The Trust strives to ensure equality of opportunity for all, both as a major employer and as a provider of health care. This Trust Records Policy has therefore been equality impact assessed by the Information Strategy Steering Group to ensure fairness and consistency for all those covered by it, regardless of their individual differences, and the results are shown in Appendix 1.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Purpose</td>
<td>3</td>
</tr>
<tr>
<td>Scope</td>
<td>3</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>4</td>
</tr>
<tr>
<td>Record Training</td>
<td>6</td>
</tr>
<tr>
<td>Legal Obligations applying to Records</td>
<td>6</td>
</tr>
<tr>
<td>Links to Other Trust Policies</td>
<td>7</td>
</tr>
<tr>
<td>Record Creation and Registration</td>
<td>7</td>
</tr>
<tr>
<td>Record Storage</td>
<td>8</td>
</tr>
<tr>
<td>Record Maintenance</td>
<td>9</td>
</tr>
<tr>
<td>Record Retention</td>
<td>10</td>
</tr>
<tr>
<td>Process for the Retention, Disposal and Destruction of Corporate Records</td>
<td>11</td>
</tr>
<tr>
<td>Process for the Retention, Disposal and Destruction of Patient Records</td>
<td>11</td>
</tr>
<tr>
<td>Confidentiality and Access</td>
<td>12</td>
</tr>
<tr>
<td>Non-Paper Records</td>
<td>13</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>14</td>
</tr>
<tr>
<td>Monitoring of Compliance with this Policy</td>
<td>15</td>
</tr>
<tr>
<td>Arrangements for Review of this Policy</td>
<td>16</td>
</tr>
<tr>
<td>Appendix 1 Equality Impact Assessment</td>
<td>17</td>
</tr>
<tr>
<td>Appendix 2 List of Key Legal and Professional Obligations Impacting</td>
<td>19</td>
</tr>
<tr>
<td>Records Management</td>
<td></td>
</tr>
<tr>
<td>Appendix 3 User Guide to Record Creation and Filing</td>
<td>24</td>
</tr>
<tr>
<td>Appendix 4 Administrative Records Retention Periods</td>
<td>28</td>
</tr>
<tr>
<td>Appendix 5 Guidance on Reviewing Trust Records Prior to Disposal</td>
<td>38</td>
</tr>
<tr>
<td>Appendix 6 Standards for Clinical Record Keeping in the Trust</td>
<td>39</td>
</tr>
<tr>
<td>Appendix 7 Audit of Clinical Record Keeping in the Trust</td>
<td>44</td>
</tr>
</tbody>
</table>
INTRODUCTION

1. It is recognised that the efficient and effective management of all records is a key component of Information Governance, and the Trust is following a strategy to improve performance in this area.

2. Information is of greatest value when it is accurate, up to date and accessible when needed. A comprehensive and effective system of records management coupled with appropriate education and training of staff will help achieve these objectives.

3. Health records are a tool of professional practice that are particularly important within the Trust. Accurate and timely documentation within both paper based, and electronic health records will determine accountability; facilitate clinical decision making; improve patient care through clear communication of the treatment rationale progress; provide a consistent approach to team working; and help defend complaints or legal proceedings.

4. This policy statement has been produced to set out the Trusts approach to records management and provide appropriate guidance to Trust staff on the management of records during their life cycle from creation to disposal.

5. Much of the information in this document has been reproduced from the NHS best practice guide ‘Records Management: NHS Code of Practice’ published in March 2006. Copies of this comprehensive guidance document can be downloaded from the following link:


PURPOSE

6. This policy is intended to:

   - Define duties and responsibilities in regard to records management in the Trust.
   - Outline the main legal obligations and statutory provisions that apply to records created and used within the Trust.
   - Provide a procedural framework with guidance to encourage best practice in records management within the Trust.
   - Specifically provide users of patient health records with guidance on their use and management including procedures for creation, tracking, retrieval, retention, disposal and destruction.
   - Identify the standards which must be used by all healthcare professionals for the completion of health records.
   - Outline the expectations in relation to records training for staff.
   - Outline a system for monitoring compliance and improvement.

SCOPE

7. This policy applies to records in all formats and media created or received in the course of the Trust's business. It outlines the personal and professional responsibility members of staff have for the records they use and create and
provides guidance on best practice and management of records during their life cycle from creation to eventual disposal.

8. The record types covered by this document include:

- Patient health records (paper and electronic including private patients seen in the Trust)
- Registers recording activities such as birth and operations
- Administrative and corporate records covering personnel, estates, financial and accounting activities
- Correspondence files
- X ray and imaging reports
- Photographs, slides and other images
- Audio and video tapes, cassettes and CD-ROM
- Microform (Microfilm/Microfiche images)
- Computer databases, output and discs
- Material intended for short term or transitory use, including notes and 'spare copies' of documents.

9. This list is not exhaustive and may not cover all records staff will come across in the course of their work. Further advice on the inclusion of other forms of records not covered above may be obtained from the Trust Records Manager.

RESPONSIBILITIES

Trust Board

10. The Trust Board is ultimately responsible for ensuring that the Trust corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements. Included within its responsibilities to maintain minimum standards of information governance is a responsibility for ensuring the quality of record keeping and record management in the Trust.

11. The Trust Board will be updated on records issues via reports from the Information Strategy Steering Group who have delegated responsibility for monitoring the standards of Information Governance within the Trust.

Chief Executive

12. The chief executive has overall responsibility for records management in the Trust. As accountable officer he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this, as it will ensure appropriate, accurate information is available as required.

13. The Chief Executive has delegated operational responsibility for Information Governance including records management to the Director of Organisational Development.
Director of Organisational Development

14. The Director of Organisational Development is the appointed Executive Director with responsibility for Information Governance including records management and is the Trust Senior Information Risk Owner (SIRO).

15. The SIRO is responsible for managing information risk in the Trust and will implement and lead the NHS Information Governance risk assessment and management processes within the Trust and advise the Board on the effectiveness of information risk management.

16. The Director of Organisational Development is the Chair of the Information Strategy Steering Group (ISSG) which is a sub committee of the Trust Executive Committee (TEC) with delegated responsibility to oversee and monitor the Trust’s strategy and performance with regard to Information Governance including record keeping.

Caldicott Guardian

17. The Trust’s Caldicott Guardian is the Director of Nursing who has a particular responsibility for reflecting patients’ interests regarding the use of patient identifiable information. The Trust Caldicott Guardian is responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

18. The duties and responsibilities of the Trust Caldicott Guardian are outlined in the Trust Confidentiality and Data protection Policy.

Trust Records Manager

19. The Trust’s Records Manager is responsible for ensuring that this policy is implemented, that the records management system and associated processes are developed, co-ordinated and monitored.

20. The Trust’s Records manager is also responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good records keeping and management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

Local Managers

21. The responsibility for local records management is devolved to divisional, care group and department heads who retain overall responsibility for the management of records generated by their activities, i.e. for ensuring that records created within their unit are managed in a way which meets the aims of the Trust’s records management policies.

Clinical Leads and Matrons

22. Clinical leads in all professions have a responsibility to ensure clinical staff within their responsibility who contribute to patient health records are adequately trained in record keeping and are aware of and adhere to the standards for record keeping outlined in this policy.
All Staff

23. Members of Staff who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

24. Staff who make entries in medical records should do so in accordance with the clinical record keeping standards published in this policy. In addition Royal Colleges and other professional bodies publish record keeping guidance for clinical staff and it is the responsibility of clinical staff to ensure they keep up to date with and adhere to relevant legislation, case law and national guidance.

RECORDS TRAINING

25. Records management is one of the topics covered in basic information governance training included within the Trust Training Needs Analysis for mandatory and statutory training. All staff are required to complete basic information governance training on joining the Trust and an update session every two years thereafter.

26. All clinical staff who contribute to patient health records are required to complete a basic record keeping training module via the NHS Information Governance Training Tool. This requirement is also included in the Trust scheme of mandatory and statutory training.

27. During local induction all staff who create and handle records should be made aware of the local arrangements for creating storing and filing records and be made aware of the guidance on record keeping contained in this policy.

28. Before staff are provided with access to any electronic health records systems (e.g. PAS, E-Quest etc) they are required to undertake the relevant training which includes appropriate aspects of record keeping and management.

29. Additional training and awareness sessions on records management and record keeping can be provided to departments and groups of staff on request. Please contact the Trust Records manager for further details.

LEGAL OBLIGATIONS APPLYING TO RECORDS

30. Under the terms of the Public Record Act 1958 all records created in the Trust are regarded as public records. The act imposes a statutory duty on the Trust to make arrangements for the safe keeping and eventual disposal of records. The ownership and copyright of records created within Trust lies with the Trust and not the individual who has created them.

31. The Trust will take actions to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice and in particular:

- The Public Records Act 1958
- The Data Protection Act 1998
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice

32. There are a number of other legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information or permit or require information to be used or disclosed. A summary of the most important legal and professional obligations and NHS guidance documents are provided at Appendix 2 for information.

LINKS TO OTHER TRUST POLICIES

33. This policy is one of a number of Trust policies that relate to the management of Information and together provide the Trust’s Information Governance Assurance Framework. Users of Trust records need to be aware of the requirements set out in the following Trust policies which may impact on their use of Trust Records.

- Information Governance Policy
- Data Protection and Confidentiality Policy
- Freedom of Information Policy
- Subject Access Policy
- IM&T Security Policy
- Risk Management Policy and Procedure
- Incident Reporting and Management Policy
- Patient Concerns and Complaints Policy and Procedures
- Being Open Policy
- PAS Patient Master Index Policy

PROCESS FOR RECORD CREATION AND REGISTRATION

Corporate Records

34. In order that we can subsequently identify, locate and manage the records we create it is normal practice to include them in a registered file system. In simple terms this means allocating each new record a unique identifier and recording that identifier in some form of register or index. These registers act as a ‘finding aid’ when subsequently information on a particular aspect of Trust business is sought.

35. Not all records need to be included in a registered file system. A decision needs to be reached based on the organisation’s information needs and requirement to maintain accountable records. While policy papers, minutes of meetings and clinical records are examples of records that should be included in registered file systems more transient records such as notes of a telephone conversation do not necessarily require registration.

36. A more detailed guide for users covering the creation and filing of corporate records is attached at Appendix 3.
Patient Records

37. A patient’s clinical record in the Trust is likely to comprise of one or more health record folders containing paper based records and other documents and images stored electronically in a number of separate clinical record systems. The key to the safe management of this situation is the consistent use of a common patient identifier in all systems.

38. Currently a unique record number (URN) is allocated to each patient added to the PAS Patient Master Index (PMI) and this is used to register and identify their main PAS record and any casenotes. (This is also known as the ‘hospital number’). By means of electronic interfaces this number is used when a patient record is created in any subsidiary Trust clinical record system such as E-Quest, E-Docs HICSS and PACS.

39. It is intended that, at a future date, a patient’s NHS number will replace the hospital number as the common record identifier. This is not possible for all patients at the moment but the NHS number should be used/shown alongside the hospital number until future system changes allow it to be the sole identifier used.

40. In most cases a patient’s clinical record will initially be created in PAS and registration details transferred to other clinical systems automatically. Once registered in PAS users can create a health record folder for the patient. Detailed guidance for staff on on registering patients and creating patient record folders is provided as part of PAS user training.

41. Before creating new clinical records it is important to ensure correct and thorough search procedures are carried out to identify if any existing records exist for the patient and avoid duplication. (See PAS Patient Master Index Policy)

RECORD STORAGE

42. When not required for operational purposes records should be kept in a secure storage area. Records in current use should ideally be stored close to the point of use while records no longer in current use can be transferred to secondary or archive storage more remote from the operational area.

43. Records should be stored in an appropriate environment to ensure they remain fit for purpose during their expected period of retention. When evaluating the suitability of a location for record storage the following points should be considered:

- Environment. Is the location suitable for the type of material being stored? Is the area free from hazards that may cause the records to deteriorate or place at risk staff that may need to access the records? i.e. excessive dust, damp, restricted access.
- Security. Is the level of security offered by the location acceptable for the type of record being stored?
- Ease of Access. Can records be easily located and retrieved? Some restrictions on access may be acceptable for records that are not frequently recalled.
• Layout. Consideration should be given to the design of the storage location to ensure the most cost effective use is made of the space available.

44. External storage companies provide an alternative to local storage and in the short term can prove a cost effective alternative in areas where record storage space is at a premium. The Trust has negotiated a contract for external record storage with a local contractor who should be used for all external storage requirements. Advice on external storage and alternative strategies such as archiving records to digital formats can be obtained from the Trust records manager.

45. A comprehensive record should be maintained of any records sent for commercial storage including a proposed date for review/destruction. A mechanism for reviewing these records for disposal should be developed and implemented to ensure records are not retained longer than necessary.

RECORD MAINTENANCE

Process for Patient Record Tracking

46. Ideally the movement and location of all records should be controlled to ensure that a record can be retrieved at any time and there is an auditable trail of record transactions. This is best achieved using some form of record tracking system to record the movement of records between locations.

47. It is the policy of the Trust that patient health record folders are tracked using the PAS record tracking component (electronic casenote record tracking e-CRT.) Users are provided with training to use e-CRT prior to being granted access to the system.

48. While electronic records do not require tracking as such, control must be exercised when hard copies are produced. If separate clinical casenotes are produced from electronic systems to form a filing system individual record movements should be tracked to aid retrieval and avoid loss of data.

49. For most areas, where movement of records is restricted, paper based systems may be employed, using registers or tracer cards to record the relevant information.

50. When making arrangements to move records which contain personal or sensitive information to destinations external to the Trust consideration needs to be given to security and confidentiality and a means of dispatch chosen that affords an adequate level of security. (See Trust Data Protection Policy.)

Process for Patient Record Retrieval

51. The Trust stores patient health record folders not in circulation at the Trust Health Records Centre (HRC). The centre is staffed 24 hours per day throughout the year to provide an emergency record retrieval service.
52. The majority of patient records required for clinic attendance and following an emergency admission will be automatically identified and retrieved by health records staff and sent to users.

53. Users who require records for other purposes should request them as follows:

- Using the PAS e-CRT request functional component. This can be used to request a single record or multiple records. The details of each record requested will be added to a request list which is used by HRC staff to manage the demand for records and identify records to be retrieved and dispatched to users in priority order.

- By faxing requests for multiple sets of records to the HRC.

54. Occasionally the urgency and of complexity of a request may justify a telephone request direct to the HRC.

55. The HRC will deal with record requests on a priority basis. In the event that a record tracked to the library cannot be found HRC staff will follow local search procedure to try and identify the records location. In the event that the record cannot be found it will be marked as missing on the eCamis system and a temporary replacement folder will be raised to replace it.

56. When a ‘missing’ record is located the HRC should be notified to remove the missing status from the record. If a temporary replacement folder has been created the contents should be moved into the main folder and the two casenote records merged on e-Camis.

57. If after an extensive investigation and full search process a patient record folder cannot be located it will be formally declared lost and a replacement volume created. The subject patient should be informed of the loss of their data.

**RECORD RETENTION**

58. The destruction of records is an irreversible act while the cost of preserving records is high and continuing. Achieving a balance between the natural desire to retain records ‘just in case’ and the need to keep storage costs to an affordable level is a continuing challenge.

59. The maximum period that public records (including NHS records) can normally be retained is 30 years. There is legal provision for some public records to be retained for longer periods but in most cases permission from the national archives is required to hold public records in excess of 30 years.

60. Part 2 of the NHS publication ‘Records Management: NHS Code of Practice.’ contains a comprehensive list of NHS clinical and corporate records and for each type or record sets out a recommended minimum period of retention along with advice on final disposal. The Trust policy on record retention is to follow the guidance on minimum retention periods provided in the Code of Practice.

61. An extract from part 2 of the code of practice is attached at Appendix 4. It lists the recommended retention period for some of the more common administrative records users will need to manage in the Trust. A full list of the document...
PROCESS FOR THE RETENTION, DISPOSAL AND DESTRUCTION OF CORPORATE RECORDS

62. Trust corporate records that are no longer required for business use should be reviewed at the earliest opportunity. Guidance on the process to be followed is provided at Appendix 5. The review will identify whether the records are worthy of permanent preservation, require a longer retention period and, if disposal is decided as appropriate, the method of that disposal.

63. Records should be kept of all decisions reached in relation to record disposal so the Trust is aware of those records that have been disposed of and are no longer available.

64. Records that are selected for destruction may contain sensitive information and the method of destruction selected must ensure adequate safeguards against the accidental loss or disclosure of the record contents. Some record media such as computer hard drives or discs require special handling to ensure safe and secure disposal and appropriate advice should be sought before making arrangements for their destruction.

65. The Trust has a confidential waste collection and disposal service in place managed by the Trust Waste Management Team. In most cases this service can be used for the secure disposal of small quantities of paper based records. Where large quantities of records are identified for disposal collection arrangements should be agreed with the waste management team in advance.

66. If a record due for destruction is subject to an information request or potential legal action destruction should be delayed until disclosure has taken place, or if not disclosed, any period allowed for appeal against that decision has passed.

PROCESS FOR THE RETENTION, DISPOSAL AND DESTRUCTION OF PATIENT RECORDS

67. The overall responsibility for managing the process for the retention, disposal and destruction of patient health records lies with the Trust Records Manager. Where possible those elements of a patient record that are held digitally will be retained for the maximum 30 years allowed by the Public Record Act. Due to the high cost of storing paper based patient records a programme of disposal, based on the guidance provided in the Records Management NHS Code of Practice is followed for records held in this medium.

68. All patient records will be retained for the minimum periods described in the guidance within the code of practice. Where possible the retention period for those elements of a patient’s record held on digital systems will be extended to 30 years. Where changes in technology or other pressures do not allow this extension earlier disposal may be considered. Such cases should be discussed.
with the Trust Records Manager so a method of review and an appropriate method of disposal can be agreed.

69. When digital patient records reach the end of the agreed retention period they should be reviewed and an appropriate method of disposal agreed. Although in most cases a decision will be reached to securely destroy the records, consideration should be given to the archival value of the record set and the potential to transfer them to a place of deposit for permanent preservation.

70. The process for the retention, disposal and destruction of patient health record folders will be carried out by Health Record Centre staff. Eight years following a patient’s death or last contact their record folder(s) will be selected for review. The folder will be reviewed to confirm its status and it will be classified as one of the following:

- Containing information subject to a longer minimum retention period. (Retain in storage).
- Possible archival value. (Discuss transfer with place of deposit).
- Passed minimum retention period. (Can be destroyed).

71. Where a longer retention period is identified for a record the outside cover of the folder will be marked to indicate the remaining period of retention applicable and whether further review at the end of that period is also necessary. These records will be returned to local or off site store as deemed appropriate.

72. Where a patient record or record set is identified as having potential archival value the Trust Records Manager will discuss with the most appropriate place of deposit the potential to transfer the record for permanent preservation. The age, contents and format of the vast majority of Trust patient record folders is such that they are unlikely to fall into this category.

73. Where it is identified that a patient record folder can be selected for destruction the record will be securely destroyed using the Trust confidential waste disposal service. The decision to destroy the record will be recorded using the Trust medical record tracking system by recording a movement to location ‘DES’ (Record Destroyed).

**RECORD CONFIDENTIALITY AND ACCESS**

74. All NHS records are public records and thus are subject to a number of statutory provisions regarding confidentiality, access and disclosure. (See Appendix 1) Patients entrust the NHS or allow it to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

75. Specific guidance on patient confidentiality issues is given in the Department of Health publication ‘Confidentiality: NHS Code of Practice’. In addition the Data Protection Act 1998 sets out a series of principles for data protection and the fair and lawful processing of data. Advice on all aspects of patient confidentiality
and the application of the Data Protection Act (1998) on the way we handle records in the Trust can be obtained from the Trust Data Protection Office.

76. The Data Protection Act (1998) also makes provision in law for patients to obtain copies of otherwise gain access to their health records. The Trust Subject Access policy covers this aspect of records management and advice on the procedure can be obtained from the Trust Records Manager. It is important that patient health records

77. In 2000 the government introduced the Freedom of information Act providing members of the public with the general right of access to recorded information held by a wide range of bodies across the public sector. The effect of this legislation is to make it possible for people to obtain copies of a wide range of Trust records that in the past would have remained confidential. Staff need to be aware that the records they keep may well be released to the public at a future date and the increased importance of adhering to the guidance provided in the Trust Freedom of Information Policy.

NON-PAPER RECORDS

78. Increasingly our records are being created and recorded using computers that hold the data in a digital format. In addition to records held in this format we record and transfer information onto a variety of CDs, films, tapes and slides. There are many benefits associated with this improvement in technology but it is very easy to replace an existing paper mountain with a less visible virtual equivalent.

79. The principles of sound record management apply equally to electronic and other non-paper records as they do to traditional paper records. The need to organise electronic records in registered filing systems and maintain, review and dispose of these records in line with the guidance in this document still applies. When considering the use of alternative storage media, maintenance in the form of back up and planned migration to new platforms should be considered, and subsequently designed and scheduled to ensure continuing access to readable information.

80. In many cases copies of documents are distributed electronically and the original held in paper form. This often leads to duplicate records being unnecessarily retained, sometime for periods beyond the recommended minimum retention period. This is particularly prevalent on file servers shared by several people/departments. Responsibility for the maintenance of such filing systems should be clearly defined and if appropriate restrictions placed on the ability to create new record folders.

81. E-mail has become a primary communication tool increasingly replacing letters and memorandums as a means of communicating and distributing information. The Trust has a separate policy on e-mail security and use which users should be familiar with. E-mail accounts tend to be structured according to personal preference and the data stored is not searchable and organised in a systematic way making e-mail accounts unsuitable for record storage purposes.

82. E-mail accounts should not be used to file records on a permanent basis but should be regarded as transient storage areas for working documents.
Important e-mails or documents distributed by e-mail that need to be retained should be copied to the appropriate paper or electronic registered file system and the e-mail copy destroyed as soon as practicable.

83. The increasing use of e-mail for personal communication can lead to business e-mails containing opinion and comment that may be inappropriate and would not have been included in more formal documents. Users should be aware that, if relevant, copies of e-mails held in the Trust will be released to requesters under the provisions of the Freedom of Information Act.

84. In cases where paper records have to be retained for long periods the option to transfer the information to a digital media such as CD ROM, Optical Disk or Hard Drive storage is often chosen. While this is sensible and cost effective, in practice care must be taken with documents stored electronically that may be required in the future for purposes of litigation. (i.e. medical records) The process of transfer and storage should conform to the Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. (BSI DISC PD 0008) This will reduce any risk inherent in destroying the original documents following transfer.

RECORD KEEPING

85. Records of business activity should be complete enough to:

• Facilitate an audit or examination of the business by anyone so authorised
• Protect the legal and other rights of the organisation, its clients and any other person affected by its actions
• Provide authenticity of the records so that evidence derived from them is shown to be credible and authoritative

86. When completing entries in or creating any form of records the following general guidance should be applied:

• Be factual consistent and accurate
• Write clearly and in such a way that text cannot be erased
• Write in such a way that any alterations or additions are dated, timed and signed in such a way that the original entry can still be read.

87. Clinical records have to fulfil additional functions in relation to patient care that do not apply to general business records and clinical staff have professional responsibilities in relation to record keeping. More stringent standards of record keeping need to be applied to clinical records and specific guidance in the form of a set of clinician’s record keeping standards is set out in Appendix 6

MONITORING OF COMPLIANCE WITH THIS POLICY

88. Any identified areas of non adherence or gaps in assurance arising from the monitoring of this policy will result in recommendations and proposals for change to address areas of non compliance and/or embed learning. Monitoring of these plans will be co-ordinated by the group/committee identified in the monitoring table.
## Process for Monitoring Compliance and Effectiveness with this policy

<table>
<thead>
<tr>
<th>Element of Policy to be monitored</th>
<th>Lead</th>
<th>Tool/Method (eg audit, review of minutes, records, training etc)</th>
<th>Frequency</th>
<th>Who will undertake</th>
<th>Where results will be reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Requirements</td>
<td>Trust Records Manager</td>
<td>Breach of legal requirements identified by information governance incident reporting process.</td>
<td>Ongoing</td>
<td>Trust records manager, patient safety team and local governance teams</td>
<td>Serious incidents reported to Strategic Health Authority. Summary report included in annual statement of Internal Control (SIC)</td>
</tr>
<tr>
<td>Legal Requirements</td>
<td>Trust Records Manager</td>
<td>Review of reported IG breaches and incidents involving records will identify trends and problem areas.</td>
<td>6 monthly</td>
<td>Trust Record Manager</td>
<td>Bi annual report to Information Governance Steering Group.</td>
</tr>
<tr>
<td>Process for Tracking Health Records</td>
<td>Trust Records Manager</td>
<td>Audit of electronic tracking recorded for 100 records of inpatients selected at random from all Trust areas and sites as part of record management audit.</td>
<td>Annual in Q4</td>
<td>Health Records Staff</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Process for Creating Health Records</td>
<td>Trust Records Operational Manager</td>
<td>Audit of 25 recently created records selected at random.</td>
<td>Quarterly</td>
<td>Health Records Staff</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Process for Retrieving Health Records</td>
<td>Health Records Operational Manager</td>
<td>Audit of response to 25 recent requests for records selected at random from all Trust areas and sites.</td>
<td>Quarterly</td>
<td>Health Records Staff</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Process for Retention Disposal and Destruction of Health Records</td>
<td>Trust Records Manager</td>
<td>Audit of process followed for 50 patient record folders selected for review from all Trust areas and sites in previous 3 months.</td>
<td>Annual Q2</td>
<td>Trust Records Staff</td>
<td>Information Governance Steering Group</td>
</tr>
<tr>
<td>Standards which must be used by all healthcare professionals for the completion of all health records.</td>
<td>Trust Clinical Records Lead</td>
<td>Audit of 100 randomly selected records of patients admitted for treatment in previous 3 months across all Trust service areas and sites.</td>
<td>Annual</td>
<td>Audit arranged by Trust Clinical effectiveness Team. See appendix 7 for more detail.</td>
<td>Clinical Effectiveness and Outcomes Steeering Group - CEOSG</td>
</tr>
</tbody>
</table>
ARRANGEMENTS FOR REVIEW OF THE POLICY

89. This policy will be reviewed every two years.

References:

See also list included at Appendix 2
Equality Impact Assessment Tool - To be completed for all new/revised policy, procedural and guideline documents.

Equality Impact Assessments (EQIAs) are a way of examining new policy documents to see whether they have the potential to affect any one group of people more or less favourably than another. Their purpose is to address actual or potential inequalities resulting from policy development. The duty to undertake EQIAs is a requirement of race, gender and disability legislation.

The word ‘policy’ is taken to mean all procedural documents i.e.: Policy, Procedure, and Guideline. (this does not include Patient Information)

---

**Document Title** | Records Management Policy | **Version** | 5.0
---|---|---|
**Is this a new or revised document?** | Revised | **Area to which document relates** | Trust Wide

**Specify whether Trust wide or, Care Group. Name Care Group**

**Name of person completing Assessment** | Paul McMahon

---

**STAGE 1 – INITIAL SCREENING**

This stage establishes if the proposed change will have an impact from an equality perspective on any particular group(s) of people. See guidance notes on completion.

<table>
<thead>
<tr>
<th>Does the document affect one group more or less favourably than another on the basis of any of the strands of diversity?</th>
<th>Positive Impact Y/N/Neutral</th>
<th>Negative Impact Y/N/Neutral</th>
<th><strong>Comments</strong> - Give details of concerns and evidence in the boxes below</th>
<th><strong>Impact Level</strong> N/L/M/H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Disability</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Gender</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Sexual Orientation</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Race &amp; Ethnicity</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Religion or Belief</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Culture</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
<tr>
<td>Other e.g. Mental Health, Geographic factors, Economic factors...</td>
<td>Neutral</td>
<td>Neutral</td>
<td></td>
<td>N</td>
</tr>
</tbody>
</table>

**Level of impact:**
Taking into account the impact level for each group, circle one of the words in the boxes below to identify the overall impact level:

| NONE | LOW | MEDIUM | HIGH |

**Significance**
Is the positive / adverse impact significant enough to warrant a more detailed assessment (Stage 2) *A full assessment will usually be required if the level of impact is above ‘LOW’ as identified above.*

**YES**/ **NO** (delete as applicable)

If no give brief details of any action taken/information gathered to justify this decision:

This policy describes the Trust approach and policy for Records Management and no significant impact on equality target groups was identified during review.

Or give brief details of how the change will be monitored to assess the impact over a specified period of time:

---

**IF NO POTENTIAL DISCRIMINATION HAS BEEN IDENTIFIED or THE IMPACT IS NOT SIGNIFICANT ENOUGH TO WARRANT A FULL IMPACT ASSESSMENT, PLEASE SIGN AND DATE BELOW.**

*(NOTE: A full impact assessment should be undertaken if initial screening demonstrates that there could be significant detrimental impact.)*

I have assessed this document and found:

- no potential impact on any group
- the impact is not significant enough to warrant a full impact assessment

(delete as applicable)

**SIGNATURE:**

**DATE:**  14th May 2010

**PRINT NAME:**  Paul McMahon  
**POST HELD:**  Trust Records Manager

THE COMPLETED EQIA MUST BE RETURNED TO THE TRUST POLICY ADMINISTRATOR ALONG WITH THE FINAL VALIDATED DOCUMENT

IF YOU HAVE IDENTIFIED ANY POTENTIAL IMPACT THAT REQUIRES FURTHER ASSESSMENT PLEASE CONTINUE TO COMPLETE STAGE 2 OF THE ASSESSMENT

Issued:Disclaimer: It is your responsibility to check against Staffnet that this printout is the most recent issue of this document.
Appendix 2 to SUHT Records Management Policy

List of Primary Legal and Professional Obligations Impacting on Records Management.

There are a range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. This appendix provides a summary of the key obligations. A more comprehensive guide is provided in the Department of Health publication ‘Records Management: NHS Code of Practice’ (Gateway Reference 6295)

The Access to Health Records Act 1990

This Act has been repealed to the extent that it now only affects the health records of deceased patients. It applies only to records created since 1 November 1991.

The Act allows access to:

a) The deceased’s personal representatives (both executors or administrators) to enable them to carry out their duties; and
b) Anyone who has a claim resulting from the death.

The Access to Medical Reports Act 1988

The aim of the Act is to allow individuals to see medical reports written about them, for employment or insurance purposes, by a doctor who they usually see in a ‘normal’ doctor/patient capacity.

The Civil Evidence Act 1995

This Act provides the legal basis for the use of documents and records of any format to be admissible as evidence in civil proceedings. This includes electronic patient records.

The Common Law Duty of Confidentiality

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider’s consent.

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

Confidentiality: NHS Code of Practice

The Confidentiality Code of Practice is a result of a major public consultation that included patients, carers and citizens, the NHS, other healthcare providers, professional bodies and regulators.

The Code offers detailed guidance on:
• Protecting confidential information;
• Informing patients about uses of their personal information;
• Offering patients appropriate choices about the uses of their personal information
• The circumstances in which confidential information may be used or disclosed.

The Code can be accessed from the Department of Health website at:

http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

The Computer Misuse Act 1990

The Act is relevant to electronic records in that it creates three offences of unlawfully gaining access to computer programmes. The offences are:

• Unauthorised access to computer material;
• Unauthorised access with intent to commit or cause commission of further offences
• Unauthorised modification of computer material.

The Data Protection Act (DPA) 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Act regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to health records; therefore the same principles apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

**Personal data** is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller’s possession. It therefore includes such items of information as an individual’s name, address, age, race, religion, gender, and physical, mental or sexual health.

**Processing** includes everything done with that information, i.e. holding, obtaining, recording, using, disclosure and sharing it. Using includes disposal, i.e. closure of the record, transfer to an archive or destruction of the record.

**Rights of the individual**

The Data Protection Act gives an individual several rights in relation to the information held about them.

Of particular relevance in a health and social care setting, is the right of individuals to seek access to their records held by the health or social care provider.

Access covers the right to obtain a copy of the record in permanent form, unless the supply of a copy would involve disproportionate effort or the individual agrees that his/her access rights can be met some other way, for example by viewing the record.
The Data Protection (Processing of Sensitive Personal Data) Order 2000


This Order amends the DPA 1998 and provides that sensitive personal data (for example information relating to physical or mental health) may be lawfully processed without explicit consent where there is a substantial public interest in disclosing the data for certain identified purposes.

The Environmental Information Regulations 2004


The Environmental Information Regulations 2004 came into force at the same time as the Freedom of Information Act 2000 and update and extend previous rights to environmental information.

The Freedom of Information Act (FOIA) 2000

http://www.justice.gov.uk/whatwedo/freedomofinformation.htm

www.ico.gov.uk

The FOIA lays down requirements for public bodies (including the NHS) to keep and make information available on request. The new rights of access in the FOIA signal a new recognition of, and commitment to, the public interest in openness about government. They are additional to other access rights, such as access to personal information under the Data Protection Act 1998, and access to environmental information under the EIR 2004.

The main features of the Act are:

- A general right of access to recorded information held by public authorities, regardless of the age of the record/document; and
- A duty on every public authority to adopt and maintain a scheme, which relates to the publication of information by the authority and is approved by the Information Commissioner.

The Limitation Act 1980

The Act sets out the law on the time limits within which actions for personal injuries, or arising from death, may be brought. The limitation period for bringing such actions is three years. This period runs from when it is first realised that a person has suffered a significant injury that may be attributable to the negligence of a third party or from 10 years after the application of a product that is found to be defective (see Consumer Protection Act).
The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000

Every NHS Trust and Primary Care Trust must take all necessary steps to ensure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except:

- For the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and
- For the purpose of such treatment or prevention.

The Public Interest Disclosure Act 1998

The Act allows a worker to breach his duty as regards confidentiality towards his employer for the purpose of ‘whistle-blowing’. A disclosure qualifying for protection under the Act is known as a ‘qualifying disclosure’.

The Public Records Act 1958

All NHS records, and those of NHS predecessor bodies, are public records under the terms of the Public Records Act 1958. The Act sets out broad responsibilities for everyone who works with such records, and provides for guidance and supervision by the Keeper of Public Records. It requires that those records that have been selected for archival preservation are transferred to The National Archives or a Place of Deposit appointed under the Act.

The maximum period for which records can be kept prior to transfer is usually 30 years (any NHS body that feels it needs to hold records for a longer period must consult with The National Archives). In practice, NHS records that have been selected for archival preservation are transferred to a Place of Deposit, which is usually the record office of the relevant (i.e. county, borough or unitary) local authority.

The Re-use of Public Sector Information Regulations 2005

The Regulations link with the Freedom of Information Act 2000, in that freedom of information is about access to information and these Regulations are about how the information can be re-used. However, there is no automatic right to re-use merely because an access request has been granted. Information that is exempt under the Freedom of Information Act or other legislation is also exempt under the Regulations.

The NHS Information Governance Toolkit

https://www.igt.connectingforhealth.nhs.uk/whatsnew.aspx?tk=669914318&cb=13%3a40%3a34&lnv=2&cnv=YES

The Information Governance Toolkit return is required from all NHS organisations and provides guidance and best practice on all facets of information governance.
Professional Codes of Conduct

All the NHS professions have their own codes of conduct setting out the standards of ethical behaviour owed by members of each profession. These standards typically include:

- Respecting patients’ decisions about their care and treatment;
- Obtaining consent for treatment or for disclosure of patient personal information;
- Protecting patient personal information by maintaining confidentiality; and
- Ensuring continuity of care through good record-keeping practice.

Information on professional codes of practice can be obtained from the following organisations.

The General Medical Council

http://www.gmc-uk.org/

The Royal college of Physicians

The RCP are in the process of developing a set of standards for shared record keeping which can be viewed at the following link:

http://www.rcplondon.ac.uk/CLINICAL-STANDARDS/HIU/Pages/Health-Informatics-Unit.aspx

The Nursing and Midwifery Council Code of Professional Conduct

The NMC Standards 07.04 informs the professions of the standard of professional conduct required of them in the exercise of their professional accountability and practice.

See link:
http://www.nmc-uk.org/

The Chartered Society of Physiotherapy: Rules of Professional Conduct

http://www.csp.org.uk/director/effectivepractice/rulesofconduct/professionalconduct.cfm

Information on record keeping can also be obtained from the following:

Midwives’ Rules and Standards – NMC Standards 05.04

The Nursing and Midwifery Order 2001 requires the NMC to set rules and standards for midwifery. The rules and standards document provides guidance on the interpretation of these rules and standards and includes record keeping. See: http://www.nmc-uk.org/(k452wr55m2qj1p2ppgy3xf45)/aDisplayDocument.aspx?DocumentID=169
Appendix 3 to Records Management Policy

User Guide to Corporate Record Creation

Introduction

1. Although most corporate records in the Trust are created and stored electronically some paper based record keeping systems are still in use. Most of the guidance provided in this document can be applied to both forms of records but where this is not the case users will need to exercise judgment when applying the guidance.

2. Common types of documents such as letters, meeting minutes, Job Descriptions etc should be always be created using the Trust Word Templates set up for these document types. When creating documents staff should take note of the guidance contained in the ‘Trust Style Guide’ published on the Trust internet.

3. All records created in the Trust should be included in a record keeping filing system and be given a unique title or name to identify it. When creating records users need to consider the need for privacy markings and version control. The guidance set out in the following sections addresses these requirements and provides guidance in their application.

Record Filing Systems

4. Records created in both electronic or paper form should be organised in some form of registered filing system so they can be easily located when needed and documents of a similar or linked nature are kept together. Filing systems can be created and organised using a variety of methods. Probably the most common method is a simple alphanumeric system whereby records are grouped together in folders that are given unique names. The folders are then organised/ordered in alphanumeric fashion in draws/cabinets (paper records) or within Trust HQ/Divisional/Care Group hard Drives (electronic records).

5. When designing and developing filing systems the following points should be considered:

   a. Retain control and continuity by restricting the number of staff who can create new folders in the system.

   b. Organise folders and sub folders in a logical manner that will make sense to those who need to access records within them. E.g. organised by function or teams.

   c. Give each folder a clear title that describes the contents within. e.g. ‘MeetingsDiv Board2009’, ‘ComplaintsPatients200804to200906’. Avoid names like ‘General’, ‘Miscellaneous’ or personal titles like ‘Kev’s Folder’. (See next section for more details on file names)

   d. Within folders records are normally filed in chronological order by date of creation or receipt. It is good practice to clearly stamp on the front or all documents received the date of receipt.

   e. Folders in hard copy filing systems should be marked with the date the folder was opened and when closed the date of closure. When files are closed the date when the folder should be reviewed prior to disposal (usually at the end of the minimum retention period) should be added. In electronic filing systems these pieces of information can often be added to the metadata for the folders created.

   f. A regular programme of reviews should be established to consider the need for
Folder and File Naming/Referencing Conventions

4. Names for folders and documents should be kept as short as possible whilst also being meaningful. Long file names create long file paths and URLs which increase the likelihood of error and are more difficult to remember. Avoid using personal names and codes and abbreviations that are not commonly understood.

   e.g. use ‘H&SCtteTOR.doc’ in preference to ‘Health___Safety_Comitee_Terms_of_Reference.doc’

5. When creating sub folders and files within electronic filing systems there is no need to include in the file name descriptive information already contained in the parent folder as this will already form part of the filename/file path.

   e.g. use: ‘/.../DivBoard/agenda20100210’
       not: ‘/.../DivBoard/DivBoardagenda20100210’

6. Avoid using spaces and underscores in file names. Some software packages have difficulty recognising file names with spaces. Use capital letters to delimit words.

   e.g. use ‘AuditMeetingsAgendas.doc’ in preference to ‘Audit_Meetings_Agendas.doc’

7. When using a number in a file name always give it as a two digit number so that when it is displayed in the file directory in alphanumeric order it will be ranked in the correct order. Organised alphanumerically ‘ab2’ will be listed after ‘ab10’.

   e.g. V01, V02, V03 etc not V1, V2, V3.

8. If using a date in the file name always state the date ‘back to front’ and use four digit years, two digit months and two digit days: YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY. Writing dates in this way will present the records in chronological order in the file list with the latest record at the end of the list.

   e.g. use ‘20100201agenda.doc’ not ‘1Feb2010Agenda.doc’

9. The elements of the file name should be ordered in the most appropriate way to retrieve the record. If records are retrieved by date the date element should appear first, if retrieved according to description then this should appear first.

   e.g. ‘20100201agenda.doc’ (date retrieval) or ‘agenda20100201’ (subject retrieval).

Protective Marking of Documents

10. The NHS has agreed a scheme of classification using two privacy markings;

   a. NHS CONFIDENTIAL. This classification should be used for paper and electronic documents.
electronic documents containing personal identifiable clinical or NHS staff information and other sensitive information the compromise of which could lead to serious consequences for the Trust. The marking should be included at the top centre of every page of the document and documents so marked should be held and transported securely at all times. (The term **NHS CONFIDENTIAL** should never be used on correspondence to a patient.)

b. **NHS RESTRICTED.** This classification should be used to mark all other sensitive information. Documents marked **NHS RESTRICTED** may also be endorsed with a suitable descriptor indicating the reason for the classification. A list of these descriptors is shown in the table below. The marking should be included at the top centre of every page of the document and documents so marked should be kept in lockable containers.

11. When classifying documents regard should be paid to the requirements of the Freedom of Information Act 2000. Careful consideration should be given to classifying documents that would be normally be published or disclosed on request. Protective markings should wherever possible only be applied to documents that would be exempt from disclosure.

<table>
<thead>
<tr>
<th>Table 1 Categories of <strong>NHS RESTRICTED</strong> Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>Appointments</td>
</tr>
<tr>
<td>Barred</td>
</tr>
<tr>
<td>Board</td>
</tr>
<tr>
<td>Commercial</td>
</tr>
<tr>
<td>Contracts</td>
</tr>
<tr>
<td>For Publication</td>
</tr>
<tr>
<td>Management</td>
</tr>
<tr>
<td>Personal</td>
</tr>
<tr>
<td>Policy</td>
</tr>
<tr>
<td>Proceedings</td>
</tr>
</tbody>
</table>

**Version Control**

12. Document version control allows the management of multiple revisions to the same document and is important as it enables users to distinguish between different versions of a document and to identify if the document they are using is the latest version. When several people are collaborating on a document version control will help identify when any changes have been made by any of the collaborators.

13. When creating a document where more than one version does or is likely to exist a unique version number should be included in the document name and clearly
14. Consecutive whole numbers should be used to identify major revisions to documents. i.e. version 1, version 2 etc. The addition of the word Draft or Final at the end of the file name can be used to indicate the status of the document.

e.g. ‘/.../AnyRecordV1Draft.doc’ First draft version
     ‘/.../AnyRecordV2Draft.doc’ Second draft version
     ‘/.../AnyRecordV3Final.doc’ 3rd and final version

15. Where documents may be subject to many changes smaller revisions can be indicated by using version numbers with decimal points to indicate major and minor changes.

e.g. ‘/.../AnyrecordV1.1doc’  First Version
     ‘/.../AnyrecordV2.1doc’  Second version with major change
     ‘/.../AnyrecordV2.2doc’  Second Version with minor change

16. In key documents (policies, strategies etc) it is useful to display at the front of the document after the title page a version control table showing the development history of the document and the version changes that have been applied. An example is shown below. It is also useful to display the document version number in the footer section of every page so readers can be clear they are viewing the latest version.

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Description</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Jan 2009</td>
<td>PW</td>
<td>Initial Draft circulated for comment.</td>
<td>0.1</td>
</tr>
<tr>
<td>10 Jan 2009</td>
<td>PW</td>
<td>Revised draft version incorporating comments from review group</td>
<td>0.2</td>
</tr>
<tr>
<td>31 Jan 2009</td>
<td>PW</td>
<td>Final Draft for approval ISSG</td>
<td>1.0</td>
</tr>
<tr>
<td>09 Sep 2009</td>
<td>AJ</td>
<td>Major update following publication of new Trust Strategy</td>
<td>2.0</td>
</tr>
<tr>
<td>12 Feb 2010</td>
<td>AJ</td>
<td>Minor changes incorporating new Trust structure and organisation</td>
<td>2.1</td>
</tr>
</tbody>
</table>
Appendix 4 to Records Management Policy

NHS RECORD RETENTION SCHEDULE

The table below lists some of the more common types of administrative records Trust staff are likely to encounter during their work and lists the minimum retention period applicable to those types of documents. Where applicable the derivation of the retention period is shown along with final disposal advice.

This list is not exhaustive and if a particular record type is not shown users should consult a full copy of NHS record retention schedules available on SUHTranet at the following link or contact the Trust Records manager for advice

http://suhtranet/index.cfm?articleid=1891

<table>
<thead>
<tr>
<th>TYPE OF RECORD</th>
<th>MINIMUM RETENTION PERIOD</th>
<th>DERIVATION</th>
<th>FINAL ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accident forms (see also Litigation dossiers)</td>
<td>10 years</td>
<td>Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (reg. 7): Social Security (Claims and Payments) Regulations (reg. 25)</td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Accident register (Reporting of Injuries, Diseases and Dangerous Occurrences register) – see also Incident forms</td>
<td>10 years</td>
<td>Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (reg. 7): Social Security (Claims and Payments) Regulations (reg. 25)</td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Accounts – annual (final – one set only)</td>
<td>30 years</td>
<td>See note 1</td>
<td>See note 1</td>
</tr>
<tr>
<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)</td>
<td>2 years from completion of audit</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Accounts - Annual (Final - one set only)</td>
<td>30 years</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Advance letters (eg DH guidance)</td>
<td>6 years</td>
<td></td>
<td>Destroy</td>
</tr>
<tr>
<td>Agendas of board meetings, committees, sub-committees (master copies, including associated papers)</td>
<td>30 years</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Agendas (other)</td>
<td>2 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Annual/corporate reports</td>
<td>3 years</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Audit Records (e.g. Organisational Audits, Records Audits, Systems Audits) – Internal &amp; External in any format (paper, electronic etc)</td>
<td>2 years from the date of completion of the audit</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Business plans, including local delivery plans</td>
<td>20 years</td>
<td></td>
<td>Destroy</td>
</tr>
<tr>
<td>Cash books</td>
<td>6 years after end of financial year to which they relate</td>
<td>Limitation Act 1980</td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Catering forms</td>
<td>6 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Chaplaincy records</td>
<td>2 years</td>
<td></td>
<td>May have archival value – see note 1</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Close circuit TV images</td>
<td>31 days</td>
<td>Information Commissioner’s Code of Conduct</td>
<td>Erase permanently</td>
</tr>
<tr>
<td>Complaints (See also litigation dossiers)</td>
<td>8 years from completion of action</td>
<td>Files closed annually and kept for 6 years following closure</td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Correspondence, investigation and outcomes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Returns made to DH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Input Forms (where the data/information has been input to a computer system)</td>
<td>2 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Diaries (office)</td>
<td>1 year after the end of the calendar year to which they refer</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Duty rosters</td>
<td>4 years after the year to which they relate</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>I.e. organisation or departmental rosters, not the ones held on the individual’s record.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exposure monitoring records</td>
<td>5 years from the date the record was made</td>
<td>Control of Substances Hazardous to Health Regulations 2002 (reg. 10(5))</td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Flexi working hours (personal record of hours actually worked)</td>
<td>6 months</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Freedom of Information requests</td>
<td>3 years after full disclosure; 10 years if information is redacted or the information requested is not disclosed</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Health and safety documentation</td>
<td>3 years</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Incident forms</td>
<td>10 years</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Job descriptions</td>
<td>3 years</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Laundry lists and receipts</td>
<td>2 years from completion of audit</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Litigation dossiers (complaints including accident/incident reports) Records/documents relating to any form of litigation</td>
<td>10 years Where a legal action has commenced, keep as advised by legal representatives</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Manuals – policy and procedure (administrative and clinical, strategy documents)</td>
<td>10 years after life of the system (or superseded) to which the policies or procedures refer</td>
<td></td>
<td>Destroy (policy documents may have archival value – see note 1)</td>
</tr>
<tr>
<td>Maps</td>
<td>Lifetime of the organisation</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Manuals (operating)</td>
<td>Lifetime of equipment</td>
<td></td>
<td>Review if issues (e.g. HSE) are outstanding</td>
</tr>
<tr>
<td>Medical device alerts</td>
<td>Retain until updated or withdrawn (check MHRA website)</td>
<td><a href="http://www.mhra.gov.uk">www.mhra.gov.uk</a></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Meetings and minutes papers of major committees and sub-committees (master copies)</td>
<td>30 years</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Meetings and minutes papers (other, including reference copies of major committees)</td>
<td>2 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Papers of minor or short-lived importance not covered elsewhere, e.g.: advertising matter, covering letters, reminders, letters making appointments, anonymous or unintelligible letters, drafts, duplicates of documents known to be preserved elsewhere (unless they have important minutes on them), indices and registers compiled for temporary purposes, routine reports, punched cards and other documents that have ceased to be of value on settlement of the matter involved</td>
<td>2 years after the settlement of the matter to which they relate</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Patient Advice &amp; Liaison Service (PALS) records</td>
<td>10 years after closure of the case</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Patient information leaflets</td>
<td>6 years after the leaflet has been superseded</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Patients’ property books/registers (property handed in for safekeeping)</td>
<td>6 years after the end of the financial year in which the property was disposed of or 6 years after the register was closed</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Patient Surveys (re access to services etc)</td>
<td>2 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Phone Message Books</td>
<td>2 years</td>
<td>NB Any clinical information should be transferred to the patient health record</td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Personnel/human resources records –major (eg personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained))</td>
<td>6 years after individual leaves service, at which time a summary of the file must be kept until the individual’s 70th birthday Summary to be retained until individual’s 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time. The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans</td>
<td>The 6 year retention period is to take into account any ET claims, or EL claims that may arise after the employee leaves NHS employment, requests for information from the NHS pension’s agency etc. Claims of this nature can include periods of up to 6 years or more prior to the claim and where evidence could be needed from a number of sources, it is appropriate to retain as much as possible from the original file.</td>
<td>See note 1</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Personnel/human resources records – minor (e.g. attendance books, annual leave</td>
<td>2 years after the year to</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>records, annual leave records, duty rosters (i.e. duty rosters held on the</td>
<td>which they relate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>individual’s record not the organisation or departmental rosters), clock cards,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timesheets (relating to individual staff members)) NB Includes locum doctors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Police Statements (made in the context of Accident and Emergency episodes.</td>
<td>10 years (congruent</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Statements are requested by the Police to the A&amp;E staff in relation to alleged</td>
<td>retention period as</td>
<td></td>
<td></td>
</tr>
<tr>
<td>injuries of or by patients coming through A&amp;E)</td>
<td>Incident Forms)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Press cuttings</td>
<td>1 year</td>
<td></td>
<td>Destroy (where bound volumes exist, see note 1)</td>
</tr>
<tr>
<td>Press Releases</td>
<td>7 years</td>
<td></td>
<td>see note 1</td>
</tr>
<tr>
<td>Public Consultations e.g. about future provision of services</td>
<td>5 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Quality assurance records (e.g. Healthcare Commission, Audit Commission,</td>
<td>12 years</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>King’s Fund Organisational Audit, Investors in People)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radioactive waste</td>
<td>30 years</td>
<td>Radioactive Substances Act 1993</td>
<td>See note 1</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Receipts for registered and recorded mail</td>
<td>2 years following the end of the financial year to which they relate</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Records documenting the archiving, transfer to public records archive or destruction of records</td>
<td>30 years</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Records of custody and transfer of keys</td>
<td>2 years after last entry</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Reports (major)</td>
<td>30 years</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>Requests for access to records, other than Freedom of Information or subject access requests</td>
<td>6 years after last action</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Requisitions</td>
<td>18 months</td>
<td></td>
<td>Destroy under confidential conditions</td>
</tr>
<tr>
<td>Research and development (organisation) i.e. all the organisation’s records associated with research and development and not individual trial records or information on patients.</td>
<td>30 years</td>
<td>Medical Research Council</td>
<td>See note 1</td>
</tr>
<tr>
<td>Research ethics committee records</td>
<td>3 years from date of decision</td>
<td></td>
<td>See note 1</td>
</tr>
<tr>
<td>TYPE OF RECORD</td>
<td>MINIMUM RETENTION PERIOD</td>
<td>DERIVATION</td>
<td>FINAL ACTION</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>--------------------------</td>
<td>------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Serious incident files</td>
<td>30 years</td>
<td>See note 1</td>
<td></td>
</tr>
<tr>
<td>Statistics (including Korner returns, contract minimum data set, statistical returns to DH, patient activity)</td>
<td>3 years from date of submission</td>
<td>Destroy</td>
<td></td>
</tr>
<tr>
<td>Subject access requests (DPA and AHR)– records of requests</td>
<td>3 years after last action</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Surgical appliances forms AP 1, 2, 3 and 4</td>
<td>2 years from completion of audit</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
<tr>
<td>Timesheets (for individual members of staff)</td>
<td>2 years after the year to which they relate NB Timesheets (for all individuals including locum doctors) held on the personnel record are minor records – retain for 2 years.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time sheets (relating to a Group or Department e.g. Ward where the timesheets are kept as a tool to manage resources, staffing levels)</td>
<td>6 months</td>
<td>Destroy under confidential conditions</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 5 to SUHT Records Management Policy

User Guide to Record Disposal

1. When records are no longer required for business use or at the end of a specified minimum retention period they should be reviewed. The aim of this review is to determine whether or not they are worthy of permanent preservation, whether they need to be retained for a longer period or whether they should be destroyed.

2. Records should not be destroyed before the end of the recommended minimum retention period published in the NHS Code of Practice. Records can be kept for longer than the minimum recommended retention period but in most cases no longer than 30 years unless transferred to the national archives or a recognised local place of deposit.

3. Recommended minimum retention periods should be calculated from the end of the calendar or accounting year following the last entry in the document. The minimum retention periods recommended in the code of practice are based on long standing practice reflecting established thinking about the usefulness of the records for the business of the NHS and take account of statutory requirements which impose a duty to retain certain records for periods of time.

4. If it is decided that a record is to be retained in its current form for a longer period the record should be marked to indicate the next date for review or a date for disposal. Records not selected for retention in this way are then considered for disposal which may take the form of:
   - Transfer to the safekeeping of another organisation
   - Transfer to another medium and retained in that format
   - Transfer to the National Archives/Local Place of Deposit for permanent preservation
   - Destruction

5. A proposal to select a record for permanent preservation may be made because of the historical significance of the data held, for purposes of future research or for example to record pioneering and innovative treatments. It is not always necessary to retain all the contents of a record or series of records but to consider only retaining a selection of material from each record, a sample of a series of records or an illustrative selection of records.

6. Advice on all aspects of preservation can be obtained from the Archivist of Southampton City Council who act as a local place of deposit for the Trust and therefore would be involved in any proposal to preserve records on a permanent basis. Proposals to preserve records permanently should in the first instance be discussed with the Trust Records Manager.

7. The Data Protection Act (1998) places restrictions on the storage and use of personal information and care must be taken to ensure that retention proposals take account of principle 5, which states that:

   ‘Personal data shall not be kept for longer than is necessary for its purpose.’
Appendix 6 to SUHT Records Management Policy

Standards for Clinical Record Keeping in the Trust

INTRODUCTION

1. The purpose of this Appendix is to provide clear multi-professional guidance for clinical record keeping in the Trust. It incorporates a set of standards based on current Department of Health, General Medical Council and Royal College guidelines for Clinical Record Keeping.

2. Healthcare professionals have individual accountability for keeping up to date with the latest evidence of best practice in record keeping and should follow any record keeping recommendations arising from National Confidential Enquiries.

3. As a minimum the Trust expects that the standards published below to be followed and compliance with these will be audited every two years in a series of Trust wide audits. The audit tools will be made available on-line by the Clinical Effectiveness Team. The audit data must be collected in a multi-professional way at care group level.

THE HOSPITAL RECORD

4. A hospital record must be maintained for every patient. Each record should contain as a minimum the following identification data:

   a. the patient’s unique hospital number
   b. the patient’s NHS number
   c. the patient’s full name, address and postcode
   d. telephone contact number
   e. date of birth
   f. sex
   g. person to notify in an emergency (NOK)
   h. marital status,
   i. the patient’s registered general practitioner (GP)

5. In both electronic and written patient records the patient’s hospital number and name should be displayed on every page/screen. If an inpatient the patient’s location should also be displayed/recorded. (Please note over the next few years the NHS number will replace the hospital number as the main patient identifier.)

6. Currently the Trust Patient Administration system (PAS) collects and records this information when a patient is registered. The information is held as part of the Patient Master Index (PMI). Other electronic clinical systems used in the Trust should be automatically linked to PAS PMI to ensure this data remains consistent and up to date on all systems.
THE CLINICAL RECORD

General Standards and process for ensuring a contemporaneous complete record of care.

7 Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order.

8 Every entry in the medical record should be dated, timed (24-hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned.

9 Every entry in the notes should be made as soon as possible after the event to be documented (e.g. change in clinical state, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded.

10 Every entry in the notes should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made.

11 On each occasion the consultant responsible for the patient's care changes, the name of the new responsible consultant and the date and time of the agreed transfer of care, should be recorded.

12 An entry should be made in the medical record whenever a patient is seen by a doctor. When there is no entry in the hospital record for more than four (4) days for acute medical care or seven (7) days for long-stay continuing care, the next entry should explain why. (The maximum interval between entries in the record would in normal circumstances be one day or less. However, the maximum interval that would cover a bank holiday weekend for example should be four days.)

13 Advance Directives, consent and resuscitation status statements must be clearly recorded in the medical record.

14 A discharge record /summary should be commenced at the time a patient is admitted to hospital.

15 Entries in the notes must not be abbreviated – any exceptions to this must be agreed and published as part of this policy.

16 Entries must not include meaningless phrases and offensive subjective statements unrelated to the patient’s care and associated observations.

Standards for Documenting Surgery

17 For patients undergoing surgery, records should include details of the following:

   a. Signed evidence that informed consent has been obtained by a doctor or an appropriately trained nurse practitioner.
b. Signed evidence that the correct procedure was followed when obtaining consent for children under the age of 16 years,

c. Documented details of the discussion with the patient including details of the written information that was issued i.e. national or local leaflet (and, where possible, include version and publication date). If the patient declines any information whether written or verbal, this must be documented.

d. For patients undergoing anaesthetic, documented details of the discussion with the anaesthetist (except in the case of local anaesthetic where the discussion can be with another member of the healthcare team)

e. The medical care plan should include the site and side of any operative procedure. Sites and sides must be written out in full and not abbreviated.

18 A record of the operation should be included in the clinical notes. It should be made immediately following surgery and should include:

a. The date.
b. The name and signature of the operation surgeon(s) and the name of the consultant responsible.
c. The diagnosis made and the procedure performed - what was done and who by: Incision, Operation, Closure, Drains, and Surgeon.
d. Description of the findings.
e. Details of tissue removed, altered or added
f. Details of serial numbers of prosthetics used,
g. Details of sutures used,
h. An accurate description of any difficulties or complications encountered and how these were overcome – documentation of: bleeding; inadvertent damage to other structures; unplanned procedures; other colleagues called to help. Documentation that the patient was informed.
i. Immediate post-operative instructions, and
j. The surgeon’s signature

19 The operation record should also contain information relating to anaesthesia including:

a. The name of the anaesthetist and, where relevant, the name of the consultant anaesthetist responsible.
b. Pre-operative assessment by the anaesthetist.
c. Drugs and doses given during anaesthesia and route of administration,
d. Monitoring data.
e. Intravenous fluid therapy, if given.
f. Post-anaesthetic instructions – fluids, drains, catheters and sutures. Reasons will be documented in notes, letters and nursing notes.
g. Name and signature of anaesthetist.

20 If the patient returned to theatre there should be clear details documented in the notes as to why, and the names of surgeons involved; whether this was planned or unplanned; complications; consent.

Patients in Intensive Therapy Units

21 The record should include:

a. A clear statement why the patient was admitted to the ITU,
b. An accurate record of monitoring of the physiological state while the patient was in ITU, and
c. Contemporaneous details of all therapeutic manoeuvres performed.

22 When the patient is moved from the ITU, a description of the patient’s clinical status must be written down and the reason for transfer adequately described in the notes.

Nursing Notes

23 The Nursing record is an important part of the hospital record should be filed in a clearly designated part of the clinical record.

Documentation Recording Admission, Handover and Discharge

24 The Trust is working towards the introduction of standardised proforma for the recording of patient admission, handover and discharge. The Royal College of Physicians have developed sets of core headings and definitions for these documents and these will be used as the basis for the development of standardised documents for use in the Trust.

(Details at: http://www.rcplondon.ac.uk/clinical-standards/hiu/medical-records/Pages/Overview.aspx

25. As a first step in this process the Trust has introduced a standardised electronic discharge summary that should be used to record the discharge of all patients. A copy of the summary should be sent to the patients GP within 24 hours of discharge and a copy filed in the patients notes.

Recording a Patient’s Death in Hospital

26 The entry made when death is confirmed should contain the following information:

   a. Date and time of entry
   b. Name of clinician confirming death in block capitals
   c. Designation of clinician confirming death
   d. Examination made establishing death
   e. Time and date patient certified dead
   f. Signature of clinician confirming death, followed by full name in block capitals

27 When the death certificate is completed, an entry should be made in the record stating:

   a. The cause of death as appearing on the death certificate.
   b. Whether a cremation form has been completed.
   c. Whether and how the deceased relatives have been or will be informed.
   d. Whether and how the general practitioner has been or will be informed.

Queries on Entries in Patient Health Records

28. Should a query arise about an entry in a in a patient health record the first course of action should be to try and identify the author and clarify the matter with them. Where this is not possible a senior member of the relevant speciality or Care Group should be
approached for advice. In the event this does not resolve the matter the issue should be raised with the Trust Records Manager.

References

2007 Royal College of Physicians, *Generic Medical Record-Keeping Standards*


1994 Royal College of Surgeons of England, *Guidelines for Clinicians on Medical Records and Notes*

Appendix 7 to SUHT Records Management Policy

Audit of Clinical Record Keeping and Management in the Trust

1. In order to assess compliance with the Trust standards for patient health record keeping and management two annual audits will be undertaken. The clinical effectiveness team will organise an audit of record keeping assessing compliance with the Trust standards for record keeping published in this document. The Trust Records Manager will organise an audit to assess compliance with patient health records management standards and record tracking.

2. In each case Care groups will participate in data collection and the results will be reported to Divisional Governance Managers and Clinical Effectiveness Leads. Compliance of less than 80% with audited standards will be deemed unsatisfactory and require remedial action.

3. Audit Proformas will be designed and supplied by the clinical effectiveness team.

4. Divisional Governance Groups will be responsible for ensuring:
   a) Care groups develop action plans
   b) Care groups monitor the implementation of actions and these are signed off
   c) The central Clinical Effectiveness Team are informed of the agreed actions and further informed once actions have been implemented.