Livewell Southwest

Health & Corporate Records Policy

Version No.1

Notice to staff using a paper copy of this guidance

The policies and procedures page of Intranet holds the most recent version of this guidance. Staff must ensure they are using the most recent guidance.

Author:	**Information Governance Lead & Records Manager**
Asset Number:	**670**

Reader Information

Title	Health & Corporate Records Policy.v.1
Asset number	670
Rights of access	Public
Type paper	Policy
Category	Clinical and Corporate
Document purpose/summary	This policy is to advise staff of Livewell Southwest (LSW) decision to adopt the Department of Health's Records Management, NHS Code of Practice and outlines the requirements to maintain standards. This policy identifies the standards expected of all registered and non-registered staff within LSW It sets a minimum standard, which will be applicable to all patient care settings, including community clinics, inpatient units, the residence of the patient and occasions when LSW staff are required to write in records of other providers of care
Author	Records Manager & CPA Lead.
Ratification date and group	24th February 2016. Policy Ratification Group.
Publication date	2nd March 2016
Review date and frequency (one, two or three years based on risk assessment)	Three years after publication, or earlier if minor changes are required.
Disposal date	The Records Manager will retain a copy for the archive in accordance with the Retention and Disposal Schedule, all copies must be destroyed when replaced by a new version or has been withdrawn from circulation
Job title	Records Manager
Target audience	All Staff and interested members of the public
Circulation	Electronic: LSW intranet and website (if applicable) Written: Upon request to the PRG Secretary on ☏ 01752 435104. Please contact the author if you require this document in an alternative format
Consultation process	Information Governance Group (IGG), Care Programme Approach Group (CPA), General Health Records Group, SystmOne Clinical Leads and Locality Managers
Equality analysis checklist completed	
References/Sources of information	The Department of Health, Records Management: NHS Code of Practice including revised part 2 2009 Information Governance Toolkit Acts of Parliament and their guidance as stated in documentCare Quality Commission (CQC) (2009) The right information, in the right place, at the right time; A study of how healthcare organisations manage personal data
Associated	N/A

documentation	
Supersedes document	Record Management Policy and Adoption Statement v1:2
Author contact details	By post: Local Care Centre Mount Gould Hospital, 200 Mount Gould Road, Plymouth, Devon, PL4 7PY. Tel: 0845 155 8085, Fax:01752 272522 (LCC Reception)

Document review history

Version Number	Type of change	Date	Originator of change	Description of change
0.1	Full review and amalgamation	1/10/14	Records Manager & CPA Lead	Complete rewrite and amalgamation of the following policies: Clinical Note Keeping V6 Records Management & Adoption Statement V1.6
0.2	Review	Dec 2015	Internal Audit	End-user updates and amendments
1	Ratified	February 2016	Information Governance and CPA Lead	Ratified minor amendments

Health & Corporate Records Policy

1 Introduction

1.1 Records management is the process by which Livewell Southwest (LSW) manages the records it holds whether internally or externally generated and in any format of media type; from their creation, through their lifecycle to their eventual disposal or permanent archiving.

1.2 Record keeping is an integral part of clinical care. It is a significant tool of professional practice and supports the delivery of care in an integrated setting. It is not an optional extra to be fitted in if circumstances allow. The quality of record keeping is a reflection of the standard of professional practice, whether the records are paper based or electronic. A good standard of record keeping is the mark of skilled and safe practitioner.

1.3 This policy identifies the standards expected of all registered and non-registered staff within LSW. It sets a minimum standard, which will be applicable to all patient care settings, including community clinics, inpatient units, the residence of the patient and occasions when LSW staff are required to write in records of other providers of care.

1.4 There is no best single model for a record. However the Health & Corporate Records Policy offers overarching guidance based on the Records Management: NHS Code of Practice to ensure the required standards of practice in the management of records within LSW are followed. It is based on current legal requirements and professional best practice.

1.5 LSW's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations.

1.6 Records support policy formation and managerial decision making, protect the rights of service users, staff and members of the public and the interests of LSW. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.7 Effective clinical record keeping is an integral part of professional practice and is essential to provide good communication between healthcare professionals and ensure services are delivered safely. All LSW staff have a duty to keep accurate records and protect the confidentiality of service users personal identifiable information.

1.8 Effective management of corporate and clinical records support better use of staff time, improved control of valuable information resources, compliance with legislation and standards.

1.9 Record Keeping improves internal management processes by ensuring information is available when required.

1.10 This document sets out a framework within which the staff responsible for creating, retaining, tracking, retrieving, archiving, disposing and destroying corporate and healthcare records can ensure the records are managed and controlled effectively in line with legal, operational and information governance requirements.

2 Purpose

2.1 To ensure that the clinical records made by staff are fit for purpose and of a quality that provide for objective, accurate, current and comprehensive information that supports and enables the best possible clinical care and treatment for the patient/client.

2.2 To ensure that records are managed legally from their creation, through their lifecycle to their eventual disposal.

2.3 The aims of this policy are to ensure that:

- Records are available when needed.
- Records can be accessed.
- Records are accurate.
- Records can be preserved and remain accessible over time in spite of changes and held in a format which remains readable for as long as records are required.
- Records are tracked and disposed of appropriately.
- Staff are trained and understand their responsibilities for record-keeping and record management whether the record is related to healthcare delivery or corporate business.

3 Scope

3.1 This policy relates to the management of corporate and health records held in any format by LSW.

3.2 It applies to all staff employed or contracted by LSW, including third parties who are required as part of their role to manage or access corporate or health records.

4 Definitions

4.1 Records are defined as recorded information in any form created or received and maintained by LSW in the transaction of its business or conduct of affairs and kept as evidence of such activity.

These include:

4.1.1 **Corporate Records:** In the context of this policy this includes all administrative records (i.e. personnel, estates, financial, contracts, tenders and accounting records litigation and records associated with complaints, Health & Safety, Infection Control etc.) policies procedures, clinical guidelines, protocols, standard operating procedures regardless of format.

4.1.2 **Health Records:** In the context of this policy consists of any information in relation to the physical or mental health condition of the individual made by or on behalf of a health professional in connection with the care of that individual (Data Protection Act 1998).

This includes patient held records and those in electronic formats, including x-ray and imaging reports, diagnostic testing or screening results etc.

In addition this may include photographs, slides and other images, audio and video cassettes, CD –ROM, emails text messages, etc., where these are related to patients care.

4.1.3 **Records Management**: Is the systems and processes used to direct and control the creation, version control, distribution, filing, retention, storage, archiving and disposal of records legally.

4.1.4 **Record keeping**: Is an integral part of clinical care. It is a significant tool of professional practice and supports the delivery of care in an integrated way.

4.1.5 **Records Life Cycle**: From creation/receipt of a record through its active use, to confidential disposal or archiving.

4.1.6 **Information**: LSW's records are important sources of administrative, evidential and historical information. They are its corporate memory providing evidence of actions and decisions and representing a vital asset to support delivery of care and business functions. Information enables LSW to meet its legal requirements to patients to hold their clinical information safe and secure. It enables LSW to meet its legal obligations to other stakeholders (i.e. under the Freedom of Information Act) and to ensure appropriate access to information for the purpose of accountability, openness and transparency.

5 Duties Roles & Responsibilities

5.1 Chief Executive

5.1.1 The Chief Executive has overall responsibility for the records management in LSW.

5.1.2 As Accountable Officer they are responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity.

5.1.3 This includes a records management system to ensure appropriate accurate information is available as required.

5.2 Caldicott Guardian

5.2.1 The Caldicott Guardian is responsible for ensuring appropriate use of patient identifiable information and access to health records.

5.2.2 They ensure that information is kept secure, only shared where it is appropriate to do so and that the process in place meets legal requirements.

5.2.3 They provide advice as necessary to clinical staff and others in the event of requests to share information and monitor such requests.

5.3 Senior Information Risk Owner (SIRO)

5.3.1 The SIRO for LSW ensures record management procedures are in place and are lawful as part of their responsibility for information governance.

5.3.2 They ensure that risks associated with corporate and health records regardless of format are effectively managed and mitigated and escalated as appropriate.

5.4 Records Manager

5.4.1 The Records Manager is responsible for the management of the archive of LSW records, storage and retrieval or specific records and is considered an information asset owner.

5.4.2 They ensure the overall development and maintenance of health & corporate records management practices throughout LSW.

5.4.3 They provide guidance for staff on good records management practice and promote compliance with this policy to ensure accessible, appropriate and timely retrieval or patient information.

5.4.4 They design the training for records management.

5.4.5 Is responsible for all matters relating to structure function and policies of health records and acts as a channel for changes to documentation that affect health records. This also includes pilot documentation.

5.4.6 Supports teams with clinical records keeping audits.

5.5 SystmOne Champions

5.5.1 SystmOne Champions are staff with SystmOne experience who can assist members of their team in the use, design and maintenance of the electronic health record.

5.5.2 They support staff in the use of SystmOne to ensure that the electronic health record reflects accurately the care delivered to the patients to the same extent as would be expected in an equivalent paper record**.**

5.6 Registration Authority Manager

5.6.1 The Registration Authority Manager ensures that only appropriate staff have access to the clinical electronic patient records relevant to their roles and responsibilities and monitors use, requests and access.

5.7 Information Governance Manager

5.7.1 The Information Governance Manager provides support and advice regarding records management and co-ordinates the submission for the Information Governance Toolkit.

5.8 Locality Managers and Deputies

5.8.1 Locality Managers and Deputies are responsible for ensuring this policy is implemented.

5.9 Matrons / Line Managers and Team Leaders

5.9.1 Matrons, Line Managers and Team Leaders are responsible for:

- Monitoring that their staff understand and work within the standards of this policy.

- Ensuring that all of their staff who complete or deal with any patient health care records will attend an annual mandatory update session.

- Ensuring that patient records are audited in line with this policy; any outcomes and action plans are followed up and completed within an agreed timescale.

5.10 All Staff

5.10.1 All staff that complete or deal with any patient health care records must attend an annual mandatory update session. All staff must comply with both this policy and also any standards for record keeping outlined by their own professional body.

5.11 The Professional Training & Development Department or appropriate trainers

5.11.1 The Professional Training & Development Department will ensure provision of mandatory training based on current policy and national guidance and record all attendance on the Electronic Staff Record (ESR) system.

5.12 Health & Corporate Records Team

5.12.1 The Health and Corporate Records Team will advise on matters relating to preparation for archiving, destruction, and storage of health and corporate records.

5.13 Data Protection Service

5.13.1 The Data Protection Service will be a single point of access for subject access requests (SAR). Any request for access to a patient or staff members records, either from an individual, third party, solicitor or the police needs to be sent as soon as possible to the Data Protection Service. The DPS will have 40 calendar days with which to deal with request.

6 Committees with Health & Corporate Record Responsibilities

6.1 Record Keeping Groups

6.1.1 **The Learning Disability & Mental Health Records Group** oversee the management of documentation used in learning disability and mental health records, approving policies and supporting a consistent approach to the management of learning disability and mental health records in line with its terms of reference.

6.1.2 **Child Services and Physical Health Services** this process is currently under review and will be updated in the policy April 2016

6.2 SystmOne Operational Group

6.2.1 The SystmOne Operational Group oversees the management and implementation of the use of electronic patient health records.

6.2.2 It assists in ensuring risks from the implementation of electronic health records are monitored and managed.

6.3 Information Governance Group

6.3.1 The Information Governance Group is chaired by the SIRO and reports to Patient Safety & Quality Committee.

6.3.2 It ensures the appropriate governance processes are in place for the management of health and corporate records regardless of format.

6.3.3 It monitors the use of the archive for health and corporate records and access and retrieval rates and subsequent destruction and disposal of records.

6.3.4 It monitors requests for access under the Data Protection Act, Subject Access & Freedom of Information requests in line with its terms of reference.

6.3.5 It ensures that LSW records management system and processes are developed, co-ordinated and monitored.

6.3.6 It is a sub-group of the Information Governance Committee.

6.4 Committees with Corporate Record Responsibilities

6.4.1 All committees and meetings have a role in creating corporate records.

6.4.2 This may be in the form of papers, minutes and action logs.

6.4.3 It may be through policy and strategy approval or in decision making based on the level of authority delegated to the committee or group as identified in the terms of reference.

6.4.4 These records are maintained and archived by the administrator for that committee, ensuring that they are maintained and kept securely on designated drives.

7 Legal Obligations that Apply to Records

7.1 The Law and other local and national guidance that pertinent to records management include:

a. Access to Health Records Act 1990

b. Access to Medical Reports Act 1988

c. Data Protection Act 1998 (The NHS Confidentiality Code of Practice)

d. Equality Legislation and Human Rights (See Local Schemes)

e. Environmental Information Regulations 2004 (Policy and Procedure)

f. Freedom of Information Act 2000 (Policy and Procedure)

g. Public Records Act 1958 (S.3 (1)-(2) and 1967

h. Re-Use of Information Regulations 2005

i. The Common Law Duty of Confidentiality

j. The NHS Confidentiality Code of Practice

k. Professional requirements (i.e. Nursing & Midwifery Council; General Medical Council)

l. Care Programme Approach

m. Other Acts affecting service specific areas

n. Any new legislation affecting records management as it arises

o. Department of Health’s Record Management: NHS Code of Practice 2006

8 **Clinical Record Keeping** (writing in health records)

8.1 Records need to be factual, accurate and made immediately after the contact or, if not possible, within 24 hours. Any reasons for delays in contemporaneous recording of care must be recorded.

8.2 Check at each contact that the patient details are valid and accurate.

8.3 Should be consecutive. Ensure when recording your clinical event in SystmOne that you put the accurate date and time of the event. The date and time that you create the entry will automatically be recorded. The event will then be in chronological order within the tabbed journal.

8.4 In the paper records ensure that the date and time of the intervention is recorded in the left hand column. The date and time of writing the entry must be recorded in the right hand column.

8.5 Should be made using the 24 hour clock. This is automatic within SystmOne.

8.6 The record should not include unauthorised abbreviations. Commonly used, service related abbreviations will be accessible via Intranet and the document library on SystmOne. There will be an annual review of these abbreviations by the appropriate clinical area and previous years lists will be archived so that they can be accessed should the need arise.

8.7 The record should not include jargon, meaningless phrases, irrelevant speculation, offensive or subjective statements.

8.8 The record should contain a full account of the assessment and the care that has been planned and provided.

8.9 Appropriate safeguarding standards, applicable to the service area, must be applied if the record involves children.

8.10 The record should be signed, timed and dated, with designation and printed name for each entry. When completing nationally agreed documentation/forms it may only be possible to sign at the end of the form. In this case this is acceptable.

8.11 When using SystmOne your Smartcard will create a digital signature. It is essential that you never lend your Smartcard to another person.

8.12 Where a member of staff has a disability that prevents them from signing in paper format (i.e. partially sighted), advice should be sought from the relevant professional body.

8.13 Paper records must be legible.

8.14 Written records must be recorded using black ink (an exception will be for the Pharmacy department who will be authorized to use green ink on prescription charts **only**).

8.15 Paper records must be readable when photocopied or scanned.

8.16 Paper records should have all corrections scored through with a single line, initialed and dated in such a manner that any justifiable alterations or additions are clearly attributed to a named person in an identifiable role.

8.17 On SystmOne, in order to make a correction, mark in error. Only the author of the entry should mark in error. There is no circumstance where it would be expected for a member of staff to mark another staff's entry in error. This is auditable by the business intelligence team. Best practice is to bring it to the attention of the author of the error, for them to mark it in error in the system.

8.18 Paper records should contain no alterations with:
- Correction fluid.
- Ditto marks.
- Highlighters.

8.19 Polythene pockets must not be used to hold patient records as these deteriorate over time and damage the record.

8.20 Paper records must not contain paper clips, staples, metal treasury tags or any other form of metal fastening as these deteriorate over time and damage the record.

8.21 In paper records use a finish off line at end of the entry if there is a blank space (between the end of the text and the signature); if a space has been left between entries a diagonal line must be scored through it to avoid recording data out of order chronologically.

8.22 All health records should be held within the patient’s file, where this does not happen there should be a robust tracer system.

8.23 The location of all paper health records must be recorded on SystmOne. For the Mental Health Module, this can be found in the administration tree, hospital notes node. For all other modules this is found in questionnaires. It is the responsibility of staff sending and receiving files to complete this information so that the whereabouts of clinical records can be traced at all times.

8.24 Information relating to carers must be stored against the carer’s registered record within SystmOne.

8.25 Information regarding complaints must not be held in the individual’s health record.

9 Good Practice in Record Keeping

9.1 Where patient/client has had previous treatment within the organisation, check for electronic records or request most recent file from the Health Records Department.

9.2 Records should be factual, consistent and accurate, written in a way that the meaning is clear, in terms that the patient or client will be able to understand. A balance is required between simplification for the patient’s understanding, and what is needed for the primary purpose of the clinically accurate records. Demonstrate where possible, that care planned is patient centred.

9.3 Records should be recorded, wherever possible, with the involvement of the patient / client or their carer.

9.4 Records should contain relevant information about the condition of the patient / client at any given time and the measures taken by the registrant to respond to their needs.

9.5 Records should provide evidence that the registrant has understood and honored their duty of care, that all reasonable steps have been taken to care for the patient / client and that any actions or omissions on the part of the registrant have not compromised their safety in any way.

9.6 A record of any arrangements that has been made for the continuing care of a patient / client must be made at the end of the episode of care.

9.7 State if supplementary records are kept to which the patient, client or family have limited or are denied access. The member of staff must be able to fully justify this decision and must be the exception rather than the norm. A statement should be made at the top of the front sheet to the effect that supplementary records are being maintained.

10 Patient Held Records

10.1 Where this type of record is professionally acceptable, such as for community, or child health records, clinicians will not be open to criticism if the patient fails to look after, loses, or destroys the records.

10.2 Records may be printed and a copy left at the patient/ service users home, i.e. care plans for the community based services and teams. It should be documented in the Tabbed Journal within SystmOne that a copy has been printed and retained by the patient.

10.3 Staff must make the patient/carer/family aware that the notes are confidential and remain the property of LSW and need to be kept safe and returned to a member of LSW staff at the end of the episode of care.

10.4 Where patient's records are held in the patient's home professional judgement will be used regarding the recording of clinical information received outside of the actual visit. This includes telephone communication.

10.5 If the patient would prefer to have their care plan emailed to them this is permissible provided they give you their email address and take responsibility for their personal data at their end.

11 Telephone/Email / Text / Faxing & Contact Recording

11.1 Faxes are not considered secure and should not be used to transmit patient identifiable information. If it is essential to fax then a safe haven fax should be used.

All telephone calls, emails, texts, faxes and any other mode of contact with or about a patient must be recorded in the clinical record or in a recognised formal patient specific communication log which can be used as evidence of a call being made. This is particularly important for those areas of – LSW where records are not immediately accessible, such as community clinics. Information required includes date, time, from whom, details and outcome.

11.2 Security and confidentiality issues must be considered and reviewed when using telephone logs/communication books. Entries made by clerical staff will require review by the supervising clinician. Leaving logs and communication books in areas that are accessible by non-staff members is not permissible.

11.3 Any emails related to patient care should be printed/copied and placed in the patient record. Emails can contain the full patient name provided the network has been agreed safe as per Livewell Southwest Communication System: Phone, Email, Internet and Fax Policy. The latest version is available on the intranet. If an email contains information about a third party it is acceptable to paste applicable content into the clinical record and cross reference to the original email. Third party information or information that is not specific to the patient's care should be not be copied into the patient's clinical record.

12 The Practitioner's Accountability for Entries made by Others

12.1 Irrespective of the type of record or the form or medium employed to create and access it, the registered practitioner who is employed by LSW must recognise his or her accountability for entries to records made by students or other unregistered staff under their supervision.

12.2 In teams using SystmOne, all entries by non-registered staff will be countersigned. The system will automatically flag non-registered members of staff entries to the registered member of staff who will then countersign them.

12.3 For non-SystmOne users in a **community setting,** where a pre-registration student or unregistered staff member **has not been assessed as competent** in keeping records, registrants delegating this responsibility must clearly countersign **each** entry in writing or through electronic recording at the interval agreed for their particular team/service.

12.4 All pre-registration students or unregistered staff in the community, **assessed as competent,** must have their records reviewed and countersigned by the registrants delegating this responsibility at the interval agreed for their particular team/service.

12.5 Non-SystmOne records must be countersigned on the date reviewed as a minimum standard, after third contact or within two weeks if the client has a regular prescribed treatment/care plan delivered by unregistered staff. For community teams it may be more practical for the notes written by unregistered staff to be reviewed and signed as part of the overall review of the care plan.

12.6 Non-SystmOne records in **inpatient settings -** registrants delegating responsibility must clearly countersign **each** entry in writing or through electronic recording for all unregistered staff and pre-registration students before the end of every shift.

12.7 The counter-signature is evidence that the record has been **reviewed and discussed**. It is not a witness to the contact or treatment given, however, registrants are advised that they remain professionally accountable for the appropriateness of the delegation and acts or omissions of pre-registration students and unregistered staff.

13 Clinical Negligence

13.1 Patient records are sometimes called into evidence in order to investigate complaints, for criminal proceedings, professional hearings or coroner's court.

13.2 The courts regard record keeping as an integral part of professional practice.

13.3 The test for adequate record keeping is based on what is "acceptable" clinical practice.

13.4 Each clinician/professional must consider whether their record keeping is clinically adequate and would be accepted as such by professional peers.

13.5 A clear and accurate written, consecutive record which includes any significant intervention, treatment and conversation recorded by a health/social care professional is likely to be the best evidence of a patient's treatment. It is likely to prevail over any other evidence.

13.6 Records will be flawed if they do not contain sufficient detail of place, date, time and authorisation.

13.7 In clinical negligence claims, the court will consider relevant information about condition of patient at any given time. The measures taken by the Professional to respond to need, the process of the patient's care, and how the treatment decisions were arrived at, as well as the treatment itself.

13.8 The approach to record keeping that courts of law adopt tends to be that 'if it is not recorded, it has not been done'.

13.9 A record must never be falsified in any format.

14 Creation and Storage of Clinical Notes/Records

Note: this includes diaries/message books/handover books and any notes that contain patient information.

14.1 No new paper clinical templates should be created. They should now be in electronic format on SystmOne or being prepared to be moved to this format.

14.2 All templates need to go through the appropriate group for ratification. This is to create standardisation of templates where possible.

14.3 Clinical information should not be written in diaries, message books or handover books. Crib notes on patients should be avoided. If used they should not contain patient identifiable information and should be destroyed at the end of each shift.

14.4 Clinical records will be maintained in accordance with the Department of Health's Record Management: NHS Code of Practice 2006 (part 2 updated 2009). and the standards as outlined in individuals professional Body. This Principle applies across all care settings and applies to all types of records in all formats (i.e. written, electronic, printed documents, emails, scanned documents, microfilm, photographs, x-rays, audio, videotapes, cassettes, CD roms, floppy discs etc.). Floppy discs, CD roms, cassettes and videotapes with patient identifiable information should be returned to the IT Department for disposal through the agreed contractor.

15 Shared Drives

15.1 Shared drives must not be used for the purpose of storing patient identifiable information. Any information will be stored in the electronic patient record or where services do not use electronic patient records, will be printed off and filed in the patient file.

16 Tracking Health Records

16.1 All new records are created through SystmOne. However the historic paper records are available on request from the following services:

16.1.1 All Mental Health records; community records, CAMHS and Children's Speech & Language Therapy – from Hatfield House.

16.1.2 Community & Rehabilitation inpatients and Children's Services from Bush Park, Derriford.

16.1.3 Learning Disabilities records – Westbourne Record Store.

16.2 Paper records can be requested from Hatfield House via the request form available on the intranet.

16.3 Any movement in the paper record should be tracked and traced via the notes node on the clinical tree in SystmOne for Mental Health and Learning Disabilities and via the Notes Tracking Questionnaire in the Community modules.

16.4 The person responsible for completion of the tracking information is the staff member using the file, or having last contact with the file prior to its transfer to another area or person.

17 Transporting Health Records

17.1 As a community service, there may be a need for health records or other confidential information to be transported between sites and department or with external agencies and partners.

17.2 This must be enclosed in a tamper proof sealed bags/ envelopes and clearly labelled with the specific name of the person or department where the package is to be received. You should clearly mark the name and base of the sender on the other side.

17.3 When sending in Crown boxes of records to be archived these must be sealed with a strip of parcel tape on each side of the box for security purposes.

17.4 Records must be carried between sites or department by authorised staff only. Authorised staff may include:

- Appropriate member of staff as part of their role (i.e. community team)
- Internal transport systems
- Authorised courier service
- Special delivery service by Royal Mail

17.5 Transporting records from LSW premises requires vigilance and the principles of confidentiality must be maintained.

17.6 On arrival at the required destination, a full check of the items transported must be undertaken to ensure no individual papers have in advertently gone missing during the transportation process.

18 Removal of Paper Health Records from LSW Premises Overnight

18.1 Staff must not take paper healthcare records home. If this is felt to be necessary in exceptional circumstances, a risk assessment must be completed and written approval from their line manager obtained prior to doing so. The record must be traced out.

18.2 The records must be returned to the office the next working day.

18.3 Records or other sensitive information must not be left unattended in transit at any time.

18.4 When carried in a vehicle they must be locked in the boot and if available placed in a tamper proof container.

18.5 This also applies to electronic equipment used to access healthcare records.

18.6 Records must not be left in vehicles overnight and unscheduled stops must be avoided.

18.7 Staff who obtain approval to take records and other sensitive information home or who are required to as an agreed part of their role, are responsible and accountable for the security and confidentiality of the records which must be kept in a locked and secure environment until they can be returned.

18.8 Additional advice and guidance on transporting records may be sought from the Health Records Service by telephoning (01752) 434525.

19 Use of Courier Services

19.1 There is an approved list with formal contracts in place to ensure that, where external courier services are used to transfer health records, these documents are transported securely and in sealed envelopes.

19.2 The contracts include confidentiality clauses and documents are signed in and out.

19.3 The use of approved couriers is to reduce the risk of records loss. A listing of approved couriers can be obtained from Hatfield House.

20 Use of Registered Mail

20.1 Where records are sent to external agencies (i.e. to comply with requests from the Courts) the courier service must be used for any original records.

20.2 Copy records may be sent by recorded delivery (i.e. to respond to requests from the solicitors as part of a legal claim) to enable receipt and delivery to be tracked.

20.3 **Use of Secure Envelope (i.e. Polylope)**

20.4 Records transferred by internal mail are sent in a new sealed tamper proof envelope each time (i.e. Poly Envelop or purpose made container fitted with security safe tags) and marked appropriately.

20.5 These can be ordered through the Records Team at Hatfield House**.**

21 Storage of Records

21.1 All paper and electronic and health records in LSW must be appropriately stored.

21.2 Records must be kept securely with appropriate security measures in place to prevent loss, unauthorised access and modification.

21.3 Inpatient clinical areas or community team offices and work bases, paper records are kept securely when not in a use in a locked office, trolley or cabinet.

21.4 Where patient or personal identifiable information is being held, a minimum of two locks are required in place between the information and any direct access with one lock being in the lockable filing cabinet or trolley.

21.5 The storage must enable controlled access to the record as required, as this prevents damage to the record and maintains integrity.

21.6 Electronic records must be accessible 24 hours per day, to staff participating in the care of that patient/client.

21.7 The managers of teams that hold records will consider:

- Security
- Protection against fire
- Protection against water
- Environmental conditions

21.8 Equipment used for records storage must meet fire regulations. The following factors must be taken into account:

- Compliance with Health and Safety regulations
- Degree of security required
- User needs
- Type of record to be stored
- Size and quantity of records
- Usage and frequency of retrievals
- Ergonomics, space, efficiency and cost effectiveness

21.9 They inform the Records Manager or records store at Hatfield House any additional storage sites used.

22 Filing Health Records

22.1 Areas where health records are stored should have a clear filing protocol in place.

22.2 All documentation should be stored in the appropriate filing system when not in use. This should have two locks (i.e. a locked cabinet in a locked room).

22.3 Filing of documentation is the responsibility of the individual who has made the entry in the record.

22.4 Complaints or litigation papers are filed separately by the Complaints and Litigation Manager and must not be filed in the patient record.

22.5 File copies of letters do not need to be signed.

23 Managing Electronic Health Records

23.1 The principle responsibilities and requirements of record management do not alter if a record is held in differing forms, such as paper, on disc, audio tape or in an electronic system.

23.2 Access to electronic health records is through the Smartcard system.

23.3 It is the responsibility of each member of staff to ensure the safety and security of their Smartcard at all times.

23.4 Any breaches or misuse of individual Smartcards maybe subject to disciplinary policy and / or security policy procedures.

23.5 All SystmOne screens must be positioned to ensure other parties are not able to read them.

23.6 The systems must be appropriately exited when not in use.

23.7 SystmOne records are protected by information security procedures against corruption and external damage with access monitored and audited to ensure appropriate use.

24 Retrieving Health Records

24.1 Archived paper records are retrieved from Hatfield House, Bush Park or Westbourne.

24.2 This includes the secure transport of the records to the area requesting them and return once the episode of care is complete.

24.3 Records retrieved from the archive are obtained on request using the request form on the intranet, and are tracked in and out of the archive using SystmOne Hospital Notes Node (mental health and learning disabilities) or Tracking Questionnaire as appropriate (other services).

24.4 Records are retrieved and transported to and from the archive using one of the secure methods previously described.

25 Missing Health Records

25.1 Retrieval rates from the archive store are monitored and reported to the Information Governance Group. They are also disseminated for information to Service Leads and Locality Managers and Deputees.

25.2 If a record cannot be found in the records library a process is in place using ePEX, SystmOne tracking node, and tracking questionnaires to identify the last location of the record and a search is initiated to locate and retrieve the record.

25.3 In the event of record not being found an incident form is completed identifying the steps undertaken to trace the record.

25.4 This is included in reports to the Records Management Group and Information Governance Group.

26 Retention of Health Records

26.1 Records are retained in line with the NHS code of Practice Part 2 Retention Schedule. This can be found on the intranet in an Excel template.

26.2 This is the identified length of time a record is required legally to be retained and the types of record to be held.

26.3 The length of time for retaining records will depend on the type of record and its importance to the LSW's business functions.

26.4 Copies of the retention schedule can be found in the Records Management Code of Practice 2009 Part 2 on the Records Management Page.

26.5 Advice must be sought from the Records Manager if staff are unsure as to whether a record must be retained and/or how to do this.

26.6 Paper records are retained at the clinical base until the end of each year and sent to Hatfield House for deep archiving.

27 Archiving for Health Records

27.1 LSW provides an archive service (Hatfield House) for its clinical paper records.

27.2 Prior to health records being archived contact must be made with the Records Team at Hatfield House to establish that the records can be archived and agree a time and date for delivery or records to the store.

27.3 In all cases Crown boxes must be used to archive the records. These can be obtained from the records team at Hatfield House. Each side of the box must be sealed with parcel tape strips.

27.4 Boxes are labelled with details of contents listed, owner, and area, potential frequency of future access and proposed destruction or retentions date.

27.5 Once received this listing is a downloaded to an archive inventory database.

27.6 Records must only be sent via the internal courier service.

27.7 On no account must collected records be transported using public transport.

27.8 Security of the records is the responsibility of those transporting the records and the security of both the physical record and the data is paramount at all times.

28 Disposal of Health Records

28.1 Once the records have reached their respective retention dates, they must be disposed in line with procedures as identified in the NHS Code of Practice.

28.2 Records held within the archive are checked monthly to determine those that are at the end of their retention period.

28.3 Those that are to be retained indefinitely e.g. as part of legal claim, ongoing investigation or of historic value are marked accordingly and stored separately.

28.4 Where any record is deemed to be of historic value, it is transferred securely to the regional records office and recorded as such by the Records Manager.

29 Scanning of Health Records

29.1 For business efficiency and storage space the scanning of paper documents may be appropriate.

29.2 LSW scans a range of health documents into SystmOne records.

29.3 The scanned document is checked to ensure that all information has been copied across; that it is legible and assigned to the correct patient to ensure compliance with the requirements of the Data Protection Act 1998 and Civil Evidence Act 1995 to assuring that scanned documents are able to be reproduced and that the integrity and content of the original document is maintained.

29.4 Only after these checks have occurred can the paper document be destroyed in full compliance with destruction procedures, by placing into a burn bag or using a cross shredder.

29.5 Scanned document information is included in SystmOne records to ensure an audit trail is in place.

29.6 Scanning equipment should meet British Standards and in particular the ‘Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically’ (BIP 0008). Further detail and guidance can be found in Records management: NHS Code of Practice (Part 1 page 13) 2006.

30 Destruction of Health Records

30.1 It is vital that confidentially is safeguarded during the disposal and destruction of paper healthcare records.

30.2 LSW has processes in place to undertake the destruction of healthcare records lawfully and completely.

30.3 Records sent for destruction are logged identifying what has been sent for destruction and when.

30.4 A log is kept by Hatfield House records team of items sent for destruction from the archive.

31 Training

31.1 All LSW staff are made aware of their responsibilities for record keeping and record management at induction.

31.2 Staff with specific roles in respect of the management of health care records are provided with additional training appropriate to their role either through access to specific eLearning packages or as part of their local induction and appraisal process.

31.3 Team leaders, heads of service and locality managers are responsible for identifying staff that may have additional training needs in respect of records management of their teams.

31.4 Advice can be obtained from the Records Manager as necessary as to any additional training or support required.

Corporate Records

32 Introduction to Corporate Records

32.1 Corporate records are part of the organisational memory of LSW.

32.2 They support the day to day business which underpins the delivery of care.

32.3 They document the administrative and managerial decision making, protect the interests of LSW and the rights of patients, staff and members of the public.

32.4 They assist LSW to meet legal requirements, including requests for information under subject access permissions of the Data Protection Act 1998 and requests under the Freedom of Information Act 2000.

32.5 They provide evidence of actions and decisions taken and as such are part of the Organisations assets.

32.6 Corporate records, whether paper or electronic, must be accessible and retrievable when and where required. This includes corporate records that area part of a formal document and recognised management system as well as records on network drives and in shared folders.

32.7 Corporate records require similar management processes to be in place as health records.

32.8 Overall Principle of Corporate Records Management:

32.8.1 **Records are available and can be accessed when needed** – records and the information within them can be located and displayed in a way consistent with their use. The current version is identified where multiple versions exist.

32.8.2 **Records can be interpreted** – the context of the record can be interpreted: who created or added to the record, when this occurred, how the record is related to other records.

32.8.3 **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.

32.8.4 **Records can be maintained through time** – records must remain available, and accessible, with the ability to be interpreted and trusted for as long as the record is needed, perhaps permanently, despite changes of format.

32.8.5 **Records are secure** – from unauthorised or inadvertent alteration or erasure. That access and disclosure are properly controlled and audit trails track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.

32.8.6 **Records are retained and disposed of appropriately** – using consistent and documented retention and disposal procedures, in line with NHS Corporate Records Retention guidelines.

32.8.7 **Staff are trained** – to be aware of their responsibilities for record-keeping and record management.

33 Definition of Corporate Records and Information

33.1 Corporate information refers to information generated and received by an organisation other than clinical, care or services user information. It includes records generated by LSW’s business activities.

33.2 This includes but is not exclusive to estate, financial, information management & technology, personnel records, purchasing and supplies.

33.3 Emails and attachments and webpages on internet and intranet sites are considered corporate records (See email Confidentiality Policy).

33.4 A document becomes a corporate record once it has been finalised and approved i.e. it’s no longer a draft or subject to further amendment and is part of LSWs corporate information, publicised, available to staff and stakeholders and available on the intranet.

33.5 At this point the record is not amended until it reaches its review date unless internal or external triggers require this review. The record is held on a corporate system not on a local drive on a PC or laptop.

34 Classification and creation of a corporate record

34.1 Corporate records are classified in order to ensure they can be tracked efficiency and retrieved as necessary.

34.2 They include policies and procedures. Meeting papers, minutes, action logs, reports published internally and externally as well as information held on individual department, team and corporate drives.

34.3 The format will ensure that those responsible for record retrieval are able to locate records more easily.

34.4 To support his process there is a naming convention in place e.g. policy, strategy and business plan.

34.5 There is a standard template for the submission or reports and papers to LSW committees including front sheets agendas, report templates, policy and strategy templates available on the intranet.

34.6 Information held electronically is identified through the information asset registered completed and reviewed annually.

34.7 Corporate electronic records must only be kept on authorised drives and kept secure from unauthorised access, unintended alteration or deletion.

34.8 Locality, Team Department Corporate Record; Each locality team and department identifies the key drives and area where information for their team is held.

34.9 This is included in the information asset register and staff are informed on induction of the areas where they are required to store information regarding their work apart from patient identifiable information or clinical care.

34.10 This includes any naming convention in use for files to ensure consistency.

34.11 Access to this information is controlled by password access where the information is held electronically and is role specific where information is held in paper or alternative formats.

35 Centrally Held Corporate Records

35.1 Corporate records in the form of policy, strategies and competencies are retained on the intranet pages and archived from there once replaced and updated. These are held and monitored by information governance lead and Policy Ratification Group.

35.2 Minute, agendas, meeting papers and information regarding LSW committees are held and managed by the person holding the role of administrator to that committee whether a standing committee, task and finish or time limited group.

35.3 Minutes agendas, meeting papers etc. for committees of the board e.g. assurance committees are held and managed by relevant staff who service that committee. This is over seen by the Organisation Secretary.

35.4 Access to this information is controlled by password access where the information is held electronically and is role specific where information is held in paper of alternative format.

36 Writing Corporate Records

36.1 When writing business documents on behalf of LSW all staff must ensure that where a template exists for that type of document it is used. All staff are required to write documents that conform to national recognised best practice standards.

37 Maintenance

37.1 To ensure best practice, document owners are responsible for ensuring their documents are maintained and updated as appropriate and maintained as part of the corporate record.

37.2 All documents not reviewed will be removed from the website and intranet and not considered a current working document of LSW.

37.3 All business records must be stored and maintained in conditions identified in Part One of the Code of Practice.

37.4 All staff must save and/or back up computer files to shared drives and maintain master copies of all records in accordance with the retention period and the need to access records within five days.

37.5 Papers contained within the records should be arranged in a logical structure and be ordered chronologically.

37.6 Duplicate papers should be removed and where a file becomes too large, a second volume should be created.

37.7 Services and departments should devise a file plan to keep track of the records they hold and to assist with records auditing. The file plan should be reflected in the physical storage of the files.

37.8 Records should be stored securely and not left unattended or accessible to staff not authorised to see them.

37.9 Where records are removed from the office, a tracking system should record who has removed the file and where it is. The process need not be a complicated one, e.g. a book that staff members sign when a corporate record is removed or returned.

37.10 Records should be transported securely in sealed envelopes or Polybag sealed with a tag.

38 Tracking Corporate Records

38.1 Corporate records are held electronically and are not physically moved elsewhere.

38.2 They are tracked by means of the naming and filing convention in place.

38.3 Where paper files are moved they have an item reference number or identifier, a description of the item, the person holding them, where they are transferred to the purpose and date.

39 Closure of Corporate Records

39.1 Records should be closed as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records has been closed, together with the date of closure should be shown on the records itself as well as noted in the index.

40 Archiving Corporate Records

40.1 When corporate records are held in paper format these may be archived centrally.

40.2 The process followed is the same as for clinical records.

40.3 Hatfield House must be contacted in the first instance to arrange the archiving method and for transfer of the records to be agreed.

40.4 Crown boxes must be used and labelled properly with the content, nature of the records being moved and the planned disposal date in line with the retention schedule contained in the Records Management: Code of Practice.

40.5 Records recovered by the archive are checked and logged into the archive data base with the minimum retention period details included.

40.6 For electronic documents these are archived in dated folders on the relevant drives.

40.7 Records for archiving are held securely and are maintained to ensure that they are properly stored and protected throughout their life cycle.

40.8 This includes any electronic records that are migrated across to new systems to ensure any legacy information remains accessible and retrievable when required.

41 Destruction of Corporate Records

41.1 Methods used throughout the destruction process must provide adequate safeguards against the accidental loss or disclosure of the contents of the records.

41.2 A record of the destruction of records, showing their reference, description and date of destruction is maintained and preserved, so that LSW is aware of those records that have been destroyed and are therefore no long available. This is retained as part of the disposal schedules within the archive.

42 Training

42.1 All LSW staff are made aware of their responsibilities for record keeping and records management at induction and mandatory training.

42.2 Staff with specific roles in respect of the management of records are provided with additional training appropriate to their roles, whether through access to specific eLearning packages or as part of their local induction and appraisal process.

42.3 Team leaders, heads of service and locality managers are responsible for identifying staff who may have addition training needs in respect of records management for their teams.

42.4 Advice can be obtained from the records manager as necessary as to any additional training or support required.

43 Standards for Corporate Record Keeping

General Standards

- A record must be kept of all activities carried out and decisions made on behalf of the LSW

- Records may serve many purposes; the most important is to have an up-to date record of events and evaluations

- The ownership (author), version number, and filename should be clearly stated in all documents; preferably in the footer of each page

43.1 **Dated**

All entries should be dated.

43.2 **Signatures**

The creator of the record should be clearly identified. Where a signature is required this should be recognisable and the name and designation of the person printed beneath the signature.

43.3 **Abbreviations**

Abbreviations should be avoided wherever possible. Where used, the full meaning of an abbreviation should be cited the first time it is used.

43.4 **Alterations**

Do not try to hide errors. Paper records should have errors scored out with a single line and be initialled, dated and timed.

43.5 Additions

If an addition needs to be made to a record it should be prefaced with a comment indicating that this is an additional or late entry and be separately dated and signed. Never try to insert notes, especially after notification of a complaint or claim. Never try to disguise additions to a record. Any amendments made must be recorded in such a way that they may be independently auditable in case of future investigation or review for example, dated, timed and signed.

43.6 Version Control

43.6.1 When considering the implications of an historic record it is important that the circumstances surrounding the creation of the record can be understood. For example, when investigating an incident it may be necessary to know which version of a particular policy or procedure was in force at the time of the incident.

43.6.2 The following version control scheme should be adopted for documents that are likely to have a number of iterations.

Document Status	
Version Number	
Status	
Draft,	
Final	
Initial Development	0.0
Iterations	0.1, 0.2
First Release	1.0
Minor Amendments	1.1, 1.2
Second Release	2.0

43.6.3 When making changes the released versions 1.0, 2.0 etc. should equate to the official record. Previous versions of the document must be retained in line with the retention schedule.

43.7 Naming of a File

A file name should be clear what information it contains and include a date and version number. Maximum characters for a file name should be 15-20.

43.8 Personal Comments

Records should contain factual information or professional opinions. Only include commentary that is relevant and appropriate to the record. Records are not the place to note offensive observations about a person’s character, appearance or habits. Under the Data Protection Act 1998, members of the public are allowed to have access and view the content of their records under the Subject Access Request Procedures. Avoid recording offensive, personal, or humorous comments about an individual.

43.9 **Dictated Notes**

- Typed notes must be checked and signed by the professional who dictates them

- Responsibility for the accuracy of the record lies with the person who created the record not the typist

43.10 **Completeness**

- A record needs to be fit for purpose. It should therefore contain information which should be adequate, relevant and not excessive for its purpose. For example, order forms should be completed fully. Insufficient information may lead to serious incidents.

43.11 **Clarity and Legibility**

- Records need to be clear and legible. A hand written record should be written in permanent black ink wherever possible. This will give the records greater clarity and legibility when photocopied. If it is not possible for a person to write legibly the record should be typed.

- Thermal faxes may fade and should not be included as part of a permanent record. The information should either be transcribed into the record, the original requested or an indelible photocopy made of the fax.

43.12 **Policies**

- All policies must comply with the requirements set out in the Policy Guidance & Template on Intranet

43.13 **Reports**

- Reports need to be evaluated by the appropriate professional and any action taken documented within the record.

43.14 **Records Systems**

- All Record Management systems should have privacy impact assessment, and an identified information asset owner and subsequent risk assessments. More information can be obtained from the Information Governance Lead.

43.15 **Filing**

- Wherever possible records should be held in a departmentalised central filing system, in electronic form on a central server to minimise duplication and reduce the costs of storage. Paper records should be held centrally within a department.

43.16 Each area where records are stored should have a clear local record keeping Procedure including:

- Provide technical and descriptive documentation to enable the efficient use and support of the system, including information to provide an administrative context for the record(s).
- The rules used for referencing, titling, indexing and, where appropriate, the protective marking of records.

43.17 All files should be stored in the appropriate filing system when not in use. Filing of documentation is the responsibility of the individual who last made an entry in the record.

43.18 **Indexing**

- The record holder should document a complete list of the files that are held. Such lists should be reviewed on a regular basis for accuracy and completeness.

43.19 **Multiple Documents**

- Multiple documents that constitute a record should be filed together. Paper documents should be securely attached to each other. Where a record constitutes electronic and paper documents it should be kept as a complete document wherever possible. Where this is not possible this should be cross referenced.

43.20 **Email**

- Email is a communication method not a record management system. Where the content of email or attachments forms part of a record it is the responsibility of the user to ensure it is added to, and becomes part of, that record whether held in hard copy or electronic format.

43.21 **Original and Duplicates** (copies)

- Maintaining multiple duplicate copies of the same document is discouraged. Access controls should be applied to centrally held records to ensure that the integrity of master records is maintained at all times. Copies may be held in circumstances where the original is forwarded outside of the organisation.

- Anyone having to create a copy of a record must immediately mark the record as a copy to avoid confusion with the original master copy. Copy records should only be retained for the period of their immediate use after which time they should be destroyed.

43.22 Tracking a Record

- Records must be traceable at all times and a system to trace records maintained in each.

43.23 Transferring Records

- The permanent transfer of original records out of a filing system is to be discouraged.

- Where there is a need to transfer original records out of a filing system (i.e. personnel records), a clear audit trail must exist showing: the date of transfer, reason for transfer, where the record has been transferred to and who actioned/authorised the transfer.

- Staff who transfer records are responsible for ensuring that appropriate safeguards are in place to ensure safe and secure delivery.

43.24 Storage and Security

- All staff are responsible for the safe custody of records in their use. Personally identifiable information must be handled in accordance with the Data Protection Act. It is important that all staff are aware of their responsibilities in respect to information security and confidentiality. Under no circumstances should personally identifiable information be left unattended and/or visible to those who should not view it, for example, on a computer screen when you are not at your desk, on top of a desk in-tray, in the boot of your car or on a car seat visible to the public. Records should be stored securely in either a locked cabinet or within a secure environment on a computerised system. Where rooms containing notes are unattended, they must be locked.

43.25 Scanning Records

- Where paper records are scanned and held electronically there should be a local procedure in place which has been approved by the Information Governance Group .

43.26 Missing Records

- If a record cannot be found your line manager must be advised immediately. When all efforts to find the record have been exhausted, local departmental policies should be followed and an incident form completed and returned in accordance with LSW procedure.

43.27 Archiving

- The Records Management Meeting will, with the assistance of the relevant Directors and Locality Managers assess the financial impact, particular in relation to storage, archiving, training, etc., and subsequently develop an action plan and guidance for staff.

44 Monitoring Effectiveness

- The clinical records will be audited against standards within this policy and other standards (i.e. CPA and local and national standards) annually using audit tools agreed with audit coordinators
- SystmOne will be audited against unauthorised access (accessing records that are not appropriate)
- Paper Health Records Inventory
- Quarterly Records Management Report
- Corporate Records Inventory
- Corporate Records Audit

44.1 Results will be presented to the Care Programme Approach (CPA) Steering Group, Records Management Group, Information Governance Group) and to the Safety, Quality and Performance Committee on an annual basis.

44.2 Following completion of audit programme, this policy is reviewed and updated to ensure it reflects current practice and national guidance.

All policies are required to be electronically signed by the Lead Director. Proof of the electronic signature is stored in the policies database.

The Lead Director approves this document and any attached appendices. For operational policies this will be the Locality Manager.

The Executive signature is subject to the understanding that the policy owner has followed the organisation process for policy Ratification.

Signed: Director of Professional Practice Safety and Quality

Date: 26th February 2016