applied following new guidance.
0003	Sept 2009	Rahima Hoque	Final	Following ratification.
0003.1	Nov 2009	Rahima Hoque	Final	Document owner added to profile box. Table of contents updated. 9.4 reference updated.
0004.0	Dec 2010	Syma Dawson	Draft	Review following NHSLA requirements re: retrieval of records

### Did you print this document yourself?

Please be advised that the Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version.

### Document Location

The source of the document will be found in the Trust Quality System.

### Freedom of Information Act 2000 Access

This document will be available via the NEAS Publication Scheme.

## TABLE OF CONTENTS

	<b>PAGE</b>
<b>1. INTRODUCTION</b>	<b>1</b>
<b>2. PURPOSE</b>	<b>2</b>
<b>3. SCOPE</b>	<b>2</b>
<b>4. DEFINITIONS</b>	<b>2</b>
<b>5. RESPONSIBILITY AND ACCOUNTABILITY</b>	<b>3</b>
<b>6. EQUALITY AND DIVERSITY STATEMENT</b>	<b>5</b>
<b>7. LEGAL AND PROFESSIONAL OBLIGATIONS</b>	<b>5</b>
<b>8. STANDARDS OF RECORDS MANAGEMENT</b>	<b>6</b>
<b>9. POLICY SPECIFIC TO PERSONAL RECORDS</b>	<b>13</b>
<b>10. POLICY SPECIFIC TO CORPORATE RECORDS (NON-CLINICAL)</b>	<b>15</b>
<b>11. RETENTION SCHEDULES</b>	<b>15</b>
<b>12. RECORDS AUDITS</b>	<b>18</b>
<b>13. CONSULTATION, APPROVAL AND RATIFICATION PROCESS</b>	<b>18</b>
<b>14. REVIEW AND REVISION ARRANGEMENTS</b>	<b>19</b>
<b>15. DISSEMINATION AND IMPLEMENTATION</b>	<b>19</b>
<b>16. DOCUMENT CONTROL INCLUDING ARCHIVING ARRANGEMENTS</b>	<b>19</b>
<b>17. MONITORING COMPLIANCE WITH AND THE EFFECTIVENESS OF PROCEDURAL DOCUMENTS</b>	<b>20</b>
<b>18. REFERENCES</b>	<b>21</b>
<b>APPENDIX A – EXAMPLES OF STRUCTURED RECORDS</b>	<b>22</b>

## 1. Introduction

- 1.1. A systematic and structured approach to Records Management within any NHS organisation ensures that information is accurate, up to date and accessible when it is needed. The North East Ambulance Service (NEAS) recognises the importance of effective records management and is committed to providing high-quality information as it underpins the delivery of high-quality healthcare, and many other key service deliverables.
- 1.2. Records Management is the process by which an organisation manages all aspects of records, which can be generated internally or externally in any format or media type, from their creation, throughout their lifecycle and to their eventual disposal.
- 1.3. This policy outlines the NEAS' records management system, which aims to ensure that records are managed and controlled effectively, and at best value, meet legal, organisational and information needs. The policy should also be read in conjunction with the Records Management Strategy which sets out how the policy requirements will be delivered.
- 1.4. Records held by NEAS are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations throughout the Trust. These records support policy development and managerial decision-making, protect the interests of the Trust and the rights of patients, employees and members of the public. They support consistency, continuity, efficiency and productivity and help to deliver services in consistent and equitable ways.
- 1.5. The Trust is committed to ongoing improvement of the records management functions which will result in a number of organisational benefits including:
  - Better use of physical and server space.
  - Better use of staff time.
  - Improved control of valuable information resources.
  - Compliance with legislation and standards.
  - Reduced costs.
- 1.6. The NEAS makes every effort to ensure its records management practice and standards are in line with legislation and national guidance, including;
  - Common Law Duty of Confidence.
  - Records Management: NHS Code of Practice.
  - Data Protection Act 1998.
  - Freedom of Information Act 2000.
  - IG Toolkit requirements in regards to the recording of patient information on health records with respect to their individual health profession.
  - IG Toolkit requirements regarding access to patient information

## 2. Purpose

- 2.1. The purpose of this policy is to provide guidance to staff to carry out their record management responsibilities and to ensure alignment with the Trust's business objectives whilst meeting their obligations in terms of legal and national guidance.
- 2.2. A number of organisational benefits will be gained from doing so. These include:
  - Compliance with legislation and standards.
  - Improved control of valuable information resources.
  - Better use of physical and server space.
  - Better use of staff time.
  - Reduced costs.

## 3. Scope

- 3.1. This policy relates to all clinical and non-clinical records held in any format (paper records, reports, diaries and registers etc, electronic records including e-mails, x-rays and other images, microform (i.e. microfiche and microfilm), and audio and video tapes) by the Trust including all administrative records (e.g. personnel, estates, financial and accounting records, contemporaneous notes associated with for e.g. complaints); and all patient health records.
- 3.2. The policy covers the management of records and not the detailed requirements of what a record should contain for either corporate or clinical use. For guidance on these matters see departmental policies.

## 4. Definitions

- 4.1. **Records Management** is described in the NHS Records Management Code of Practice as 'the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records'.
- 4.2. **Information** is a corporate asset. The Trust's records are important sources of administrative, clinical, evidential and historical information. They are vital to the Trust to support its current and future operations, for the purpose of accountability (including meeting the requirements of Freedom of Information (FOI) legislation), and for an awareness and understanding of its history and procedures.
- 4.3. **Records** are defined as 'recorded information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity'. They are the final versions of documents and do not change e.g. policies, minutes.
- 4.4. **Documents** are work in progress by an individual or group of individuals.

- 4.5. **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.
- 4.6. **The Caldicott Guardian** is the Director of Clinical Care and Patient Safety and is responsible for approving and ensuring that national and local guidelines and protocols on the handling and management of confidential patient information are in place.

## 5. **Responsibility and Accountability**

5.1. The Chief Executive, Executive Directors and Senior Managers have corporate responsibility and accountability for overseeing the implementation of this policy and appropriate aspects of records management within their remits.

5.1.1. **All staff** have a responsibility to:

- Whether clinical or administrative, all staff who create, receive and use records have records management responsibilities.
- Maintain awareness that any records created are not their personal property, but belong to the Trust and understand their responsibilities under legislation, particularly their responsibilities under the Data Protection Act 1998 (DPA) and Freedom of Information Act (FOI) 2000.
- All staff have a personal Common Law Duty of Confidence, and should share records and the information they contain in accordance with the Trust(s) Information Sharing Protocols.
- Staff may only access those records that are relevant to their current job roles and where appropriate authorisation has been obtained.
- Paper records - staff must ensure that paper records are kept secure, active records should be kept in locked cabinets and access to them appropriately restricted.
- Records must be accessible when required and securely disposed of when no longer required.
- Electronic records - staff must always log out of any computer system or application when work on it is finished, they must never leave terminals unattended and logged in.
- Staff must only access systems using their own allocated logins. They must never share these logins with others. Where appropriate a password-protected screen saver should be used to prevent casual viewing of confidential information.
- It is the responsibility of all appointing officers to ensure that responsibilities for records management are written into all accountable individuals job descriptions.

5.1.2. **Line managers** have a responsibility to:

- Ensure all current, new and temporary staff are appropriately trained in records management in line with the requirements of their post.

- Take active responsibility for records management and for ensuring that all staff are involved in the programme for implementing the records management policy.
- 5.1.3. The **Data Quality and Records Management group** (which consists of Records Management Officers) has a responsibility to:
- Implement, review and promote the records management policy
  - Regularly monitor standards for health care and corporate records
  - Report (non) compliance with Information Quality and Records Management standards
  - Document, implement and monitor controls within electronic and paper records management systems, including access controls
  - Ensure that record audits are conducted on a regular, systematic basis to provide assurance that current controls are working effectively
  - Report any confidentiality breaches or potential risks of confidentiality breaches to the Information Governance Working Group (IGWG).
- 5.1.4. **The Caldicott Guardian** has responsibility to:
- Reflect patients' interests regarding the management and use of patient information and their records.
  - Ensure patient identifiable information is shared in an appropriate and secure manner in line with the Caldicott Principles.
- 5.1.5. **Clinical departmental managers** are responsible for the implementation of the annual audit of health records. NCS 1999 / 065 (Clinical Governance in the new NHS), quotes as one of the four main requirements of Clinical Governance: "Effective monitoring of clinical care with high quality systems for clinical record keeping and the collection of relevant information". They are also responsible for the development and maintenance of health records management practices throughout the Trust, in particular got the drawing up of good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.
- 5.1.6. **Directorate senior managers** are responsible for periodically reviewing records in line with their retention schedules (it is recommended that this is done every 12 - 18 months).
- 5.1.7. **The Data Protection Lead** has responsibility for:
- Providing guidance on records management issues in relation to the legislation and for ensuring that related policies and procedures conform to the latest legislation and NHS guides on Data Protection, patient confidentiality, information security and rights of access to information.
- 5.1.8. **The FOI Lead** has responsibility for:
- Facilitating requests for information under the legislation, and for maintaining the Trusts Publication Schemes and maintaining the Trusts Information Asset Registers.

5.1.9. **Human Resources** are responsible for ensuring that staff induction programmes include reference to records management.

5.1.10. **IT** are responsible for providing the infrastructure to support electronic record keeping.

## **6. Equality and Diversity Statement**

6.1. The Trust is committed to providing equality of opportunity, not only in its employment practices but also in the services for which it is responsible. As such, this document has been screened, and if necessary an EIA has been carried out on this document, to identify any potential discriminatory impact.

6.2. If relevant, recommendations from the assessment have been incorporated into the document and have been considered by the approving committee. The Trust also values and respects the diversity of its employees and the communities it serves. In applying this policy, the Trust will have due regard for the need to:

- Eliminate unlawful discrimination.
- Promote equality of opportunity.
- Provide for good relations between people of diverse groups.
- For further information on this, please contact the Equality and Diversity Department.

## **7. Legal and Professional Obligations**

7.1. Once created records become public under the Public Records Act 1958 and all NHS organisations have a duty under this legislation to make appropriate arrangements for the effective management of their records. These records include:

- Patient health records (electronic or paper-based).
- Administrative records (including personnel, estates, financial and accounting records, notes associated with complaint handling).
- Material intended for short-term or transitory use, including notes and spare copies of documents.
- Computer databases, output and disks.
- E-mails and other computerised records.
- Audio and visual tapes, cassettes, CD-ROM etc.
- Photographs, slides and other images.
- Microfiche or film.
- Scanned records.
- Text messages.

7.2. It is individuals within an NHS organisation that are responsible for any records they create or use in the performance of their duties. This responsibility is established at, and defined by,

law. It is therefore imperative that all employees of the Trust make themselves aware of their obligations and responsibilities described within this policy and the associated guidelines.

7.3. In addition to the Public Records Act there is a further range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and a range of statutes that permit or require information to be used or disclosed. Additionally clinicians are under a duty to meet records management standards set by their professional regulatory bodies.

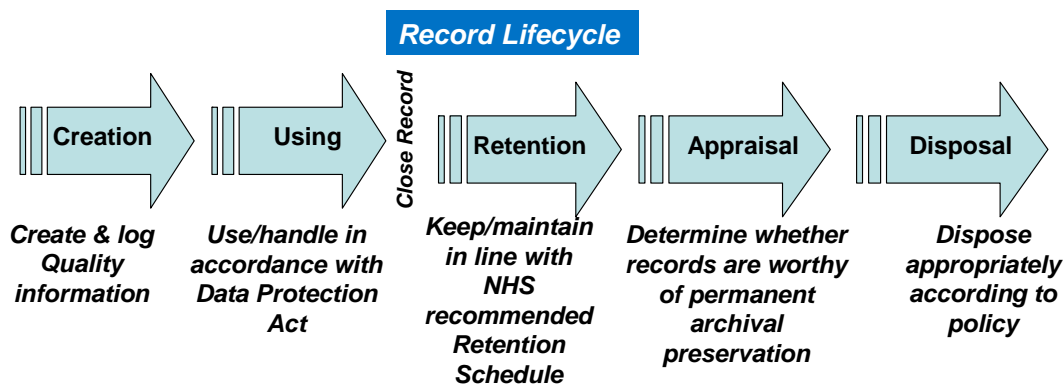
7.4. The Trust will comply with the following legislation and other legislation as appropriate:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality and the NHS Confidentiality Code of Practice
- Access to Health Records Act 1990
- Health Professions Council Code of Professional Practice

7.5. The Records Management: NHS Code of Practice published by the Department of Health in 2006 details guidelines for the management of all types of NHS records. Additionally the Department of Health Standards for Better Health describes the level of quality that health care organisations are expected to meet. This policy has been based on the requirements contained within these documents.

## 8. Standards of Records Management

From the moment a record is created or received until it's ultimate disposal, the Trust must ensure that both the quality and quantity of information it generates is controlled, that the information is maintained in a manner that effectively services the needs of the organisation and its stakeholders and that it disposes of the information appropriately when it is no longer required. In order to ensure that records are managed and controlled effectively commensurate with legal, operational and information needs the following key components of records management must be considered:



## 8.1. **Structured record keeping**

Where the Trust's business requires a collection of information using a numbering system that is accessed by more than one person, such records must be capable of being identified and retrieved as needed. This covers all records holding personal information. A list of examples that may be classified as structured records is attached Appendix A. Structured systems should be monitored regularly and reviewed at least once every two years to ensure that they continue to operate effectively and efficiently and meet the needs of users.

## 8.2. **Record creation**

8.2.1. In the creation of a record, that is anything which contains information which has been created or gathered as a result of any aspect of Trust work, consideration must be given to what is being recorded, how it is being recorded and why. This is to ensure that the records which are created are not only adequate and consistent but necessary for statutory, legal and business requirements.

8.2.2. Records are valuable because of the information held in them. This information can only be of use if it is legible, up to date and easily accessible. Trust records should be accurate and complete to allow Trust employees and their successors to undertake appropriate actions in the context of their responsibilities, to protect the legal and other rights of the Trust and its stakeholders and to provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.

8.2.3. Records created by the Trust should be arranged in a record keeping system that will enable the Trust to obtain the maximum benefit from the quick and easy retrieval of information. This will include a set of rules for referencing, titling, indexing and, if appropriate, security marking records which are easily understood and enable the efficient retrieval of information. Mechanisms through which the departments can register the records they are maintaining will need to be established.

8.2.4. The Trust Business Continuity Plan must identify the arrangements that are in place to provide protection for all the organisations records that are vital to the continued functioning of the organisation.

## 8.3. **Updating records**

### 8.3.1. **All records**

All record entries must:

- Be factual, consistent and accurate.
- Be recorded as soon as possible after an event has occurred
- Keep the use of abbreviations to a minimum. If abbreviations are used, they should be from an agreed list which can be made available on request.

### 8.3.2. **Hand written records**

Hand written record entries must:

North East Ambulance Service NHS Trust  
Records Management Policy

- Be written clearly, legibly and in such a manner that they cannot be erased.
- Be readable on any photocopies.
- Not have errors cancelled using erasers, liquid, paper or any other obliterating agents. A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment.
- Be accurately dated, timed and signed, with the signature being printed alongside the first entry.
- Be consecutive.
- Be bound and stored so that loss of documents is minimised.
- Be written in black ink.

#### 8.4. **Storage of records**

8.4.1. The following factors should be taken into account when considering how records will be stored:

- Security of the records.
- Health and safety requirements.
- Access requirements (i.e. how accessible does the record need to be).
- The type of record being stored and its environmental requirements (e.g. electronic storage media should not be placed in close proximity to strong magnetic fields).
- The choice of media should be based on consideration of practicality and costs.

8.4.2. Paper should be used where the original record of an event may be required – for example:

- Patient records, until superseded by electronic records.
- Quotations and signed contracts.
- Signed minutes of meetings.
- Original job applications.

This list is not exhaustive.

8.4.3. For the majority of working documents, storage in electronic format is preferred because of convenience, cost, efficiency and security.

#### 8.5. **Means of storage**

8.5.1. Records must be stored in a way that allows the information contained within them to be available when they are needed, where they are needed, and by the person who needs them. The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with and that there is an auditable trail of these record transactions.

8.5.2. Current records should be stored in the business area adjacent to users held in a secure location when not being used e.g. lockable filing cabinets, cupboards, rooms (locked and / or alarmed when out of normal working hours). Storage locations should be clean and tidy with

proper environmental controls and adequate protection against fire and flood and should provide a safe working environment for staff.

8.5.3. Records should be closed as soon as they have ceased to be active for use other than reference. Where records are no longer required for the conduct of current business their placement in a designated storage (place of deposit) area with specified destruction dates is more economical and efficient. These must be controlled via formal contracts that clearly stipulate storage, security and retrieval requirements.

8.5.4. Electronic records should be stored in folders that have been designed to enable security and ease of:

- Storage and back-up.
- Access.
- Folder designs, including security controls, to be approved by the record owners.
- Technical matters in respect of storage will be covered by the Information Security Policy.

In terms of back up, these should be designed with schedules to ensure continuing access to readable information.

8.5.5. Other media

- In the case of photographs, the quality of the images available from negatives or original prints should be considered and new prints may be made in cases where the original is deteriorating.
- Film should be stored in dust-free metal cans and placed horizontally on metal shelves.
- Sound recordings and video recordings (tapes and DVDs) should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

8.5.6. All staff need to be aware that the DPA is equally applicable to identifiable images or audio recordings as it is to written records.

8.5.7. The licence conditions of the Telecommunications Act 1984 require the Trust to make every reasonable effort to inform callers if their calls are liable to be recorded, and maintain a record of the means by which callers have been informed. If there is any circumstance in which a patient's telephone call may be recorded (e.g. within control, complaints etc), the patient must be informed of this. It is not permitted to make intentionally secret recordings of a patient's telephone call.

8.5.8. Scanning

The option of scanning paper records into electronic format may be considered for reasons of business efficiency, to address problems with storage space or to include a record of a paper document within an existing electronic record. Where this is proposed, the following factors should be taken into account:

- Costs.

- Archival Value.
- The need to protect the evidential value of the record by copying and storing in accordance with British Standards. In particular, the Code of Practice of Legal Admissibility and Evidential Weight of Information Stored Electronically (BIP 0008) should be adhered to.
- Current regulations relating to the use of scanned documents with existing electronic records.

## 8.6. **Transporting records**

### 8.6.1. Manual records

Where manual records containing person-identifiable information are transported the following guidelines must be followed.

- Records must be placed in new sealed envelopes clearly marked confidential.
- Envelopes must be clearly marked with the name of the recipient (not just the name of the department).
- When posted outside of the Trust(s) i.e. via Royal Mail a level of assurance commensurate to the level of risk resulting from loss should be applied. E.g. where a copy of a case file is being sent, it may be appropriate for that information to be sent via Special Delivery, due to the amount of confidential information contained within the file. The level of assurance applied should be determined via local guidelines and operational procedures.

### 8.6.2. Electronic records

Person identifiable information held in electronic format must not be transferred on portable storage media devices (USB memory sticks, laptops, etc) unless encrypted. Where records need to be routinely transported in this manner without encryption, approval in writing must be obtained from Information Governance Lead. Where there is an immediate need, authorisation must be obtained from a Trust Director.

8.6.3. Taking person identifiable records off site e.g. home is strictly prohibited.

## 8.7. **Tracking records**

8.7.1. Fast and efficient access to records releases the information and knowledge they contain. However, records must be kept securely to protect the confidentiality and authenticity of their contents, and to provide further evidence of their validity in the event of a legal challenge. Employees should only have access to those parts of the records required for them to carry out their role.

8.7.2. Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. The movement and location of records should be controlled to ensure that a record can be easily located and retrieved at any time as records can become misplaced or lost when they are removed from their source and their next destination not clearly recorded.

8.7.3. Different methods of tracking such as paper registers, diaries and log books may be used but it is essential that all employees handling records are familiar with the system in place and comply with it. Tracking mechanisms should record:

- The item reference number or identifier.
- A description of the item (file title).
- The person / department or place to whom it is being sent.
- The reason for the request and the date of transfer and return.

8.7.4. Requests for records access should be logged and periodically audited to ensure compliance with legislative requirements.

8.7.5. Borrowers of records are personally responsible for the security and subsequent return to the place of storage for every set of record that they borrow.

## 8.8. **Retention of records**

8.8.1. Regardless of the type of record, there is a requirement to keep records for a minimum period of time. The length of time for retaining records will depend on the type of record and its importance to the Trust's business functions. There is also a legal requirement under the DPA that personal information should not be kept for longer than is necessary.

8.8.2. The Trust has adopted the retention periods set out in the Records Management: NHS Code of Practice and it is a fundamental requirement that Trust records are only retained for the specified periods of time for legal, operational, research and safety reasons.

## 8.9. **Retrieving Records**

8.9.1. In order to ensure the successful retrieval of records, it is important that information is arranged and stored in a record-keeping system (see section 8.1). This will enable the quick and efficient retrieval of information when required but also, enable the implementation of authorised disposal of records in line with the Trust's Records Retention Schedule.

8.9.2. The Clinical Audit department securely store all paper Patient Report Forms (PRFs), immediately following their arrival from the courier. Paper PRFs are stored in a locked cupboard and the locked scanning room which can only be accessed by authorised personnel. The paper PRFs are filed by station and week to ensure successful retrieval of records.

8.9.3. Should a member of staff wish to retrieve a record that contains person-identifiable or confidential information in regards to another individual, i.e. PRF or control report (including e-PRF), then a justified reason for the request must be obtained e.g. clinical investigation or child death review etc. Staff can submit their requests to the Clinical department using the request form provided on the intranet under 'Information Governance'.

8.9.4. All requests for information are logged with the Clinical Administration Assistant and in some cases, may require authorisation from either the Caldicott Guardian or Information Governance Manager. The disclosure of such information must always meet information governance requirements that are subject to the Data Protection Act 1998 and other relevant legislation.

8.9.5. Under the right of subject access of the Data Protection Act 1998, an individual is entitled to retrieve their own personal data; staff should refer to the subject access procedure for further information.

#### 8.10. **Archiving records**

8.10.1. A review should be made of the records to determine whether records should be selected for preservation, retained or disposed.

8.10.2. The purpose of the appraisal process is to ensure that records are examined at the appropriate time to determine whether or not they are worthy of archival preservation, whether they need to be retained for longer as they are still in use or whether they should be destroyed. Record owners should determine whether records which have been retained for the minimum required period are to be selected for permanent preservation, destroyed or retained by the Trust basing their decisions on the need to preserve records which may be of value to future employees or influenced by local factors such as ongoing research.

8.10.3. Records identified for permanent preservation must be transferred to the appropriate repository e.g. the County Archive or Public Records Office.

#### 8.11. **Disposal of records**

8.11.1. The specified periods define when a review should be made of the records to determine whether records should be selected for preservation, retained or disposed of bearing in mind that the destruction of records is an irreversible act but the cost of keeping them is high and ongoing.

8.11.2. Where the need for disposal has been identified secure destruction of the record must be carried out as many Trust records contain sensitive and / or confidential information.

8.11.3. Destruction of all records, regardless of the media, should be conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure. The normal destruction method for paper records used within the Trust is shredding, undertaken by an approved contractor. There must be a formal contract between the contractor / supplier and the Trust which details the security and confidentiality requirements associated with the transportation and destruction of confidential information.

8.11.4. Record owners should compile a register of records which have been destroyed providing details of the type of record, when it was generated, when it was destroyed and by whom.

8.11.5. Secure destruction of electronic records will be undertaken by IT experts within the Trust.

#### 8.12. **Record of disposal**

8.12.1. When records are disposed of it is necessary to record the disposal. A Records Disposal Notification form should be completed and retained by the relevant department for 30 years.

8.12.2. If records or documents are disposed of, in error, before the end of their retention period, A Records Disposal Notification form should be completed and clearly marked "Disposal within minimum retention period" and a NEAS07 form should be completed, so that the risks

associated with inappropriate disposal can be assessed and managed, and any necessary actions can be taken.

8.12.3. If it is found that records have been deliberately and inappropriately disposed of, or otherwise altered, to prevent lawful access under the DPA, FOI or other relevant legislation, the parties responsible will be liable to disciplinary action (under the NEAS Disciplinary Policy) and may also be liable to criminal prosecution.

### 8.13. **Disclosure and public access to records**

8.13.1. Access to personal information is permitted via the DPA and is covered within the Trust(s) Data Protection Policy. Staff must refer to these for further guidance.

8.13.2. Access to the health records of deceased patients is permitted in certain circumstances by the Access to Health Records Act 1990. Access is limited to the personal representative of the deceased patient or any person who may have a claim arising out of the patient's death.

8.13.3. Access to corporate information is permitted via the FOI and is covered within the Trust(s) FOI Policy. Staff must refer to these for further guidance.

8.13.4. It is a criminal offence to alter, deface, block, erase, destroy or conceal information to prevent lawful access, unless the NEAS is exercising a statutory exemption from disclosure in accordance with the above Acts.

8.13.5. If NEAS receives a request for access to a record or document that is due for disposal, the normal procedure for processing access requests will be followed.

8.13.6. No member of staff should dispose of a record – even if its retention period has expired - if they are aware that it is subject to an information request, until they have been advised by the relevant department that the processing of the request has been completed (including the appeals process, if appropriate).

## 9. **Policy Specific to Personal Records**

9.1. Records holding personal identifiable information on staff and the public will need to be managed in accordance with the DPA and the common law duty of confidence. Where data are not capable of identifying anyone either directly or indirectly or where they have been effectively anonymised, neither the DPA nor the common law duty of confidence applies.

9.2. Personal information processed or kept for any purpose:

- Should not be kept for longer than is necessary for that purpose.
- Should not be passed on to others without the individual's consent except as permitted under schedule 2 and 3 of the DPA or, where applicable, under the common law where there is an overriding public interest.

Further guidance on disclosing patient information can be found within the Data Protection Policy and Confidentiality Policy.

9.3. Creating records – When records containing personal information are created, it is essential that indices are first checked to avoid duplicate records being created for the same person e.g. records held on any patient information system.

9.4. Creating new record collections – If any new record collections are created containing personal information, the Personal Data Report Form must be completed and sent to the Data Protection Officer. This ensures that the requirements of the DPA and the Caldicott Report are met.

### 9.5. **Structured record keeping of personal records**

9.5.1. Records will be deemed structured by:

- The allocation of a unique identifier; such as medical record number, NHS number, or name and date of birth.
- The identifier will be recorded:
  - on the file cover for paper records, and
  - in a 'register' or index to enable the record to be found.

9.5.2. With the development of electronic patient records, the NHS number will become the unique identifier for all records. Systems should be monitored regularly and reviewed at least once every two years to ensure that they continue to operate effectively and efficiently and meet the needs of users.

9.5.3. Determining which records require structured record keeping is a decision that should be made by staff with advice from the IGWG, and, in the case of clinical records between the Clinical Records Lead and the Caldicott Guardian.

### 9.6. **Updating records**

9.6.1. Clinical electronic records must:

- Be accurately dated, timed and with the identity of the user assigned to each entry.
- Have an integral audit trail providing at least the equivalent information.

9.6.2. The method of updating records must be in accordance with extant clinical and human resources policies. However, no clinical or staff record should include:

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements.
- Personal opinions, unless these are professional judgements.

### 9.7. **Validating records**

9.7.1. All managers of personal records must have procedures in place to ensure the records are:

- Timely
- Accurate
- Complete
- Relevant

## **10. Policy Specific to Corporate Records (non-clinical)**

Records on corporate matters may be subject to the common law duty of confidence and may also be classified as sensitive or non-sensitive in terms of their impact on the running of the business if lost or leaked.

### **10.1. Creating records**

10.1.1. When records are created the following standards must be applied:

- The file title must be unique and accurate.
- Where appropriate, there must be a description of the content, the department, the service and the name of the person responsible for creating the document.
- Documents must be stored in files as per the stated referencing system.
- The date of creation.
- Any security markings.
- Each department should keep an index of the categories of the files kept.
  - The index to be developed to include the full details of each file only when a full electronic management system has been implemented.

### **10.2. Updating records**

10.2.1. Corporate electronic records must be:

- Kept up-to-date and accurate.
- Easily accessible when needed.
- Managed in accordance with the requirements of the Information Security Policy.

### **10.3. Validating records**

The fitness for purpose of the Trust's corporate records will be agreed by managers responsible for its business processes.

## **11. Retention Schedules**

11.1. The records retention schedules provide information about all records commonly found within NEAS. For ease of use, there are separate schedules relating to health and corporate (i.e. non-health) records. The retention schedules apply to all the records concerned, irrespective of the format (e.g. paper, databases, e-mails, photographs, CD-ROMs) in which they are created or held.

### **11.2. Interpretation of the schedules**

11.1.1. Type of record: lists alphabetically records created as part of a particular function. The business and corporate records schedule has grouped together records of major functions commonly found in NHS organisations.

11.1.2. Minimum retention period: 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. If records need to be kept longer than the recommended minimum period, then the period can be varied accordingly with the decision and the reasons behind it, on its own retention schedule. Records selected for permanent preservation by the relevant place of deposit should normally be transferred there as soon as they reach the retention period specified and in any case before they reach 30 years old, unless a longer operational retention period is specified in this schedule, in which case transfer should take place as soon as possible after this period has been reached. NHS organisations wishing to keep records more than 30 years old for operational reasons beyond the minimum period specified in this schedule should consult The National Archives for advice. Note that transfers of selected records to places of deposit will be covered by Condition 7(1) of Schedule 3 and s.33 of the DPA.

11.1.3. Derivation: notes the details of legislation and any other references of relevance to the recommended minimum retention period.

11.1.4. Final action: at the end of the relevant minimum retention period, one or more of the following actions will apply:

- Review: records may need to be kept for longer than the minimum retention period due to ongoing administrative need. As part of the review, the organisation should have regard to the fifth principle of the DPA, which requires that personal data is not kept longer than is necessary. If it is decided that the records should be retained for a period longer than the minimum (provided that this does not total a period of 30 years or more from creation, in which case see the comments on the minimum retention period above), the internal retention schedules will need to be amended accordingly and a further review date set. Otherwise, one of the following will apply:
- Transfer / consult a Place of Deposit or The National Archives (see 'Archives' section below): if the records have no ongoing administrative value but have or may have long-term historical or research value, or they have some administrative value but are more appropriately held as archives. Records with such value must be transferred to the organisation's approved Place of Deposit. Where the organisation has no existing relationship with a Place of Deposit, The National Archives should be contacted in the first instance. Where an organisation is unsure whether records may have archival value, The National Archives or the Place of Deposit with which the organisation has an existing working relationship should be consulted.
- Destroy: where the records are no longer required to be kept due to statutory requirement or administrative need and they have no long-term historical or research value. In the case of health records, this should be done in consultation with clinicians in the organisation (see section 11.3 below).

## 11.2. Retention periods

- 11.2.1. As previously stated, records should not ordinarily be kept for longer than 30 years. The Public Records Act does, however, provide for records, which are still in current use to be legally retained. Additionally, under separate legislation, records may be required to be retained for longer than 30 years (e.g. Control of Substances Hazardous to Health Regulations).
- 11.2.2. Also, in respect of any records that contain personal data as defined by the DPA, consideration should be given to the fifth principle of the Act, i.e. that 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'. Note that transfers of selected records to places of deposit will be covered by Condition 7(1) of Schedule 3 and s.33 of the DPA.
- 11.3. **Who makes the decision regarding disposal and destruction of records?**
- 11.3.1. There are two principal options: to dispose (e.g. by passing on to another organisation) or to destroy. Staff in the operational area that ordinarily uses the records will usually be able to decide. Senior managers are responsible for making sure that all records are periodically and routinely reviewed to determine what can be disposed of or destroyed in the light of local and national guidance.
- 11.3.2. In respect of health records, it is recommended that a multi-disciplinary Health Records Committee and / or Health Records User Group should be established to provide advice on local policy, particularly for the retention, archiving or disposal of sensitive personal health records. Input from local healthcare professionals should be a key element of any records management strategy.
- 11.3.3. Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Because of the sensitive and confidential nature of such records and the need to ensure that decisions on retention balance the interests of professional staff, including any research in which they are or may be engaged, and the resources available for storage, it is recommended that the views of the profession's local representatives should be obtained.
- 11.3.4. Although retention schedule has been condensed to contain the most common types of records held by NEAS, those responsible for records management may wish to consult the full Code for the comprehensive list in regards to record type and category. However, it is not possible to list every type. Where a record type is not listed record holders should consider how other organisations manage these record types and should carry out a risk assessment of the pros and cons of destroying the record or maintaining it for a prolonged period in order to decide how best to manage the record.
- 11.3.5. Attention should also be paid to other retention periods for similar record types. The decision process around why a particular record type may be maintained or destroyed should be clearly documented.

## **12. Records audits**

12.1.1. An effective records management programme depends on the knowledge of what records are held, in what form they are accessible and their relationship to organisational functions. An information audit has been undertaken to establish a Trust wide information asset register so as to meet this requirement as well as to help promote control over the records and provide valuable data for developing records appraisal and disposal procedures.

12.1.2. Regular programmes of audit of compliance with records management standards will be established. The results from these audits will be reported to the Trust Board with evidence of action on the audit results to improve and maintain the organisations performance on records management.

12.1.3. The audit will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and / or guidance should comply with the policy.
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be made.
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance.
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

## **13. Consultation, Approval and Ratification Process**

### **13.1. Consultation**

13.1.1. This document has been produced by the author on behalf on the IGWG. This group was consulted upon and their comments added to the document as appropriate.

### **13.2. Approval and Ratification**

13.2.1. The Trust Policy Review Group is the committee with the authority for the review of this document. The Joint Consultative Committee and the Trust Board have responsibility for ratification of this policy.

13.2.2. The IGWG has carried out a full and proper consultation and has considered the content of the document in terms of current best practice, guidelines, legislation and mandatory and statutory requirements, in considering the document for approval the committee also took into account the results of the recommendations of the EIA.

## **14. Review and Revision Arrangements**

14.1. The document will be reviewed every 2 years or when appropriate after changes in legislation or guidance. The document owner will be responsible for this review.

## **15. Dissemination and Implementation**

### **15.1. Dissemination**

15.1.1. This policy is available for all staff to access via the Trust Quality System. Staff without computer network access should contact their line manager for information on how to access policies.

15.1.2. All staff will be notified of new or revised documents via internal communications systems.

15.1.3. This document will also be included in the Publication Scheme for NEAS in compliance with the FOI Act 2000.

### **15.2. Implementation**

15.2.1. This policy will be implemented in the following ways:

- Regular communications to staff on new policies and procedures through IG Circulars.
- Regular audit of IG processes undertaken in line with policies and procedures in key areas i.e. records management, confidentiality, information security, FOI and data quality.
- Monitoring through the IGT.

### **15.3. Training**

15.3.1. Training will be regularly assessed and refreshed in order that staff may remain appropriately skilled / knowledgeable over time.

15.3.2. Broad IG training will be included in the Trust induction programme. Additional training can be requested at the discretion of a manager, or by an individual wanting personal development along with mandatory yearly update training.

15.3.3. Further guidance and information relating to data protection issues will be distributed periodically via various media including the intranet site, 'The Pulse' (monthly service journal) and via email.

## **16. Document Control Including Archiving Arrangements**

### **16.1. Register / library of procedural documents**

All documents shall be held within the Trust Quality System and will be managed in line with quality standards.

### **16.2. Archiving arrangement**

Archiving of documents will be in line with this Records Management Policy.

## **17. Monitoring Compliance With and the Effectiveness of Procedural Documents**

### **17.1. Process for monitoring compliance**

17.1.1. All staff must adhere to this policy and comply with applicable UK legislation and any regulatory requirements for data protection.

17.1.2. Failure to follow this policy and related IG policy and procedures may lead to disciplinary, criminal or civil action being taken against the staff member.

17.1.3. Monitoring staff compliance through:

- Verifying that, where appropriate, agreement to disclosure decisions are recorded.
- Obtaining patient feedback of the process, e.g.:
  - Did they understand when and to whom their information would be disclosed?
  - Did they understand the choices available to them regarding disclosure?
  - Did they have the opportunity to ask questions and have them answered?
  - Did they understand that withholding of consent does not affect the way they are handled by staff but may reduce the number of treatment options available to them?
  - Did they feel under pressure to agree to disclosure?
- Evaluating whether staff understand disclosure issues and their responsibility for obtaining consent.
- Evaluate how staff handled questions about disclosure, and in particular review cases where:
  - Patients have declined to agree to disclosure.
  - Patients have changed their disclosure decision during the care episode.
  - A senior healthcare professional has overridden a non-disclosure decision

### **17.2. Standards and Key Performance Indicators**

There are a number of national standards and requirements relating to IG.

#### **17.2.1. Department of Health Records Management: NHS Code of Practice**

The Code of Practice replaces all previous directives relating to the management of NHS records. It provides practical guidance on managing records sets standards and includes a comprehensive retention schedule for all NHS records.

#### **17.2.2. IGT**

The connecting for Health IGT is a framework for implementing the IG agenda and consists of a series of requirements against which an organisation's current and planned attainment levels can be monitored. The Trust is required to complete a self assessment by 31st March each year, the results which will contribute to the assessment undertaken by the Healthcare Commission.

#### **17.2.3. Standards for Better Healthcare**

- The Department of Health's standards for better health include 24 core standards that all NHS healthcare providers in England should achieve, and 13 developmental standards that they should be working towards achieving.
- Core standard 13 requires that health care organisations have systems in place to ensure that:
  - Staff treat patients, their relatives and carers with dignity and respect;
  - Appropriate consent is obtained when required for all contracts with patients and for the use of any patient confidential information; and
  - Staff treat patient information confidentially, except where authorised by legislation to the contrary.

#### 17.2.4. NHS Litigation Authority

- The NHSLA Risk Management Standard for Ambulance Trusts applies to all Ambulance Trusts, are designed to address organisational, clinical, and non-clinical / health and safety risks.
- Parts of the Clinical Care standard are of relevance to IG, including patient / service user identification and quality of written and electronic clinical records.

## 18. References

- Department of Health: Records Management: NHS Code of Practice [http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT\\_ID=4131747&chk=tMmN39](http://www.dh.gov.uk/PublicationsAndStatistics/Publications/PublicationsPolicyAndGuidance/PublicationsPolicyAndGuidanceArticle/fs/en?CONTENT_ID=4131747&chk=tMmN39)
- NHS Connecting for Health: Records Management Roadmap <http://www.connectingforhealth.nhs.uk/infogov/records>
- NHS Connecting for Health IGT <https://www.igt.connectingforhealth.nhs.uk/>.

## **Appendix A – Examples of Structured Records**

The types of records most likely to be kept under a structured system include:

- Care / clinical records
- Personnel records
- Financial papers
- Estates papers
- Performance monitoring
- Policy papers (reports, correspondence, etc)
- Minutes, circulated papers etc of meetings
- Papers relating to the preparation of legislation
- Complaints papers and correspondence
- Research and development papers

This list is not exhaustive.

For further guidance please contact the IGWG.