

Title: **RECORDS MANAGEMENT POLICY**

Reference No: NHSNYYIG - 002

Owner: Director of Performance & Delivery

Author: Records Management & Freedom of Information Officer

First Issued On: 19th February 2009

Latest Issue Date: February 2010

Operational Date: March 2010

Review Date: April 2011

Consultation Process: Key internal stakeholders (management & staff-side); JNCC; LNC

Policy Sponsor: Information Governance Steering Group

Ratified and Approved by: Governance Committee

Distribution: All staff

Compliance: Mandatory for all permanent & temporary employees, contractors & sub-contractors of NHS North Yorkshire and York

Equality & Diversity Statement: Compliant

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERS No
27/08/2008	Records Management & FOI Officer	New policy draft: Model Connecting for Health Records Management Roadmap Records Management Policy (document 02A). Formatted in compliance with NHS NYY Policy on Policies (PoP) and additional paragraphs added as follows: Preface – in compliance with PoP 4.3 Director of Performance & Delivery & AD of IM&T delegated responsibilities 4.8 SLA's & contracts 8.3 Annual audits 8.5 Research governance 8.6 Security breaches & lost records 10.2 Retention of policy (in compliance with PoP) 11.0 Equality & diversity statement (in compliance with PoP) 12.0 Disciplinary statement (in compliance with PoP) 13.0 References (in compliance with PoP)	0.001
27/08/2008	IG Manager	New policy draft forwarded to AD IM&T for initial comment.	0.001
29/09/2008	IG Manager	New policy draft circulated to key stakeholders for comment.	0.001
12/01/2009	IG Manager	Updates and the addition of section 7 – 15 after Records Management Audit by Paul Finn.	0.101
11/02/2009	IG Manager	Document Approved by IGSG	0.102
13/02/2009	IG Manager	Changes as per Tanya Matalainan	0.103
19/02/2009	IG Manager	Document Approved by Governance Committee	1.001
15/04/2009	IG Manager	Formatting Errors Corrected	1.002
10/02/2010	IG Manager	Updates to policy	2.000



Contents

Preface.....	4
Document Objectives	4
Intended Recipients.....	4
1. Introduction	4
2. Scope and Definitions	5
3. Aims of our Records Management System	6
4. Roles and Responsibilities	7
5. Legal and Professional Obligations	8
6. Registration of Record Collections	9
7. Record Structures	10
8. Creating and Updating Records	11
9. Accessing and Retrieving Records	13
10. Access Enablement - Tracking.....	14
11. Storing Records.....	15
12. Means of Storage	17
13. Transporting Records.....	21
14. Retention of Records.....	23
15. Disposal of Records	24
16. Records Management Systems Audit	24
17. Research Governance	26
18. Security Breaches and Lost Records	26
19. Training	27
20. Policy Review & Retention	27
21. Equality & Diversity Statement	27
22. Disciplinary Statement	27
Annex A Legislation and National Policies	28
A.1 Record Management: NHS Code of Practice	28
A.2 Standards for Better Health	28
A.3 The Data Protection Act 1998	28
A.4 Access to Health Records Act 1990	29
A.5 The Caldicott Review.....	29
A.6 Freedom of Information Act 2000	29
Annex B Examples of Records and Media	31
Annex C References	32
Annex D Information Flow Data Mapping Tool.....	33
Annex E Types of Records Requiring Registration	34
Annex F Records Management Audit Report.....	35
Annex G Information Asset Register.....	36

Preface

This Policy is made between NHS North Yorkshire and York (NHS NYY; “the organisation”) and the recognised staff side organisations, using the mechanism of the Joint Negotiation and Consultative Committee (JNCC). It will remain in force until superseded by a replacement Policy, or until terminated by either management or staff side, giving no less than six months notice. The purpose of the notice to terminate the Policy is to provide the opportunity for both parties to renegotiate a replacement Policy. Withdrawal by one party, giving no less than six months notice, will not of itself invalidate the agreement. If agreement cannot be reached on a revised policy, then either party may refer the matter to the Advisory, Conciliation and Arbitration Service (ACAS) for conciliation.

Intended Recipients

All staff with record management responsibilities.

1. Introduction

- 1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their life cycle to their eventual disposal.
- 1.2 The Records Management: NHS Code of Practice© has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.
- 1.3 The organisation's records are important sources of administrative, evidential and historical information, providing evidence of actions and decisions, and represent a vital asset to support the organisations daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisation, to support patient care and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.
- 1.4 The organisation has adopted this records management policy and is committed to ongoing improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:
 - helping to improve accountability
 - showing how decisions related to patient care were made
 - supporting the delivery of services
 - supporting effective clinical judgements and decisions
 - supporting patient care and communications
 - making continuity of care easier
 - providing documentary evidence of services delivered
 - promoting better communication and sharing of information between members of the multi professional healthcare team
 - helping to identify risks, and enabling early detection of complications
 - supporting clinical audit, research, allocation of resources and performance planning
 - helping to address complaints or legal processes
 - support compliance with requirements of the Freedom of Information Act 2000
 - making better use of physical and server space;
 - supporting better use of staff time;
 - improved control of valuable information resources;
 - compliance with legislation and standards; and
 - reducing costs.
- 1.5 The organisation also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.
- 1.6 This document sets out a framework within which the staff responsible for managing the organisation's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

- 1.7 This policy document should be read in conjunction with the organisation's Records Management Strategy which sets out how the policy requirements will be delivered and the Policy for Clinical Records Keeping Standards which details specific requirements for the professional maintenance of health records.

2. Scope and Definitions

- 2.1 This policy relates to all clinical and non-clinical operational records held in any format by the Organisation. See Annex B for examples of different types of media covered by this policy.

Records holding personal identifiable information on service users and their contacts, staff and the public will need to be managed in accordance with the Data Protection Act 1998 (DPA) and the Common Law Duty of Confidence. Such information may include next of kin, emergency contacts and carers.

Where information does not identify an individual either directly or indirectly or where it has been effectively anonymised, neither the DPA nor the Common Law Duty of Confidence apply.

Policy on the Data Protection and the Duty of Confidence are set out in the following organisation policy documents:

- Data Protection Policy;
- Confidentiality Policy and Confidentiality: NHS Code of Practice; and
- Other Information Governance policies, procedures, guidance and relevant Legal and Professional obligations.

Records on corporate matters may be subject to the Common Law Duty of Confidence and may also be classified as sensitive or non-sensitive in terms of their impact on the running of the business if lost or disclosed. However in certain circumstances it may be appropriate to disclose certain non-personal information that has been classified as sensitive that is held by the organisation in accordance with the Freedom of Information Act 2000.

- 2.2 **Records Management** is a discipline which utilises an administrative system to securely direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the organisation and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- disposal.

- 2.3 The term **Records Life Cycle** describes the life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.
- 2.4 In this policy, **Records** are defined as 'recorded information, in any form, created or received and maintained by the organisation in the transaction of its business or conduct of affairs and kept as evidence of such activity'. However a distinction must be made between a document and a record. A document becomes a record when it has been finalised and becomes part of the organisations corporate information or is included as part of the health record. This refers to records held in any media.
- 2.5 All NHS records are public records under the terms of The Public Records Act 1958 and as such the organisation has a duty to make arrangements for the safe keeping, maintenance, archiving and eventual disposal of all types of records. To do this effectively the organisation needs to ensure that it can provide adequate audit trails, have logical filing structures, control access, establish naming conventions, apply version control standards, and protectively mark records. Where records are held electronically the organisation must support technological upgrades to ensure records remain accessible and usable throughout their lifecycle and systems must permit cross referencing of electronic records to their paper counterparts where dual systems are maintained.
- 2.6 **Information** is a corporate asset. The organisation's records are important sources of administrative, evidential and historical information. They are vital to the organisation to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.
- 2.7 This policy covers the management of records and not the detailed requirements of what a record should contain for either organisational or clinical use.

3. Aims of our Records Management System

- 3.1 The aims of the Records Management System are to ensure that:
- **records are available when needed** - from which the organisation is able to form a reconstruction of activities or events that have taken place, and facilitate the effective continuity of day to day business;
 - **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
 - **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
 - **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
 - **records can be maintained through time** – the qualities of availability, accessibility, interpretation and organisational worthiness can be maintained

for as long as the record is needed, and on occasion permanently, despite changes of format;

- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled to ensure that audit trails will track all use and changes and clinical staff are confident that organisational records management procedures support them in their professional duty to protect the confidentiality of the patient records. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records should be protected by a contingency or business continuity plan** – protection needs to be in place for all types of records that are vital to the continued functioning of the organisation. Based on an assessment of risk and following the corporate approach documented plans should be drawn up, tested and reviewed.
- **records are retained and disposed of appropriately** - using consistent, secure and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

4. Roles and Responsibilities

4.1 Chief Executive

The Chief Executive has overall responsibility for records management in the organisation. As the Accountable Officer he/she 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.

The organisation has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 Caldicott Guardian

The organisation's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. The Caldicott Guardian also has a strategic role which involves representing and championing information governance requirements and issues at Board / Management Team Level. The Caldicott Guardian is the Deputy Chair of the Information Governance Steering Group.

4.3 Director of Performance & Delivery / Assistant Director of Information Management & Technology

The organisation's Director of Performance & Delivery has been delegated with the responsibilities of the Senior Information Risk Officer (SIRO) and as the Board Level Lead for Information Governance, and as such is accountable for Information Governance. The SIRO chairs the Information Governance Steering Group. The SIRO must ensure that specific reference to information governance in terms of

identifying and managing information risks is included in the organisations annual Statement of Internal Controls.

4.4 Information Governance Steering Group / Records Management Officer

The organisation's Information Governance Steering Group / Records Manager supported by the Information Governance Team are responsible for ensuring that this policy is implemented, through the Records Management Strategy, and that the records management system and processes are developed, co-ordinated and monitored.

4.5 Records Manager/ Records Management Office

The Assistant Director of Governance (Provider Services), Records Manager and Local Records Managers are responsible for the overall development and maintenance of health records management practices throughout the organisation, in particular, in conjunction with the Records Manager, for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

4.6 Local Record Managers

The Local Records Managers appointed at each main NHS NYY location are responsible for ensuring that the Records Management Policy is available and understood by all staff at the location, for ensuring that records controlled within their location are managed in a way which meets the aims of the organisation's records management policies.

4.7 Local Team Leaders / Supervisors

The responsibility for local records management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units and business functions within the organisation have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the organisation's records management policies.

4.8 All Staff

All organisation staff, whether clinical or administrative, 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 organisation and manage those records in keeping with this policy and with any guidance subsequently produced.

4.9 Contractors and Support Organisations

Service Level Agreements and contracts must include responsibilities for information governance and records management as appropriate.

5. Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. The organisation will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;
- The Data Protection Act 1998;

- The Freedom of Information Act 2000;
- Safeguarding Vulnerable Groups Act 2006;
- The Common Law Duty of Confidentiality;
- Existing Clinical Professional Obligations;
- The NHS Records Management Code of Practice;
- The NHS Confidentiality Code of Practice;
- Access to Health Records 1990
- The Computer Misuse Act 1990
- Human Fertilisation and Embryology Act 1990
- The Caldicott Report 1997
- Security Management NHS Code of Practice 2007

This is not an exhaustive list. See Annex A.

6. Registration of Record Collections

- 6.1 The organisation will establish and maintain mechanisms through which directorates/ departments and other units can register the records they are maintaining. The inventory of record collections will facilitate:
- the classification of records into series; and
 - the recording of the responsibility of individuals creating records.
- 6.2 The register must be reviewed annually.
- 6.3 A list of records that require registration is attached, see Annex E.
- 6.4 If any new record collections are created containing personal information, the Information Flow Data Mapping Tool must be completed and sent to the organisations Records Manager; see Annex D. This ensures that the requirements of the DPA and the Caldicott Report are met.
- 6.5 Registration will be achieved by:
- For Patient Records, the allocation and recording of a unique identifier which will be in accordance with the requirements of the pseudonymisation project for secondary uses.
 - For other Records, the allocation of a unique identifier the format of which will be in accordance with the requirements of section 7 below.

With the development of electronic patient records, the NHS number will become the unique identifier for all Patient Records.

- 6.6 Registration systems should be monitored regularly and reviewed at least annually at the same time as the register is reviewed to ensure that systems continue to operate effectively and efficiently and meet the needs of users.
- 6.7 All records held by the organisation that are listed within the Retention and Disposal Schedule of the Records Management: NHS Code of Practice and any organisational additions require registration. Any further decisions around registration in the case of clinical records should be made between the Records Manager and the Caldicott Guardian. To ensure consistency and avoid duplication the corporate registration document will be the same document used to meet criterion 307 of the Information Governance toolkit which is known as the 'Information Asset Register'. See Annex G

7 Record Structures

- 7.1 To ensure appropriate information governance is applied across the organisation it is essential that certain criteria are met, for both corporate and clinical records to ensure that records are held in a secure and logical manner and to support the organisations business activities. This will also facilitate the organisation in applying the required appropriate access controls to information, on a need to know basis in order to ensure the right information is in the right place, at the right time, and available to the right people
- 7.2 **Referencing:** Each Directorate should establish, document and ensure compliance to a referencing system that meets its business needs that it easily understood by staff members that create, file or retrieve records held in any media. Several types of referencing can be used, e.g. alpha-numeric, alphabetic, numeric or keyword. The most common of these is alpha-numeric, as it allows letters to be allocated for a business activity, e.g. HR for Human Resources, followed by a unique number for each electronic record or document created by the HR function. It may be more feasible in some circumstances to give a unique reference to the file or folder in which the records are kept, and identify the record by reference to date and format.
- 7.3 **Naming:** Each Directorate should nominate staff to establish and document file naming conventions in line with national archives advice; i.e.
- Give a unique name to each record,
 - Give a meaningful name which closely reflects the records contents,
 - Express elements of the name in a structured and predictable order,
 - Locate the most specific information at the beginning of the name and the most general at the end,
 - Give a similarly structured and worded name to records which are linked (for example, an earlier and a later version).
- 7.4 **Indexing and Filing:** Each Directorate should establish and document a clear and logical filing structure that aids retrieval of records. The register or index is a signpost to where paper corporate records are stored, e.g. the relevant folder or file, however it can be used as a guide to the information contained in those records. The register should be arranged in a user friendly structure that aids easy location and retrieval of a folder or file. Folders and files should be given clear logical names that follow the organisations naming convention.

The filing structure for electronic records should reflect the way in which paper records are filed to ensure consistency. Filing of corporate records to local drives on PC's and laptops is not appropriate, files must be saved to the departmental network,

to ensure access authorized is available and that appropriate backups are taken. Likewise, the filing of key organisational paper records or clinical records in desk drawers is not appropriate, departmental accessible secure storage should be used.

8 Creating & Updating Records

8.1 When records are created and/or updated, it is essential that indices are first checked to avoid duplicate records being created for the same person e.g. records held on any patient information system. These must comply with the requirements of section 7 above.

8.2 Local procedures should be put into place to ensure data quality for both manual and electronic records complies with the requirements of the corporate Data Quality Policy. These procedures should be regularly reviewed and updated where required.

8.3 All Records

All record entries must:

- Meet mandatory data sets such the Mental Health Minimum Data Set to ensure adequate information is held.
- Be factual, consistent, accurate and consecutive.
- Be recorded as soon as possible after an event has occurred.
- Keep the use of abbreviations to a minimum. If abbreviations are used, they should be from an agreed list which can be made available on request.
- Provide clear evidence of action or care planned.

8.4 Clinical Records

Clinical record entries must as a minimum:

- Contain the patients name, NHS Number and date of birth
- Be written clearly, legibly and in such a manner that they cannot be erased.
- Be factual, consistent and accurate and recorded in such a way that the meaning is clear
- Give accurate details of assessments and reviews undertaken and provide clear evidence of arrangements for ongoing care.
- Record risks or problems identified and action taken to deal with them.
- Not have errors. A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment.
- Be accurately dated, timed and signed, with the persons name, job title and signature being printed alongside the first entry or the signature sheet completed.
- Be bound and stored so that loss of documents is minimised.
- Be written in black ink (manual records)

- Contain a filing index and section dividers (manual records)
- Named in line with the local naming conventions (electronic records)
- Have an integral audit trail providing at least the equivalent information (electronic records).
- Records should be readable when photocopied or scanned
- Clinical records must be marked confidential.
- Avoid unnecessary abbreviations, jargon, meaningless phrases, personal opinions, irrelevant speculation and offensive subjective statements, do not use coded expressions of sarcasm or humorous abbreviations to describe those cared for.
- Professional judgment should be used to decide what is relevant and what should be recorded
- Be written at the time of or as soon as possible after an event has occurred, providing current, contemporaneous information on the care and condition of the patient.
- Record details of any assessments and reviews undertaken and provide clear evidence of any arrangements made for future and ongoing care. This should also include details of information given about care and treatment. There is a duty to fully and effectively communicate with colleagues ensuring that all information is provided regarding the people cared for.
- Be consecutive
- Where appropriate the patient or their carer should be involved in the record keeping process and the language used should be easily understood by those cared for.
- Do not alter or destroy any records without being authorised to do so
- In the unlikely event that healthcare records need to be altered it any alterations must be approved and signed, dated include name and job title and the date of the original documentation. The alterations made and the original record are clear and auditable.
- NEVER falsify records

8.5 Validating Records

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

- Timely
- Accurate
- Complete
- Relevant
- Secure
- Accessible
- And comply with all requirements detailed above

The organisation must have an appropriate audit programme in place for all such records to ensure standards are maintained.

The organisation has developed both a clinical record keeping standards audit programme (as detailed in the Clinical Records Keeping Standards Policy) and a records management audit tool detailed at Annex F in place for all such records to ensure standards are maintained.

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

8.6 Correspondence from Relatives of Patient

Where correspondence from a Patient's relative(s) is to be included in a Patient's record, permission must first be obtained from the relative(s) who created the correspondence, they must be made aware of who will access the information, including the patient and the reasons why. If permission is received the correspondence can be added to the record unmarked, if permission is not received, the correspondence must be marked as "This correspondence is not to be released *include any limitations on disclosure* without the express permission of the creator of the correspondence".

9 **Accessing and Retrieving Records**

9.1 When a record is in constant or regular use, or is likely to be needed quickly, secure easy access must be available for staff within their working environments.

9.2 All records must be accessed solely on a need to know basis and control of access levels must be documented and maintained in accordance with the organisations information security policy.

9.3 Multi-agency patient records

Where the care of patients is managed by a number of different agencies, this may be supported by multi-agency care records.

The organisation will formally agree with partner agencies the processes and common standards for the creation and updating of records, the periods of retention and the secure authorised access to multi-agency care records. These are to be documented maintained and audited across all such agencies.

9.4 Patient held records

Control of access to patient held records must be on a need to know basis. This should be enabled by:

- The patient being advised of their rights in respect of whom they show their records to.
- Practitioners observing the need to know principle when looking at such records.

9.5 Personal Data

Under the requirements of DPA – Part II, Section 7, subject to specific provisions referred to below, an individual is entitled to be:

- Informed whether their personal data are being processed by the organisation.
- Advised of the nature of the data, the purposes for such being processed and with whom it is being disclosed.
- Informed of the data held and its source(s).
- And have access to information held about them, subject to certain exemptions. Please see the Subject Access Policy for further guidance.

10 **Access Enablement – Tracking**

The accurate recording and knowledge of the whereabouts of all records regardless of the media they are held on, is essential if the information they contain is to be accessed quickly, efficiently, this will also provide a mechanism to ensure appropriate security of records is in place at all times.

There is a requirement to record the movement and whereabouts of all records, whether they are the original or a copy (herein referred to as 'the record'). The whereabouts and movement of any records must be formally recorded so that they are traceable at all times. Formal procedures for tracking and tracing of records should enable the business functions of the organisation to continue without unnecessary disruption

10.1 Tracking Mechanisms for all records irregardless of the media they are held on

Directorates must ensure that all departments have tracking systems in place to record the following information as a minimum:

- The reason for the removal of the record, including appropriate authorisation and details of who it may be shared with
- The name of the record.
- The media it is held on
- The method of transfer
- The person who has removed the record,
- The person, unit, department or place to which it is being sent or taken.
- The date of removal or transfer of the record.
- Signature of the person removing it.
- The expected and actual date of the return of the record.
- Signature of the person returning it

Each tracking system, manual or electronic, must meet all user needs and be supported by adequate equipment and should provide an up-to-date and easily accessible movement history and audit trail.

Since the success of any tracking system depends on the people using it, all staff must be made aware of its importance and given adequate training and updating.

Tracking systems must take into account the absolute requirement to have a complete patient's health record present to facilitate appropriate consultation and treatment.

Tracking systems must be implemented and reviewed annually or after any serious untoward incident for operational effectiveness.

10.2 Manually operated tracking systems

Files/ records must be tracked when removed from the department/ building that stores them.

Acceptable methods for manually tracking the movements of active records include the use of:

- A paper register – a book, diary, or index card to record transfers
- File “on loan” (library-type) cards for each absent file, held in alphabetical or numeric order
- File “absence” or “tracer” cards put in place of absent files

Where manual tracking systems are used they must be kept to update otherwise the system will quickly be rendered ineffective.

10.3 Electronically operated tracking systems

Acceptable methods of tracking include the use of:

- A computer database with clearly defined access permission rights.
- Bar code labels and readers linked to computers.
- Workflow software to electronically track documents.
- Functionality built into any electronic records management systems.

Electronic tracking systems are a preferred option; if used, the Records Manager should be contacted and will advise of the appropriate procedure to be followed.

Where electronic tracking systems are used, staff must be fully trained; otherwise the system will quickly be rendered ineffective.

11 **Storing Records**

11.1 Choice of Media

The choice of media should be based on consideration of practicality and costs; advice will be provided by the Records Manager.

11.2 Paper

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

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

This list is not exhaustive.

11.3 Archives

For reasons of business efficiency or in order to address problems with storage space the organisation may wish to consider the option of storing records on microfilm and fiche or the option of scanning in to electronic format records which exist in paper format. Where this is proposed the factors to be taken into account include:

- the cost of the initial and any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept.
- The need to consult in advance with the local place of deposit or the national archives with regard to records which may have archival value, as the value may include the format in which it was created, and
- The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards in particular the 'Code of Practice for Legal admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008)

11.4 Electronic Files

For the majority of working documents, storage in electronic format is preferred because of convenience, cost, efficiency and security. This must be completed in line with the requirements of section 7 of this policy.

11.5 Other Media

Data may be stored as radiology images, photographs, films, videotape or sound recordings where this is necessary for specified purposes.

All staff should follow organisation policies and procedures for the storage, retention and disposal of audiovisual recordings held on paper or in electronic form.

Recordings must be stored securely, in a manner that enables ease of access and backup and which complies with the organisation's Minimum Information Security Measures.

Recordings must be retained in compliance with the retention periods described in the Records Management: NHS Code of Practice (part 2) 2nd Edition January 2009, and only disposed of once the full retention period has elapsed and the record has

been appropriately considered for permanent archiving. Records must be disposed of in a secure and confidential manner.

The consent of the subject must, in all circumstances, be obtained in order to make any recording for the assessment and treatment of patients.

12 Means of Storage

12.1 Paper Records

12.1.1 Individual Record Folders

Individual record folders should enable ease of adding information to different sections and must be designed in line with any local practices which are based on professional guidance for which the records are used.

12.1.2 Carbonised Records

Where carbonised duplications are made, the original top copy should be retained by the organisation due to the eventual deterioration in quality of archived carbonised paper records.

12.3 Other Media

12.3.1 Microfilm and Fiche (Microform)

Microform can be in roll film format or in microfiche format. Master negative and working positive copies should be made. Only the positive copies should be used for reference purposes.

Master copies should be stored in closed non-airtight containers made of non-corrosive materials, such as inert plastic. Containers should also be free of bleaching agents, glues and varnishes.

Rolls of film should be mounted on inert reels and secured by the use of acid free paper ties. Fiche and jacketed film should be stored in acid-free envelopes.

Rubber bands and paper clips should not be used.

Microform should be stored in controlled atmospheric conditions, with temperature between 15 and 20 degrees centigrade (ideally not exceeding 18 degrees).

12.3.2 Visual Images

In the case of Radiology Images and photographs, the quality of the images available from negatives or original prints should be considered and new prints may be made in cases where the original is deteriorating.

Film should be stored in dust-free metal cans and placed horizontally on metal shelves.

Sound recordings and video recordings (tape and DVDs) should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

12.3.3 Scanning

The option of scanning paper records into electronic format may be considered for reasons of business efficiency, to address problems with storage space or to include a record of a paper document within an existing electronic record.

Where this is proposed, the following factors should be taken into account:

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

Advice and guidance on the choice of an acceptable format for scanned documents should be sought from the Records Manager.

The choice of format must take into account the requirement to ensure that any attachment to an existing electronic clinical record should be regarded as having equal medico-legal weight as notes made within the usual recording system and should be accorded the same standards regarding an audit trail and backup.

12.1.3 Patient Held Records

Patients should be advised to keep their records safe, but in a location where they can be readily accessed when needed, by healthcare or other appropriate professionals following the need to know basis as laid down by the Caldicott Principles.

12.1.4 Bulk Storage – Current Records

Storage equipment for current records in use must be secure and located in a manner that enables speedy access by users. This may be:

- In central or approved local filing systems e.g. for common corporate files or patient record files.

Records must always be kept securely and when a room containing records is left unattended it must be locked.

An appropriate sensible balance should be achieved between the needs for security and accessibility.

Decisions on the suitability of office filing equipment must take the following factors into account:

- Compliance with Health & Safety regulations.
- Users' needs, usage and frequency of retrievals.
- Security (especially for confidential material).
- Type(s) of records to be stored and their size and quantities.
- Suitability, space efficiency and price.
- Fire-proofing and Water-proofing.
- Protection from environmental damage (e.g. light damage to negatives).

Appropriate advice on the above will be provided by the Records Manager, Information Governance Team or the Health and Safety Representative.

12.1.5 Bulk Storage - Semi-Current Records

As the need for quick access to particular records reduces, it may be more efficient to move the less frequently used material out of the work area and into archive storage.

Semi-current records contain information that is required on an infrequent basis.

An appropriate sensible balance should be achieved between the needs for security and accessibility.

Such records should:

- Not need to be retrieved quickly.
- Be accessible.
- Be stored in a format and state that complies with the Information Security Policy.
- Be stored in a secure records store that:
 - Is kept locked at all times
 - Has access restricted to relevant staff only
 - Is fitted with a suitable fire door
 - Is fitted with a suitable smoke/fire detector
 - Is fitted with window bars where the store is on the ground floor and has windows next to public areas
 - Is safe from any form of environmental damage to the records (e.g damp etc)
- Be compliant with the Record Retention Periods set out in Department of Health guidance 'Records Management: NHS Code of Practice'.
- Be stored in a manner that conforms to Health and Safety Policy.

- Be stored in a manner to prevent deterioration or loss.

12.1.6 Non-Current Records

Storage of non-current records should be in accordance with the requirements set out in section 13.1.5 on semi-current records.

The Department of Health guidance 'Records Management: NHS Code of Practice' takes account of the legal requirements and sets the minimum retention periods for both clinical and non-clinical records and must be followed.

The organisation has local discretion to keep material for longer, subject to local needs, cost, and, where records contain personal information, the requirements of the Data Protection Act 1998.

12.1.7 Off-Site Storage

Records should only ever be taken off site with the appropriate approval and in accordance with the Minimum Information Security Measures and Safe Haven Policy and guidance. These require staff to give the highest priority to the security of these records held off site, especially in the case of confidential records. The Records Manager and/or the Information Governance Team can provide further advice.

Where a number of records need be carried during the day and they cannot practicably and securely remain with the member of staff carrying them then they must be locked out of sight in the boot of the car, during appointments. This method of storage is only to be used for the short term. Records must never be left in the boot of the car for long periods of time or overnight. All records removed from the boot of the car must be carried in a locked container.

If records are to be taken home, the records must be stored securely in accordance with the staff members' Professional Code of Conduct and this policy in conjunction with Minimum Information Security Measures and Safe Haven Policy and guidance. It is essential that any such records are logged out of the department and trackable to enable the organisation to be made aware of the location of the record at all times.

Where records need to be taken home, for example where they are needed for or an early appointment the next day, they must be stored in a manner so that others members of the household or visitors can not view these records i.e. in a lockable container and placed somewhere secure within the home.

Please refer to the Information Security Policy for further guidance on this subject.

12.2 Electronic Records

12.2.1 Using the approved corporate network storage all files should be stored in line with requirements of records structure section above to enable security and ease of:

- Storage and back-up.
- Access control, based on the need to know Caldicott Principle must be documented and kept up to date.

12.2.2 The preferred method of access to electronic information is from the secure network, the organisation will provide authorised encrypted mechanisms to achieve this whilst off site, where required and authorised. However on the few occasions where it is not possible to access information in this way, any information held outside of the secure network must be encrypted and held only on equipment authorised by the organisation. All information must always be returned to the secure network, as soon as possible, to ensure the most up to date information is held on the secure network. When copies of the information have been successfully returned to the secure network, any copies held away for the secure network must be securely removed. (Separate approved contractual arrangements will be made for information processed by third parties)

Where a number of records need be carried, in electronic format on PCT approved equipment, during the day and they cannot practicably and securely remain with the member of staff carrying them then they must be locked out of site in the boot of the car, during appointments. This method of storage is only to be used for the short term. Records and equipment must never be left in the boot of the car for long periods of time or overnight. All records and equipment removed from the boot of the car must be carried in a lockable container.

Where records need to be taken home on PCT approved equipment, for example where they are needed for or an early appointment the next day, the equipment must be stored in a manner so that others members of the household or visitors can not view these records, i.e. in a locked container and placed somewhere secure within in the home.

12.2.3 Technical matters in respect of storage are covered by the organisation's Information Security Policy.

13 Transporting Records

This section covers transport between:

- Organisation's sites
- Organisation's sites and other NHS or Non-NHS sites.
- When visiting patients or others

13.1 Transporting Records

Any transportation of records in whatever media must always have the appropriate authorisations, and must be recorded in the relevant departmental tracking system.

Mailing of Paper Records by Post or Courier

There are various options available if records are to be mailed. The Government has provided minimum security measures for such eventualities which the organisation was required to adopt. These measures are contained in the Minimum Information Security Measures annexed to the Information Security Policy. They detail the appropriate measures to be employed for the sending of person/patient identifiable or corporate information by mail.

13.2 Transporting by hand

When staff are transporting information off site they must obtain the appropriate authorisations and ensure that the Minimum Information Security Measures and Safe Haven Policy and guidance detailed above are adhered to, which includes the requirement to transport sensitive personal information in a suitable lockable container or folder, and in an encrypted format where held electronically. These measures will provide appropriate protection from damage, unauthorised access or theft or loss.

13.3 Handling Records

The following rules must be applied when handling records

- No one should eat, drink or smoke near the records.
- Clinical records being carried on-site, e.g. from the archive storage to the department, etc, should never left unsupervised and should be enclosed in a container e.g. an envelope or covered trolley, to prevent unauthorised access whilst in transit.
- Records should be handled carefully when being loaded, transported or unloaded. Records should never be thrown.
- Records should be packed carefully into vehicles to ensure that they will not be damaged by the movement of the vehicle.
- Records transported in vehicles must be fully enclosed so that they are protected from exposure to the weather, excessive light and other risks such as theft.
- No other materials that could cause risks to records (such as liquids or chemicals) should be transported with records.

Where records or PCT equipment holding records need to be left in a vehicle for a short period of time it must be ensured that they are locked out of sight in the boot of the car. This method of storage is only to be used for the short term. Records must never be left in the boot of the car for long periods of time or overnight. All records removed from the boot of the car must be carried in a lockable container.

13.4 Emailing Records

Transport of electronic documents, including via e-mail must be in accordance with the Minimum Security Measures and Safe Haven Policy and guidance detailed above. Where records are emailed they must be added to the appropriate record to

ensure completeness, once the information is added to the record the email should be deleted.

14 Retention of Records

14.1 General Principles

Records should be kept for only as long as they are required subject to the appraisal process detailed in section 14.3. When various versions of documents are produced prior to agreement of a final version, unless there is a reason to keep these, they should no longer be retained.

Documents should be retained if they contain significant major changes to content, which are recorded in the version history.

Records containing personal information should only be retained as long as the purpose for holding the information applies; see Schedule 1, Part 1, and Principle 5 of the Data Protection Act 1998.

The organisation has adopted the retention periods for health and non-health records as set out in the Records Management: NHS Code of Practice (Department of Health, January 2009) as detailed in Part Two of the Code available from the Information Governance pages (IG Policies & Guidelines) of the organisation's staff website. The retention schedule will be reviewed annually by the Records Manager, and maintained in accordance with the NHS Records Manage Code of Practice. Evidence of this process and communication of relevant up dates will be reported to the Information Governance Steering Group.

14.2 Statutory Requirements

NHS Records Retention and Disposal Schedules are set out in the document **Records Management: NHS Code of Practice Part 2** as follows:

- **Annex D1:** Health Records Retention Schedule.
- **Annex D2:** Business and Corporate (Non-Health) Records Retention Schedule.

Where there are records which have been omitted from the retention schedules, or where new types of record emerge, the Records Manager should be notified.

If necessary, the Records Manager will consult the Department of Health and/or the National Archives for advice and guidance.

All new retention periods agreed will be added to the policy.

14.3 Appraisal of Records for Preservation

Appraisal refers to the process of determining whether the records are worthy of permanent archival preservation. This should be undertaken in consultation with the Records Manager and where appropriate the National Archives or with an approved Place of Deposit. Appraisals should usually take place when records have reached their retention period to determine whether they should be retained for a longer

period because they are worthy of archival preservation or because they are still in use.

The Records Manager and a senior manager with appropriate training and experience who has an understanding of the operational area to which the record relates should undertake and document the appraisal process and any decisions arising from it, including the date the decision was taken, who took the decision and reasons for permanently preserving or destroying the record.

The Records Manager will ensure that storage arrangements for records selected for permanent preservation are made with an approved Place of Deposit.

15 Disposal of Records

The method used to destroy all records must be fully effective and secure their complete illegibility.

Except for early versions of completed documents, a brief description must be kept in the organisation's disposal register of everything that has been destroyed, identifying:

- The document
- When destroyed and by whom.

The Records Manager should be consulted for advice and guidance.

15.1 Disposal of Documents

Following the appraisal process detailed in section 14.3 paper records or documents may be disposed of via shredding, pulping, or incineration this process should be undertaken at least annually. This can be done on site, or via an approved contractor who will provide certificates of destruction. See Minimum Information Security Measures for disposal of information.

All approved Contractors must have a current contract in place containing all relevant Information Governance and clauses, refer to the Information Governance Manager for details.

15.2 Disposal of Records held in Electronic Format

Following the appraisal process detailed in section 14.3 disposal of documents held in electronic format must be completed by a method which ensures that the information cannot be retrieved from the electronic media on which it was held. This can be done on site, or via an approved contractor.

Destruction of files and/or electronic media must be undertaken by the Informatics Department to ensure that all records to be destroyed are done securely.

16 Records Management Systems Audit

- 16.1 The organisation will regularly audit its records management practices for compliance with this framework.

16.2 Audits will:

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

16.3 There are two types of records audit that must be carried out on an annual basis:

16.3.1 Records Management Audit

As part of the Information Governance Assurance Programme and to meet the requirements of the Freedom of Information Act 2000, all NHS organisations are required to regularly audit their Records Management Practices. This is to be carried out at all locations on an annual basis by the Local Records Managers. The Local Records Manager is to use the Records Management Audit tool detailed in Annex F. The completed audit is to be submitted to The Records Manager, who may, supported by the Information Governance Team, if deemed necessary conduct a more detailed audit at any location. Further information regarding this audit is available from the Records Manager.

16.3.2 Information Flows Mapping and Audit

As part of the Information Governance Assurance Programme, all NHS organisations are required to have an up-to-date register of the information they hold and understand how it is handled and transferred to others. The mapping of routine information flows, using the data mapping tool available on the information governance pages on the intranet, will help the organisation identify how and when person identifiable information is transferred into and out of the organisation and form part of the required register. More importantly it will allow the organisation to assess and address risks to ensure that sensitive and or personal information is transferred with appropriate regard to its security and confidentiality, and ensure that staff are provided with clear local procedures that meet organisational and national standards regarding the handling of personal information. Risks identified as part of this process must be added to the appropriate risk register. Directorates must nominate appropriate staff to complete and report on the mapping of information flows. The Information Governance Team will support this work by providing information mapping tools, safe haven material, organisational policies, procedures, guidance, and additional auditing as appropriate. All information mapping reports must be provided to the Information Governance Team within a time frame specified in the audit schedule. An audit schedule will be approved by IGSG and issued by the Information Governance Team any significant risks arising from the results of

reports or audits will be recorded on the departmental risk register and reported to the IGSG which is chaired by the SIRO.

16.3.3 Defensible Documentation (Clinical Record Keeping) Audit

In line with the requirements of the NHS Litigation Authority Risk Management Standards for organisations, all clinical professional groups / services will be required to undertake a yearly record keeping audit regarding the quality of documentation of clinical records. An audit schedule will be issued by the Records Manager.

The results from the audit will be fed back to line managers. It is the responsibility of line managers to ensure that audit takes place on an annual basis and that all action points are implemented in order to improve and maintain performance.

Also see Policy for Clinical Record Keeping Standards

- 16.4 The results of audits will be reported to the Governance Committee via the Information Governance Steering Group.

17 Research Governance

- 17.1 Any research (as opposed to audit) undertaken using patient records must first have formal governance and ethics approval as part of the Research Governance Framework. For advice on who to contact for approval regarding your proposed research project, please contact the organisations Governance team.

18 Security Breaches and Lost Records

- 18.1 Any incident or near miss relating to a breach in the security regarding use, storage, transportation or handling of records must be reported using the organisation's Incident Reporting system.
- 18.2 A serious breach of security (such as a major loss of records – through fire or theft for example), must be reported and managed in accordance with the organisations Serious Untoward Incident Policy. The organisations Caldicott Guardian (in the case of patient information) and Information Governance Manager must be informed. These must be reported to the Board via the IGSG, chaired by the SIRO.
- 18.3 Any suspected thefts must be reported to the Police, by the individual responsible for the records at the time and noted on the organisations Incident Reporting System.
- 18.4 It is the responsibility of the line manager, liaising with and taking advice as necessary from relevant PCT personnel (e.g. the Information Governance Manager, Local Security Management Specialist, Records Management Officer), to investigate such incidents and identify any learning points that must be implemented in order to prevent a recurrence.

19. Training

- 19.1 All staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance.

20 Policy Review & Retention

- 20.1 This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).
- 20.2 This policy will be retained in line with the Records Management: NHS Code of Practice (Department of Health, 2006) retention schedules.

21 Equality & Diversity Statement

- 21.1 The PCT recognises the diversity of the local community and those in its employ. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. The PCT recognises that equality impacts on all aspects of its day to day operations and has produced an Equality and Human Rights Strategy and Equal Opportunities Policy to reflect this. All strategies, policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

22. Disciplinary Statement

- 22.1 Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the PCT's disciplinary procedure.

Annex A Legislation and Professional Guidelines

i. A.1 Record Management: NHS Code of Practice

The code of practice replaces previous guidance as listed below:

- HSC 1999/053 – For the Record.
- HSC 1998/217 – Preservation, Retention and Destruction of GP General Medical Services Records Relating to Patients.
- HSC 1998/153 – Using Electronic Patient Records on Hospitals: Legal Requirements and Good Practice.

The guidelines contained in this Code of Practice draw on advice and published guidance available from the Department of Constitutional Affairs and The National Archives, and also best practices followed by a wide range of organisations in both the public and private sectors. The guidelines provide a framework for consistent and effective records management that is standards based and fully integrated with other key information governance work areas.

ii. A.2 Standards for Better Health

Standards for Better Health were introduced in July 2004, and set out the level of quality that all organisations providing NHS care will be expected to meet or aspire to across the NHS in England.

These standards will require all health care organisations to have a systematic and planned approach to the management of records to ensure that, from the moment a record is created until its final disposal, the organisation maintains information so that it serves the purpose it was collected for and disposes of information appropriately when no longer required.

iii. A.3 The Data Protection Act 1998

Since March 2000 the key legislation governing the protection and use of person identifiable information is the Data Protection Act. The Act does not apply to information relating to the deceased.

The Act gives seven rights to individuals in respect of their own personal data held by others, they are:

- Right to have their information processed fairly and lawfully
- Right of subject access
- Right to prevent processing likely to cause damage or distress
- Right to prevent processing for the purpose of direct marketing
- Rights in relation to automated decision taking
- Right to take action for compensation if the individual suffers damage
- Right to take action to rectify, block, erase or destroy inaccurate data
- Right to make a request to the Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

The Data Protection Act applies to 'personal data', that is, data about identifiable living individuals. Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as the data protection principles, and the other requirements of the Data Protection Act.

iv. A.4 Access to Health Records Act 1990

Data subjects now have access rights to all records irrespective of when they were created, although under section 30, access to some health, education and social work data may be constrained or denied.

The Data Protection Act 1998 supersedes the Access to Health Records Act 1990, apart from the sections dealing with access to information about the deceased. The Access to Health Records Act 1990 provides rights of access to the health records of deceased individuals for their personal representatives and others having a claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law duty of confidence requirements.

v. A.5 The Caldicott Review

In March 1996, guidance on The Protection and Use of Patient Information was published by the Department of Health. This guidance required that when the use of patient information was justified, only the minimum necessary information should be used and it should be anonymised wherever possible. In the light of that requirement the Chief Medical Officer established the Caldicott Committee to review the transfer of all patient-identifiable information from NHS organisations to other NHS or non-NHS bodies for purposes other than direct care, medical research or where there is a statutory requirement, to ensure that current practice complies with the Departmental guidance.

On completion of the work, the committee concluded that, whilst there was no significant evidence of unjustified use of patient-identifiable information, there was a general lack of awareness throughout the NHS of existing guidance on confidentiality and security, increasing the risk of error or misuse.

The Caldicott committee's report, published in December 1997, included 16 recommendations, which related to ensuring best practice in the use of information flows between organisations.

vi. A.6 Freedom of Information Act 2000

The introduction of Freedom of Information Act 2000 highlights the requirement for systematic and sufficient records management. The Act provides individuals rights of access to all recorded information held by public authorities, whether personal or non-personal, unless these are covered by a limited number of exemptions.

The organisation has a duty to ensure that supporting systems and procedures that will ensure compliance with Lord Chancellor's Code of Practice on the Management of Records under section 46 of the Freedom of Information Act 2000 are in place.

The Freedom of Information policy and associated procedures address issues of active records management – creation, keeping, maintenance and disposal – according to the requirements that the law places upon the organisation.

Provides guidance to the NHS and NHS related organisations on patient information and confidentiality issues. The British Medical Association, General Medical Council and Office of the Information Commissioner have endorsed the document. This will help to send a consistent message across the Service on confidentiality and issues around the processing of patient information

Annex B Examples of Records and Media

Examples of types of record and media covered by the policy include:

- Health Records (electronic or paper based).
- Emails
- Letter to and from other health professionals
- Laboratory reports
- Printouts from monitoring equipment
- Tape recordings of telephone conversations
- Administrative records (including e.g. personnel, Incident Report Forms and Risk Assessments, estates, financial and accounting records; notes associated with complaint-handling).
- X-ray and Imaging reports, photographs and other images.
- Microform (i.e. fiche/film).
- Audio and videotapes, cassettes, CD-ROM etc.
- Computer databases, output, and disks etc., and all other electronic records.
- Material intended for short term or transitory use, including notes and 'spare copies' of documents.

This list is not exhaustive.

Annex C References

Connecting for Health Records Management Roadmap *Model Records Management Policy* (document 02A). [Online] [27.08.08]. Available from World Wide Web www.connectingforhealth.nhs.uk/systemsandservices/infogov/records/manpolicy.doc

Department of Health Information Governance Assurance Programme. [Online] [27.08.08]. Available from World Wide Web www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Dearcolleagueletters/DH_084992

Department of Health (2006). *Records Management: NHS Code of Practice: Parts 1 & 2*. [Online] [27.08.08]. Available from World Wide Web www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_4133200

Department of Health (2003). *Confidentiality: NHS Code of Practice*. [Online] [27.08.08]. Available from World Wide Web www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

The Common Law Duty of Confidentiality [Online] [27.08.08]. Reference to available from World Wide Web www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084181

The Data Protection Act (1998). [Online] [27.08.08]. Available from World Wide Web www.opsi.gov.uk/acts/acts1998/19980029.htm

The Freedom of Information Act (2000). [Online] [27.08.08]. Available from World Wide Web www.opsi.gov.uk/acts/acts2000/20000036.htm

The NHS Litigation Authority Risk Management Standards for organisations. [Online] [27.08.08]. Available from World Wide Web www.nhsla.com/RiskManagement/PCTStandards

The Public Records Act (1958). [Online] [27.08.08]. Available from World Wide Web www.opsi.gov.uk/si/si2001/20014058.htm

Annex D Information Flow Data Audit Tool

This tool is available at:

<http://nww.northyorkshireandyork.nhs.uk/Corporate/InformationGovernance/DataAuditTool.htm>

Annex E Types of Records Requiring Registration

The types of records, which are most likely to be placed on a registered file include:

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

This list is not exhaustive.

For further guidance please contact the Records Manager



Records Management Audit Report

Site Name

Site Audited	
Audit Date	
Services Audited	
Site Contacts	
Auditor	
Report Distribution List	

Audit Overview

Brief Description of Audit and what was done etc.

Audit Summary

Non-Conformance details/Observations/Improvement Opportunities (Part 1).

Root cause investigation and proposed Corrective action to eliminate root cause(Part 2)

Additional Comments

Records Inventory

Record Type	Description	Record Owner

Audit Report

1 : Records Inventory			
Objective: The records inventory is accurate, up to date and reviewed annually			
Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1.A Records Inventory Strategy and Procedure has been approved by the IG Steering Group			
2. A Records Inventory has been completed for the whole organisation or is underway using a stepped approach			
3. The inventory differentiates between different records types, e.g. clinical, corporate, HR, estates, financial etc			
4. The inventory differentiates between electronic and paper records			
5. The Records Inventory is reviewed annually and updated			
6. Each location on the inventory is uniquely identified.			
Compliance Testing			
<i>Review a sample of records inventory forms or other source information to check that these have been correctly and accurately entered to the inventory.</i>			

2 : Creation of Records

Objective: Records are created as relevant to the organisations clinical and corporate activities and captured into the appropriate record keeping systems upon creation or receipt

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. There is guidance on what constitutes a record and what should be done to safeguard it and make it accessible via a record keeping system within each department/ Guidance should include: Naming conventions and metadata requirements (i.e. title, subject, name of creator, date created, locality etc.)			
2. There is specific provision within the organisation's guidance for the capture, management and secure storage of electronic information (e.g. e-mails)			
3. The organisation has established a record keeping system (e.g. an electronic record management system) to manage its records			
4. Where a set of records is held in physical form (e.g. paper, microform) the relationships to other physical records, or to electronic records and systems, have been recorded			
5. The record keeping or record management system records the physical location of each record set			
6. Patient Records always include the Patient's NHS number, and this is validated with the Patient when appropriate.			

3: Storage of Records

Objective: All record keeping systems and storage facilities are protected from unauthorised access, destruction or theft or from accidental damage from environmental hazards.

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. Storage areas allocated to hold physical records have adequate space to accommodate anticipated growth.			
2. Storage areas for physical records conform to agreed standards (e.g. BS 5454) to ensure records are safe from environmental or biological hazards, e.g. damp, fire, flood or chemical contamination.			
3. Storage areas for electronic records (including file servers) ensure records are safe from environmental or biological hazards, e.g. damp, fire, flood or chemical contamination.			
4. Electronic records are stored in accordance with British Standards, in particular the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008).			
5. Access to records storage areas is restricted to prevent unauthorised access, damage, theft or other catastrophic loss of records.			
6. The organisation's business continuity and/or disaster management programmes include records maintenance/management			
Compliance Testing			
<i>Review storage arrangements within a specified area/ department / locality and assess whether these comply with the good practice measures outlined above.</i>			

4 : Disposal Of Records

Objective: Records are archived, destroyed or disposed of in accordance with disposal schedules

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. Procedures have been drawn up outlining methods for archiving, disposal and destruction of different record types. E.g. Confidential records are destroyed using methods which provide adequate safeguards against accidental loss, disclosure or re-construction.			
2. The organisation has a board approved records retention and disposal schedule that addresses all records created or held by the organisation. (including electronic and non-paper records)			
3. A register is maintained of all destroyed records and records pending destruction.			
4. Archiving/ disposal and destruction of records is undertaken regularly, e. g. at least annually, and with specific targets and timescales for implementation.			
5. Decisions to retain or destroy records outside of periods specified in approved retention schedules are fully documented.			
6. Formal contractual arrangements that include compliance with information governance requirements, are in place with all off site Archive Companies.			
7. Appropriate processes are in place to record and monitor all records being sent to, received from or destroyed by the off site Archive Company.			
Compliance Testing			
<i>Select a sample of records held at department/ clinic/ locality level and ensure retention is in accordance with the organisations approved retention schedule.</i>			
<i>Review the register of destroyed records and ensure destruction has been undertaken in accordance with procedures and retention schedules.</i>			

5: Security and Confidentiality of Records

Objective: Access to records takes place in a managed manner using prescribed policies and procedures.

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. Breaches of record confidentiality, loss of records etc are recorded as security incidents and managed appropriately			
2. The organisation has board approved policies for: <ul style="list-style-type: none"> • NHS Confidentiality Code of Practice • Data Protection Act • Freedom of Information 			
3. The organisation has an appropriately supported Caldicott Guardian			
4. The organisation has developed, with other agencies. An Information Sharing Protocol to control the transfer and use of confidential records			
5. All staff are aware of their responsibilities regarding confidential records			
6. The organisation ensures that Patients are informed of the proposed use of their records, and permission obtained where that use is not directly for clinical purposes.			
Compliance Testing			
<i>Obtain and review reports of any incidents relating to confidentiality breaches and ensure action has been taken to address issues. (See also tests suggested for checklists 3, 4 & 5.)</i>			

6: Reliability of Records**Objective : Departments have taken measures locally to ensure the reliability of their records**

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. Staff validate information with patients, carers or against other records. (IGT 503)			
2. Spot checks are undertaken locally to confirm that records are an adequate reflection of what has been created or received			
3. Where evidence of non-compliance is identified guidance and training is offered			
4. Local Record Managers have been appointed			

7: Records Management			
Objective: Records management is organised, documented, planned and executed in a strategic and corporate manner			
Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. The organisation has a Records Management Policy approved by the board and this Policy adequately covers the NHS Records Management Code of Practice.			
2. The organisation has access to expertise across the Records Management agenda.			
2. The organisation has a Board approved Records Management Strategy to deliver the policy.			
3. Records Management policies and procedures cover clinical, HR and corporate records.			
4. Records Management policies and procedures cover both electronic and physical records			
5. Records Management policies and procedures are regularly reviewed			
Compliance Testing			
<i>Review policy content for compliance with the NHS Records Management Code of Practice.</i>			

8: Records Management Training

Objective: All staff receive appropriate training in records management

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
1. Records Management training is included in the organisation's Education, Training & Development Plan			
2. Staff understand what they are recording, how it should be recorded and why they are recording it			
3. Staff are trained to validate information with patients, carers or against other records			
4. Staff are trained to identify and correct errors			
5. Staff are advised as to the eventual use of records			
6. There is provision for the regular review of training needs in records and information management			

9: Electronic Records

Objective: Storage media and related technologies and practices for maintaining, storing and transferring electronic records are specified, designed, operated and maintained to prevent unauthorised access, corruption, damage or loss.

Good Practice Measure	Evidence	Compliance 0 (None) – 5 (Full)	Action Required
<p>1a. Documented procedures or instructions are available on the operation and use of electronic records systems</p> <p>1b. Staff are aware of the procedures and trained appropriately</p>			
<p>2. Levels of access available to the electronic system has been documented and approved and only permit staff with the relevant access rights to create new records or edit existing ones.</p>			
<p>3. IT support services have created and maintain system documentation and procedures, such as a system portfolio and change control register. The documentation provides a description of how the system operates including information about the hardware, software and network elements that comprise the electronic system and how they interact. It also records how the system is configured and any changes to the system. E.g. specification of the system, the type of network used, any software patches applied and when these were applied.</p>			
<p>4. Electronic records are retained in accordance with current, approved retention schedules and within appropriate environments.</p>			
<p>5. Storage of electronic records, particularly file servers, back up media etc is secure, appropriate and sufficient.</p>			

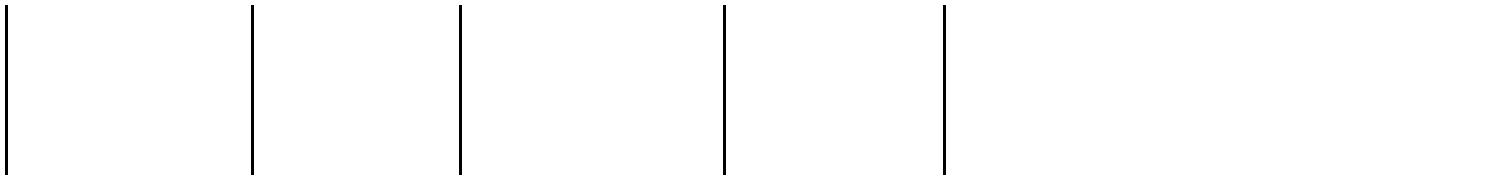
Annex G

Information Asset Register Tool - January 2009

Information Asset name or unique descriptor	Location of the Asset or its components	Information Asset Type	Information Asset Components
	Asset Locations include: Data centre Hospital computer room Hospital Clinic / Ward GP Practice Networked resource Other	Information Asset Types include: Patient Information System Staff Information System Clinical Management System Administration Information System Functional Management Information System Finance Information System Other Information System	Asset Components include: Databases / data files System information and documentation Research information Operations and support procedures Audit data Manuals and training materials Contracts or agreements Business continuity plans Back-up / Archive data Applications / Systems Software / Utilities Development and maintenance tools Hardware Environmental services (power / aircon etc) Other

Information Asset classification	Information Asset Owner	Risk Assessor Name	Risk assessment frequency	Date last risk assessed	Additional comments (may include details of networked resources / servers / drives etc)
NHS Information Asset Classifications:					

NHS CONFIDENTIAL
NHS PROTECT
Other 'local'
Unclassified



Annex H Transporting Records Securely

The Records Management Policy has recently been amended and now requires that information must be carried in a lockable container when being transported away from its place of secure storage.

If you carry person identifiable information or any other sensitive PCT information in order to complete your duties please ask yourself the following questions.

	How do you carry documents and files?	Corrective Action
1.	Already carried in locked case.	None required – continue with current practice
2.	Carried in a case or bag that is not locked	Review the current case used to see if it can be locked through the use of a small combination padlock. (by securing the bag e.g. lock through zip pulls etc)
3.	Do you use lockable cases to carry other equipment etc.	<ul style="list-style-type: none"> • Assess whether the files/documents can be carried in this case, if so please use this case • If the answer is no go to 4
4.	Lockable case is not currently used	Assess the type of case that would be most suitable to your working practices and order at next purchase of new cases or at earliest opportunity to upgrade your

Suitable cases may range from a document brief to a brief case on wheels with a handle dependant on the number and size of files that may need to be carried. The use of lockable containers will be mandatory.