NHS
Ashford and St. Peter's Hospitals
NHS Foundation Trust

Records Management Policy

Author(s): Melanie Grant (Health Records Manager)
Laura Ellis-Philip (Associate Director of Informatics)

Executive Lead: Simon Marshall (Director of Finance & Information)

Status:	Approval Date:	November 2017
	Ratified by:	Information Governance Steering Group (Chair's action)
	Review date:	November 2020

Patients first • Personal responsibility • Passion for excellence • Pride in our team

History

Issue	Date Issued	Brief Summary of Change	Author
1	October 2004	New policy	
2			
3			
4	August 2009	Page 4: Section 4 updated to include electronic records Page 8: Section 13 updated to include training details	Cath Jago (Head of Information Services)
5	December 2010	Page 3: Section 3: Roles and Responsibilities updated to include further roles	Cath Jago (Head of Information Services)
6	November 2014	New Trust policy format Page 4-5: Section 4: Record Creation updated to include Electronic Records and Protective Markings Page 7: Section 5: Record Keeping Standards – updated to reflect audit Page 9: Section 11: Monitoring updated to include aspects of how monitoring carried out Page 7-8: Section 13: Training updated to reflect new training requirements Replacement of embedded documents and Retention Schedules with references and hyperlinks	Melanie Grant (Health Records Manager)
7	November 2017	Page 6: Section3: Roles and Responsibilities – updated to replace Records Management Committee with Information Governance Steering Group Page 14: Section 11 Monitoring - Monitoring of Destruction of Health Records updated to include scanned records. Page 15 : Section 16: Implementation of Policy - updated to reference General Data Protection Regulation (GDPR); References: updated to include the Records Management Code of Practice for Health and Social Care 2016, Independent Inquiry into Child Sexual Abuse and the ASPH Print and Fax Policy Cosmetic changes	Melanie Grant (Health Records Manager)

For more information on the status of this document, please contact:	
Policy Author(s)	Melanie Grant (Health Records Manager) Laura Ellis-Philip (Associate Director of Informatics)
Department	Health Informatics
Date of Issue	November 2014
Review due	November 2020
Ratified by	Information Governance Steering Group (Chair's action)
Audience	All Staff

Executive summary

This policy identifies the actions required to ensure that records of all types (administrative as well as medical, and both paper and electronic) are properly controlled, readily accessible and available for use, and eventually archived or otherwise appropriately disposed of.

For the purposes of this policy, a record is defined as anything which contains information (in any medium) which has been created or gathered as a result of any aspect of the work of NHS employees. The definition covers all clinical and non-clinical records.

Contents

See also: Freedom of Information Policy
Standard Operating Procedures for Health Records
Confidentiality Policy
Information Governance Policy
Information Security Policy
Learning Education & Development Policy

1. INTRODUCTION

All NHS records are public records under the terms of the Public Records Act 1958 which confers a statutory duty on Trusts for their safekeeping and eventual disposal.

The Department of Health Records Management Code of Practice has been replaced by the Information Governance Alliance (IGA) Records Management Code of Practice for Health and Social Care 2016. It performs the same function, that is, a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It clarifies legal obligations that apply to NHS records including responsibilities to ensure compliance with the following acts.

- The Data Protection Act 1998
- The Freedom of Information Act 2000

2. PURPOSE AND SCOPE OF THE POLICY

This policy identifies the actions required to ensure that records of all types (administrative as well as medical) are properly controlled, readily accessible and available for use, and eventually archived or otherwise appropriately disposed of.

For the purposes of this policy, a record is defined as anything which contains information (in any medium) which has been created or gathered as a result of any aspect of the work of NHS employees. The definition covers all clinical and non-clinical records.

3. ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has overall responsibility for records management in the Foundation Trust. The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.

Senior Information Risk Owner (SIRO)

The Trust SIRO (Senior Information Risk Owner) is accountable to the Chief Executive for the management of Information Risks across the Trust. This role is currently carried out by the Director of Finance and Information.

Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility for safeguarding patients' interests regarding the use of patient identifiable information. This role is currently carried out by the Medical Director.

Data Protection Officer

The data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

Board Committees / Groups

The secretaries of the committees / groups should ensure that the agenda and minutes of the meeting are set out in the Trust format. They are responsible for maintaining efficient records systems for work undertaken by the committee / group.

Board Secretary

Responsible for managing the official records of the Trust Board and its archives.

Local Managers

The responsibility for local records management is devolved to the relevant directors, unit managers and department managers for the management of records generated by their activities.

Senior Managers and Departmental Managers

Are responsible for:

- the quality of records management and compliance with Trust policy
- ensuring that policy and procedures are implemented across the Divisions and Departments and that they operate efficiently and effectively
- developing local procedures to support implementation of this policy
- providing appropriate storage space for the storage of departmental records in line with requirements set out in the document 'Records Management: NHS Code of Practice'
- ensuring departmental records are disposed of in accordance with retention schedules in Appendix B of this document
- developing business continuity and disaster recovery processes as appropriate
- as senior individuals involved in running the relevant business areas they are regarded as the Information Asset Owners

Line managers must ensure that staff are adequately trained and that policies and procedures are followed

Every member of staff is responsible for any records / documentation they create and what they do with records / documentation they use.

Project Leads

Frequently projects cross the boundaries of directorates / departments. It is the responsibility of the Project Lead to clarify the arrangements for record keeping.

Associate Director of Informatics/Information Governance Steering Group

The Information Governance Steering Group is responsible for ensuring that:

- a Records Management Policy is implemented
- a Records Management system and processes are developed, co-ordinated and monitored

Health Records Manager

The Health Records Manager is responsible for the overall development and maintenance of health records management practices throughout the Trust, including:

- best practice guidance for health records management
- training
- promoting compliance with policies to ensure the easy, appropriate and timely retrieval of patient information

Corporate Records

The Information Governance Manager is responsible for providing best practice guidance on all records other than health records.

Information Governance Manager

- is responsible for ensuring that storage, processing and use of personal data meet the requirements of the Data Protection Act.

- also responsible for the effective implementation of the Freedom of Information Act.

- ensuring there are trust-wide guidelines for the handling of FOI requests and procedures for the staff responsible for the administration of FOI requests.

- is responsible for providing best practice guidance on all records other than health records.

Information Asset Owners / Information Asset Administrators

See information Security policy.

All Staff

All Trust 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 Trust;
- manage those records;
- comply with the Records Management Policy and guidance
- are mindful of their information governance training and lawfully comply with the Data Protection Act
- comply with all relevant policies as listed at the beginning of this document

4. RECORD CREATION

Each operational unit (eg Finance, Estates, IT, Healthcare) should have a process or Standard Operating Procedure for documenting its activities, taking into account the legislative and regulatory environment in which it operates.

All records should be complete and accurate:

- to allow staff to undertake appropriate actions in the context of their responsibilities
- to facilitate audit
- to protect legal and other rights of the organisation, patients, staff and other people affected
- to show proof of validity and authenticity

Records should have a logical filing structure to enable the quick and efficient filing and retrieval of records when required.

Further detail on record creation for Health Records can be found in the Standard Operating Procedure for Health Records: Medical Records Standard Operating Procedure

Electronic Records

All staff should have access to a departmental file share (e.g. G: drive), this is an area of the network accessible to all members of a department. All records which are to be accessible to other members of a department should be saved on the department's G: drive

Where records are to be shared across departments, a folder should be set up on an inter-departmental drive (e.g. the T: drive at Peter's or U: drive at Ashford) and the records saved there.

The IT Department manages the folders and provides controlled access to them.

Documents that are personal to a user, including Outlook Personal Folders, should be saved to the user's H: drive so that only the user has access to them.

All records should have a logical filing structure and follow these principles

- give a unique name to each record
- give a meaningful name which reflects the records contents
- put elements of the name in a structured and predictable order
- put the most specific information at the beginning of the name
- give a similarly structured and worded name to records which are linked

For example, "Records Management-working group-final report" is more useful than "Final report of the working group on Records Management".

Referencing

Each operational unit should use a referencing system that meets its business needs and can easily be understood by staff members who create records for example, the abbreviation "HR" for Human Resources.

Protective Markings

All records regardless of media may be classified to reflect their status. They should be appropriately marked into different categories such as:

- NHS confidential
- NHS Protect

This enables the record to be handled appropriately at all the stages of its lifecycle.

Version Control

Version control is a process which leaves a clear audit trail of change to the record. Version control is important for electronic records as they can easily be changed.

The original should be numbered as 1.0 and subsequent versions should be numbered consecutively.

This information should be recorded on the front cover and in the footer bar.

5. RECORD KEEPING STANDARDS

Record keeping is a tool of professional practice and one which should help the care process. It is not separate from the process and it is not an optional extra to be fitted in. Professional organisations all have standards for record keeping which covers all formats (e.g. paper, electronic format).

Generic medical record keeping standards define good practice for medical records and address the broad requirements that apply to all clinical note keeping. These standards were developed by the health Informatics Unit of the Royal College of Physicians following review of published standards and wide consultation. They were first published in 2007 in Clinical Medicine.

Purpose of the Standards:

- to maximise patient safety and quality of care
- to support professional best practice
- to assist compliance with Information Governance and NHS Litigation Authority Standards and Maternity CNST Standards.

There are 12 Record Keeping Standards and they are attached in Appendix A. As the Trust aims for good, high quality written records and entries, it has adopted additional standards to which users should adhere:
All entries are:

- full, factual, consistent, contemporaneous, accurate and legible
- when written, they are in black pen (not ink, as ink will run if it comes into contact with a liquid) and on white paper, (although other coloured pens and paper can be used providing the combination of pen and paper produces a legible and permanent record)
- when written, they are written clearly and in such a way that the text cannot be erased
- when they contain a signature, it is accompanied by a printed name
- any alterations or additions are dated, timed and countersigned in such a way that the original entry can still be read clearly – correction fluid is not permitted and errors are to be scored through with a single line and signed free from abbreviations (unless officially accepted and in accordance with an authorised Trust/local list)
- free from jargon, meaningless phrases, irrelevant speculation, judgemental, offensive, subjective or unprofessional statements or language
- entries by unqualified staff are countersigned by a registered professional;
- photocopies should be clearly legible

- documentation and charts used in patient care are labelled on every page with the patient identification
- registered professionals should be aware that in accordance with the Data Protection Act 1998, patients are normally entitled to access their records. Access is available from the Trusts' Subject Access Team which complies with the Data Protection Act 1998, as shown in the Subject Access process. This process is captured in the Trust's Standard Operating Procedure for Health Records.

6. RECORD STORAGE

On-site Storage

All records will be kept in a secure storage area for which access restrictions will apply as appropriate. These storage areas can be electronic or physical.

Where there is a tracking system in use, all records should be tracked to their location and stored in a secure way.

All records will be filed in a way that facilitates their location and retrieval.

Wherever possible central storage should be established.

Off-site Storage

When records are no longer required for operational purposes, they may be sent to a secure off-site storage facility, under contractual arrangements that must comply with relevant legislation and guidance.

The criteria for deciding when a record should be sent off-site will take into account amongst other things the last time the record was required for operational purposes, on-site storage availability, and the likelihood of the record being required for operational purposes again.

Requests for the return of records will be controlled by an appropriate Trust manager, e.g. the Health Records Manager.

7. RECORD RETRIEVAL MOVEMENT & TRACKING

Requests for the provision of records (both routine and urgent) should be directed to the appropriate managers who are responsible for their storage.
The process for the retrieval of Health Records is shown in the Standard Operating Procedure for Health Records:
Medical Records Standard Operating Procedure

The physical movement of records within the buildings of the Trust will be undertaken in a safe and secure way.

The routine transport of records between the Trust locations and to other local hospitals will be via the internal transport system.

Arrangements for the urgent transport of records between Trust locations and the routine transport of records to other destinations not covered by the Trust's transport service will be left to the discretion of the local manager who will be responsible for their safe delivery and receipt.

Records must not be left in a car, other vehicle or left unattended whilst off-site.

Records may not be taken home or to the residencies under any circumstances.

Where records/documents (including x-rays) are requested by another organisation, a copy of the originals is sent and the originals retained at the Trust. The copy must be clearly marked as "copy".

Original records should not be removed off site apart from in the most exceptional circumstances when transported between Trust sites in the personal custody of a consultant or senior manager, and this movement tracked accordingly.

When the electronic scanning of patient records was introduced in 2016, a contract was established to transport original records between the Trust and the offsite scanning bureau. This contract is compliant with industry standards for an off-site scanning service

Transport of records to and from off-site storage facilities will be covered under the contractual arrangements with the provider.

All records will be tracked on a tracking system showing their current location in order to ensure that these records are obtainable at all times thereby ensuring patient care is not affected. The system used for Health Records is the Patient Administration System (PAS/ Patient Centre). Users are trained in the systems used to do this.

The Standard Operating Procedure for Health Records explains procedures used within the department.
Medical Records Standard Operating Procedure

Training materials for case note tracking are available from the IT Training Department in the Minerva Centre.

8. RETENTION AND DESTRUCTION OF RECORDS

The retention period depends upon the type of record and its importance to the Trust. The DoH provides guidance in the IGA Records Management Code of Practice for Health and Social Care 2016 which sets out the minimum retention period for both clinical and administrative records. See Appendices for further guidance.

The decision to dispose of records either Paper or Electronic will be taken by a relevant Trust senior manager (e.g. clinical records by the Health Records Manager, administrative records by the Head of Department) only after the minimum retention period has been exceeded.

Where there is any reason to believe or suspect that a complaint may be received or legal action may be initiated relating to a period or episode covered by the record, then the entire record(s) should be retained even after the minimum retention period. If necessary, the advice of the Trust's legal services manager should be sought.

A detailed process of disposal and destruction of records can be found in the Standard Operating Procedure for Health Records.
Medical Records Standard Operating Procedure

Options for the disposal of paper records include:

- digitizing for electronic storage
- depositing with a Public Records body
- transferring to a bona-fide research body recognised by the Local Research Ethics Committee
- destruction

It is the responsibility of the Trust to satisfy itself that records are destroyed in a way that safeguards against accidental loss or disclosure of contents.
This will normally involve an approved contractor shredding, pulping or incinerating records, and providing written certification as proof of destruction.

9. CONFIDENTIALITY AND SECURITY OF RECORDS

The storage, distribution, use and disposal of records will comply with relevant legislation (eg Data Protection Act 1998, Human Rights Act 1998), guidance (eg Caldicott, BS7799), local policies (eg the Trust Confidentiality Policy) and take account of best practice.
Legal Admissibility: BS 10008:2008

To prevent unauthorised access, best practice is to follow a clear desk policy.

To prevent unauthorised access to electronic records, electronic devices must be locked when unattended.

Appropriate physical security measures will be in place to control access to work areas where records are stored or used.

A written procedure to locate or replace missing records will be followed.

Where a record cannot be found, it should be reported on an incident report form and forwarded to the Risk Manager and Directorate/Department Manager.

A periodic sample audit of patient case note files (looking at amongst other things condition, content and location) will be undertaken by relevant managers with results reported to the Information Governance Steering Group.

10. ACCESS TO RECORDS

Under the Data Protection Act 1998, the right of “subject access” allows an individual to gain access to personal data held about them. Typically, this will involve supplying an individual with access to or a copy of their record when asked to do so. The Access to Health Records Act 1990 applies to requests for access or a copy of records of deceased patients by their personal representatives.

Although it is good practice to share the contents of a record with the data subject as personal data is being recorded, the individual can apply for access to that record at any time.

Formal requests for access should be made in writing to the Trust’s, Subject Access Team. A fee may be payable. Access to a personal record will be facilitated within 21 or 40 days as appropriate.

Personal data contained within a record may be shared with other people, subject to that conforming to the second principle of the Data Protection Act 1998, which requires the disclosure to be compatible with the express purpose for which that data was obtained.

The Freedom of Information Act 2000 gives a general right of access from 1 January 2005 to recorded information held by public authorities, subject to certain conditions and exemptions.

In accordance with section 8 of the Freedom of Information Act, a request for information under the general rights of access must be received in writing, stating the name of the applicant and an address for correspondence, and describes the information requested. For the purpose of general rights of access, a request is to be treated as made in writing if it is transmitted by electronic means, is received in legible form and is capable of being used for subsequent reference.

The Trust will establish systems and procedures to ensure that the organisation complies with the duty to confirm or deny and to provide the information requested within 20 working days of a request in accordance with section 10 of the Freedom of Information Act and guidance received.

11. MONITORING

This policy will be monitored in various ways as explained below:

Clinical Audit of Medical Records

The Clinical Effectiveness and Audit Lead will ensure a clinical audit of record-keeping standards is undertaken at least annually across clinical specialties, with results discussed within clinical areas and action plans developed which include:

- the planned improvement
- the person responsible
- the timescale (within a 3 month period)
- the outcome

Areas will provide reports to the Quality Department for discussion at the Trust Clinical Effectiveness & Audit Group (CEAG) meetings. CEAG will monitor progress and confirm completion of actions; CEAG will inform the Trust's Clinical Governance Committee (CGC) about areas where there are issues and there is a need for re-audit within a 6 month period. Both CEAG and CGC act as fora for discussion and sharing of lessons learnt.

CEAG reports to CGC and CGC reports to the Integrated Governance Assurance Committee (IGAC) which reports to Trust Board.

The Clinical Effectiveness and Audit Lead provides support and guidance to areas undertaking the audits to enable areas to follow the standard methodology and use the Trust's standard clinical audit tools. The Clinical Effectiveness and Audit Lead produces an annual report on trust-wide audits to CEAG and CGC.

Copies of the Trust's standard clinical audit tools based on RCP generic record-keeping standards (Appendix A) and tools based on the Trust's Consent Policy are available from the Quality Department.

Monitoring of Health Records

Performance Indicators for health records are a standard agenda item for the Information Governance Steering Group. The Performance Indicators include:

1. failed ingestions (the number of documents which fail ingestion into Evolve-monitored daily)
2. pre-scan rejects (the number of documents returned to the originator by Medical Records – monitored daily)
3. exported documents (the department and reason for exporting – monitored weekly by the System Administrator)
4. other monitoring (for example, users creating summary notes are reported quarterly; users accessing the Safeguarding tab ad hoc; users accessing Restricted Patients ad hoc)
5. R and D audits - as and when required, the R and D department requests a report to check that auditors have accessed only the patient notes of the patients requested)
6. other departmental audits – as and when requested (no depts. are doing this ….)
7. individual investigations as and when required
8. number of Datix incidents related to health records

Monitoring of Destruction of Health Records

Each year, the Health Records department carries out destruction of records in accordance with the retention timescales stated in this policy. Destruction lists are completed for each record destroyed stating the patient hospital number, name and signature of the individual identifiying records for disposal. A Destruction certificate is issued to the Portering Manager for all records destroyed by the contracted 3rd party company.

A template of the Destruction list to be used can be found in the Standard Operating Procedure for Health Records.

For Health Records that are scanned by Hugh Symons and stored electronically, the paper record is destroyed after one month. A spreadsheet listing the records to be destroyed is emailed to the Health Records Manager who gives the order to destroy. A Destruction certificate is then issued.

A copy of the Destruction certificate can be found in the Standard Operating Procedures for Health Records as Appendix 10 under (DSSD) Detailed Scanning Service Description, Appendix 15.
Medical Records Standard Operating Procedure

Information Governance Steering Group

Freedom of Information Requests and Subject Access Requests are monitored monthly by the Information Governance Manager and reported quarterly to the Information Governance Steering Group.

Annual training in Information Governance is mandatory across the Trust and further information on this is contained in the Training section below.

The Information Governance Steering Group reports on the Information Governance Toolkit annually to the Trust Executive Committee and to Trust Board.

An annual audit of corporate records will be carried out by a nominated individual for each department and feedback will be given to the Information Governance Manager. The results will be reviewed by the Information Governance Steering Group.

12. EQUALITY IMPACT ASSESSMENT

See Appendix G

13. TRAINING

All staff are required to complete annual mandatory Information Governance training. Various forms of mandatory training are provided to ensure that staff are compliant e.g. Induction, Classroom training, and online, the Data Security Awareness Training Tool which includes Information Governance, Records Management and Clear Desk guidance.
This is reflected in the Trust's Education Policy and Training Needs Analysis.

Further information on training procedures for Health Records are included in the Standard Operating Procedure for Health Records.
Medical Records Standard Operating Procedure

All new staff are provided with an induction session which refers to records management and instructions on how to complete the online training.

Additional training will be received via local induction and will be dependent on job roles.

Job-specific training is available by contacting the IT Training team at The Minerva Centre on ext 2938 or emailing asp-tr.it.training@nhs.net.
The IT Department also provides a leaflet called 'Guide to IT' and a booklet called 'Guide to IT at Ashford and St Peter's Hospitals NHS Trust.'

14. REVIEW

The Records Management policy will be reviewed every 3 years in line with Trust policy or updated in line with any new legislation issued or change in procedures.

15. ARCHIVING OF POLICY

All archived copies of this policy are retained by the Quality Department within the Trust. Copies can be requested through this department.

16. IMPLEMENTATION OF POLICY

Implementation of this policy will be carried out by the policy being advertised on the Aspire Bulletin and published on TrustNet.

The General Data Protection Regulation (GDPR) comes into effect in May 2018 and the Trust has already begun preparation to ensure that it is compliant with this new statutory regulation.

REFERENCES

Nursing and Midwifery Council Standards for Records and Record Keeping 1998
General Medical Council Good Medical Practice 1998

Health Quality Service Accreditation Programme
Department of Health Records Management: NHS Code of Practice – Part 1
Department of Health Records Management: NHS Code of Practice (Part 2 – 2nd Edition)
Information Governance Alliance: Code of Practice for Health and Social Care 2016
Connecting for Health Information Governance Toolkit
Standards for Practice and Care
Independent Inquiry into Child Sexual Abuse (www.iicsa.org.uk)
ASPH Print and Fax Policy

APPENDIX A: RCP APPROVED ‘GENERIC MEDICAL RECORD KEEPING STANDARDS’

Prepared by the Health Informatics Unit of the Royal College of Physicians

Generic medical record keeping standards define good practice for medical records and address the broad requirements that apply to all clinical note keeping. These standards were developed by the Health Informatics Unit of the Royal College of Physicians following review of published standards and wide consultation. They were first published in 2007 in Clinical Medicine.

Standard	Description
1	The patient's complete medical record should be available at all times during their stay in hospital
2	Every page in the medical record should include the patient's name, identification number (NHS Number) (1) and location in the hospital
3	The contents of the medical record should have a standardised structure and layout
4	Documentation within the medical record should reflect the continuum of patient care and should be viewable in chronological order
5	Data recorded or communicated on admission, handover and discharge should be recorded using a standardised proforma (2)
6	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
7	Entries to the medical record 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
8	Every entry in medical record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made
9	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
10	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 (3)
11	The discharge record/discharge summary should be commenced at the time a patient is admitted to hospital
12	Advanced Decisions to Refuse Treatment, Consent, Cardio-Pulmonary Resuscitation decisions must be clearly recorded in the medical record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney
Notes:	
1	*The NHS number is being introduced as the required patient identifier.*
2	*This standard is not intended to mean that handover proforma should be used for every handover of every patient rather that any patient handover information should have a standardised structure.*
3	*The maximum interval between entries in the record would in normal circumstances be one (1) day or less. The maximum interval that would cover a bank holiday weekend, however, should be four (4) days.*

APPENDIX B: HEALTH RECORDS RETENTION SCHEDULE

Organisations should remember that records containing personal information are subject to the Data Protection Act 1998.

Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years. Where a retention period longer than 30 years is required (e.g. to be preserved for historical purposes), or for any pre-1948 records, the National Archives should be consulted.

The Minimum Retention Period for all records is contained in the Information Governance Alliance: Code of Practice for Health and Social Care 2016; the Minimum Retention Period for the principal type of health records is:

- Adult health records not covered by any other specific guidance should be retained from date of discharge, or patient last seen, for 8 years after which they should be reviewed and if no longer needed, destroyed
- Children's records including midwifery, health visiting and school nursing should be retained from date of discharge, or patient last seen, until 25th birthday or if the patient was 17 at the conclusion of the treatment, until their 26th birthday, after which they should be reviewed and if no longer needed, destroyed retain

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound, and including all records of NHS patients treated on behalf of the NHS in the private healthcare sector): patient health records (electronic or paper-based, and concerning all¡ specialties, including GP medical records);

- records of private patients seen on NHS premises;
- Accident & Emergency, birth and all other registers;
- theatre, minor operations and other related registers;
- X-ray and imaging reports, output and images;
- photographs, slides and other images;
- microform (i.e. microfiche/microfilm); audio and video tapes, cassettes, CD-ROMs, etc;
- e-mails;
- computerised records; and
- scanned documents.
- If viewed in electronic format, the search facility in Word or PDF can be used to search for particular record types.

Notes

The coding below denotes the status of the type of record and its retention period:

C = a previously existing record type (ie referenced in the previous retention schedule dated March 2006) but a Change to the retention period

N =a New record type (either not referenced in the previous retention schedule or a more explicit description of a record type than previously published)

S = a previously existing record type, with the Same retention period.

Retention Schedules

An organisation with an existing relationship with an approved Place of Deposit should consult the Place of Deposit in the first instance. Where there is no pre-existing relationship with a Place of Deposit, organisations should consult The National Archives.

APPENDIX C: PRINCIPLES TO BE USED IN DETERMINING POLICY REGARDING THE RETENTION AND STORAGE OF ESSENTIAL MATERNITY RECORDS

British Paediatric Association
Royal College of Midwives
Royal College of Obstetricians and Gynaecologists
Nursing and Midwifery Council for Nursing and Midwifery.

Joint Position on the Retention of Maternity Records

1. All essential maternity records should be retained. 'Essential' maternity records mean those records relating to the care of a mother and baby during pregnancy, labour and the puerperium.

2. Records that should be retained are those which will, or may, be necessary for further professional use. 'Professional use' means necessary to the care to be given to the woman during her reproductive life, and/or her baby, or necessary for any investigation that may ensue under the Congenital Disabilities (Civil Liabilities) Act 1976, or any other litigation related to the care of the woman and/or her baby.

3. Local level decision making with administrators on behalf of the health authority must include proper professional representation when agreeing policy about essential maternity records. 'Proper professional' in this context should mean a senior medical practitioner(s) concerned in the direct clinical provision of maternity and neonatal services and a senior practising midwife.

4. Local policy should clearly specify particular records to be retained and include detail regarding transfer of records, and needs for the final collation of the records for storage. For example, the necessity for inclusion of community midwifery records.

5. Policy should also determine details of the mechanisms for return and collation for storage, of those records which are held by mothers themselves, during pregnancy and the puerperium.

List of Maternity Records to be Retained

Maternity Records retained should include the following:

i. documents recording booking data and pre-pregnancy records where appropriate;

ii. documentation recording subsequent antenatal visits and examinations;

iii. antenatal in-patient records;

iv. clinical test results including ultrasonic scans, alpha-feto protein and chorionic villus sampling;

v. blood test reports;

vi. all intrapartum records to include, initial assessment, partograph and associated records including cardiotocographs;

vii. drug prescription and administration records;

viii. postnatal records including documents relating to the care of mother and baby, in both the hospital and community settings.

Notes

The introduction of BadgerNet in November 2017, provided the Trust with electronic recording of patient information and gives women electronic access to their pregnancy notes, which improves the Trust's ability to comply with these principles of retaining and storing maternity records.

APPENDIX D: BUSINESS AND CORPORATE (NON-HEALTH) RECORDS RETENTION SCHEDULE

Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years. Where a retention period longer than 30 years is required (e.g. to be preserved for historical purposes), or for any pre-1948 records, the National Archives should be consulted.

The Minimum Retention Period for all records is contained in the Information Governance Alliance: Code of Practice for Health and Social Care 2016.

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

- administrative records (including personnel, estates, financial and accounting
- records, and notes associated with complaint handling);
- photographs, slides and other images (non-clinical);
- microform (ie microfiche/microfilm);
- audio and video tapes, cassettes, CD-ROMs, etc;
- e-mails;
- computerised records; and
- scanned documents

The schedule is split into the following types of records:

Administrative (corporate and organisation)
Biomedical Engineering
Estates/Engineering
Financial
IM & T
Other
Personnel/Human resources
Purchasing/Supplies

If viewed in electronic format, the search facility in Word or PDF can be used to search for particular record types.

Notes

An organisation with an existing relationship with an approved Place of Deposit should consult the Place of Deposit in the first instance. Where there is no pre-existing relationship with a Place of Deposit, organisations should consult The National Archives.

APPENDIX E: ELECTRONIC RECORD/ AUDIT TRAILS

1. Electronic records are supported by audit trails, which record details of all additions, changes, deletions and viewings. Typically, the audit trail will include information on:

    - who - identification of the person creating, changing or viewing the record;
    - what - details of the data entry or what was viewed;
    - when - date and time of the data entry or viewing; and
    - where - the location where the data entry or viewing occurred.

2. Audit trails are important for medico-legal purposes as they enable the reconstruction of records at a point in time. Without its associated audit trail, there is no reliable way of confirming that an entry is a true record of an event or intervention.

3. Guidance on the retention of Non-Clinical Quality Assurance Records is contained in the Information Governance Alliance: Code of Practice for Health and Social Care 2016:

    > “Non Clinical Quality Assurance Records should be retained from the end of the year to which the assurance relates for a period of 12 years at the end of which, they are to be reviewed and if no longer needed, to be destroyed”.

4. There is also guidance on records managed within an Electronic Patient Records System (EPR), although the IGA is undertaking further work to refine the rules for record retention and to specify requirements for EPR systems:

    > “Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the Code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed.
    >
    > If the system does not have this capacity, then once the records have reached the end of their retention periods they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule”.

APPENDIX F: APPROVED PLACES OF DEPOSIT

'Where an NHS Trust has previously deposited records with a given place of deposit listed here, it should continue to /liaise with the same institution unless it receives guidance from The National Archives (TNA) to the contrary. If a Trust is not aware of any previous transfers, or as a result of re-organisation has previously transferred records to more than one place of deposit, it should contact National Advisory Services at TNA (nas@nationalarchives.gov.uk, tel 020 8392 5330 x2620), who will be able to advise which place of deposit should be contacted regarding further transfers. National Advisory Services will also be happy to advise on any other queries regarding the working of the Public Records Act in respect of NHS records".

A list of all the current appointed Places of Deposit is available on The National Archives website:
http://www.nationalarchives.gov.uk/documents/archives/10.12.2015_Approved_repositories_and_places_of_deposit.pdf

The current contact details of these institutions are given at:
http://discovery.nationalarchives.gov.uk/find-an-archive

APPENDIX G: EQUALITY IMPACT ASSESSMENT SUMMARY

ASHFORD & ST. PETER'S HOSPITAL NHS FOUNDATION Trust

Name: Melanie Grant (Health Records Manager)

Policy/Service: Records Management Policy

Background

- Description of the aims of the policy
- Context in which the policy operates
- Who was involved in the Equality Impact Assessment

All NHS records are public records under the terms of the Public Records Act 1958 which confers a statutory duty on Trusts for their safekeeping and eventual disposal.

The Department of Health Records Management: Code of Practice is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It clarifies legal obligations that apply to NHS records including responsibilities to ensure compliance with the following acts.

- The Data Protection Act 1998
- The Freedom of Information Act 2000

The guidance provided in this policy is to assist all staff members in ensuring that correct procedures are followed in relation to the records management for both Medical and Corporate records

Methodology

- A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age)
- The data sources and any other information used
- The consultation that was carried out (who, why and how?)

Data sources come directly from the legislation and guidance offered by the National Archives who oversee Records Management.

This is reviewed in line with current Trust processes by the Health Records Group

Key Findings

- Describe the results of the assessment
- Identify if there is adverse or a potentially adverse impacts for any equalities groups

No adverse or potentially adverse impacts have been assessed for any equalities groups. The policy equally effects all from any equalities group.

Conclusion

- Provide a summary of the overall conclusions

The policy reflects statutory legislation and national guidance from the National Archives and details the Trust’s operating procedures around Records Management including Creating, Retrieval, Tracking and destruction
Recommendations • State recommended changes to the proposed policy as a result of the impact assessment • Where it has not been possible to amend the policy, provide the detail of any actions that have been identified • Describe the plans for reviewing the assessment
No changes recommended

Guidance on Equalities Groups

Race and Ethnic origin (includes gypsies and travellers) (consider communication, access to information on services and employment, and ease of access to services and employment)	**Religion or belief** (include dress, individual care needs, family relationships, dietary requirements and spiritual needs for consideration)
Disability (consider communication issues, access to employment and services, whether individual care needs are being met and whether the policy promotes the involvement of disabled people)	**Sexual orientation including lesbian, gay and bisexual people** (consider whether the policy/service promotes a culture of openness and takes account of individual needs
Gender (consider care needs and employment issues, identify and remove or justify terms which are gender specific)	**Age** (consider any barriers to accessing services or employment, identify and remove or justify terms which could be ageist, for example, using titles of senior or junior)
Culture (consider dietary requirements, family relationships and individual care needs)	**Social class** (consider ability to access services and information, for example, is information provided in plain English?)