The Tavistock and Portman NHS
NHS Foundation Trust

Health Records Management Procedure

Version:	4.2
Bodies consulted:	Caldicott Guardian, CCIO, Clinical Governance Manager, Informatics Manager, Governance Manager,
Approved by:	PASC
Date Approved:	7.9.16
Lead Manager:	IM&T Director
Responsible Director:	Deputy Chief Executive
Date issued:	Sep 16
Review date:	Aug 18

Contents

Health Records Management Procedure

1 Introduction

The Tavistock and Portman NHS Foundation Trust (the Trust) is dependent on its health records to deliver care efficiently and to account for its actions. This procedure defines the structure and processes for the management of clinical records in all media at the Trust. Records management through the proper control of content, storage, transporting and access to records reduces the risk of poor clinical care, due to missing records, legal challenge and financial loss. This procedure sets out the way in which the Trust will meet its legal obligations in relation to the Data Protection Act 1998, and Freedom of Information Act 2000 and standards set by the Care Quality Commission, The Health and Social Care Information Centre, and the NHSLA in respect of records management. This procedure should be read in conjunction with the Corporate and DET Records Procedure.

2 Purpose

The purpose of this procedure is to set out the way in which the Trust will meet its legal obligations and organisational requirements in relation to the management of its clinical records. It details what should be included in patient clinical notes and how information is to be recorded and sets out the standards for record keeping that are to be followed by staff.

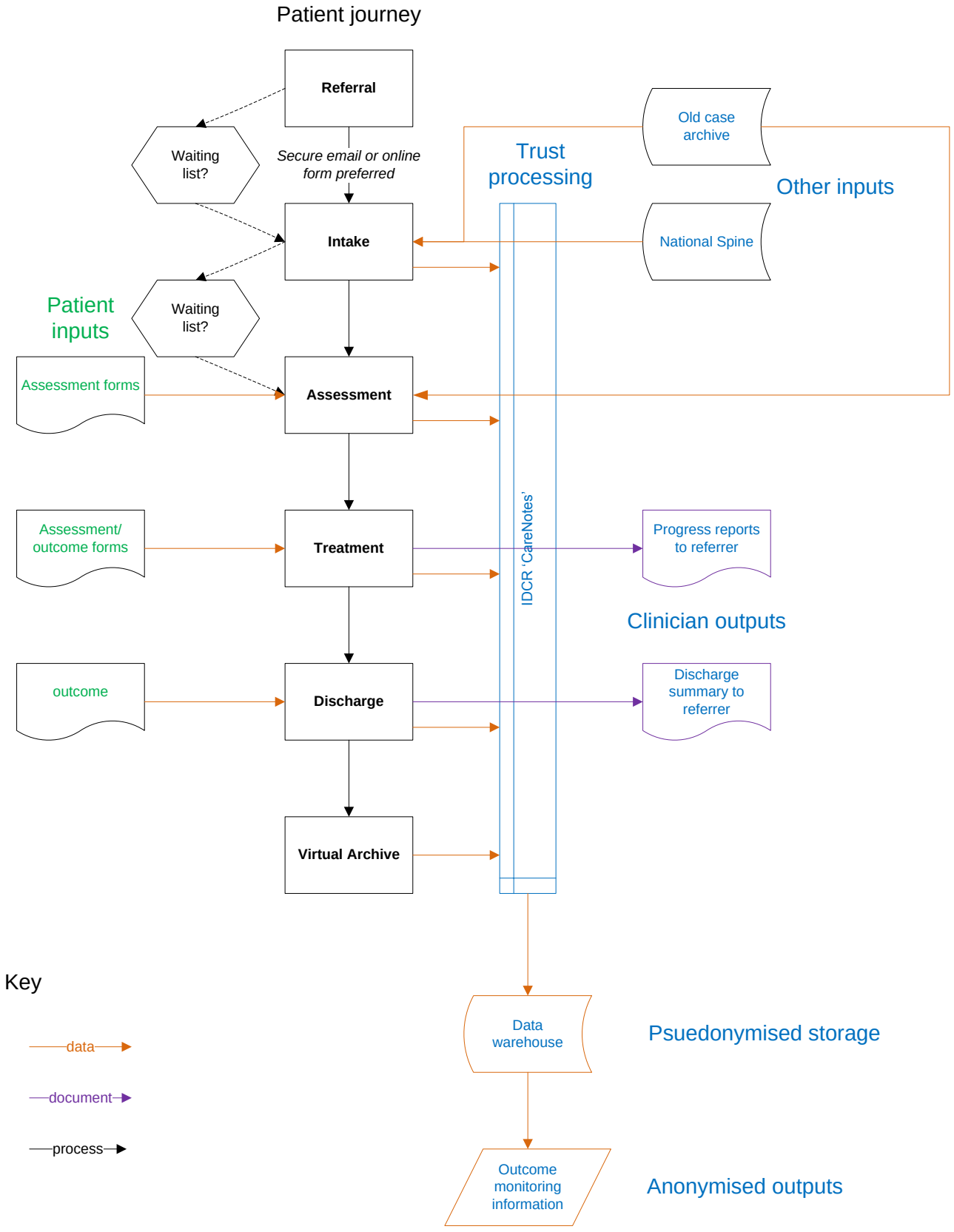
3 Scope

This procedure is applicable to all staff in the Trust who handle, use, and/or access clinical records of all types using CareNotes.

This procedure must be read in conjunction with the Clinical Governance Handbook, which provides additional detail on the management of processes at team level.

This illustration of the summary data flow illustrates the areas this procedure covers:-

Healthcare records journey



4 Definitions

Term	Definition
Patient record	The integrated digital care record (IDCR) contains all the personal information about a service user and their care. Such information may include the clinical notes, letters and legal documents, reports, and any other records required to be held on the service user. Different categories of information are held under specific tabs on the electronic record for ease of reference.
Clinical Notes	The clinical notes of the work with the service with a service user.
Personal Confidential Information	Relates to a living child, young person or adult who can be identified by this information. It includes factual information, opinion, and any indication of the intentions of the Trust in relation to the individual or any other person in respect of the individual.
Sensitive Personal Information	Information as to a person's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; physical or mental health or condition; sexual life. Information as to whether they are a member of a trades' union; the commission or alleged commission by him/her of any offence, or any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.
Accessing Personal Information	Making available to the individual their own personal information held on them by the Trust by letting them read it, by reading it to them, or showing it in a way that they can fully understand
Third Party	Any person, other than the service user who is either the subject of the information or a member of the Trust staff.

Data Subject	An individual whose personal information is the subject of a record.

5 Duties and responsibilities

5.1 The Chief Executive Officer

The CEO is responsible for appointing an officer who is accountable for the management of records. The CEO has appointed the Governance Manager to have lead responsibility for the corporate management of records.

5.2 Director of Information Management and Technology

The director is responsible for the operational management of the electronic patient records system.

5.3 Governance Manager

The Governance Manager is the Trust's subject matter expert on data protection. The manager has operational responsibility for management of closed (archived) clinical records in the Trust. The manager is responsible for supporting the implementation of records management policies and procedures throughout the Trust and is the Trust's Privacy Officer. The manager will audit and report on compliance with the Records Management Code of Practice.

5.4 Medical Director

The Medical Director shall set the standards for clinical record keeping, see appendix C.

5.5 Clinical Governance Manager

The Clinical Governance Manager will make arrangements for the annual records audit to assess compliance with the record keeping standards.

5.6 Access to Records Officer

The Officer will be responsible for processing all requests for information in clinical records.

5.7 Directors and Managers

Directors are responsible for ensuring that their staff are fully aware of the importance of good records management and that staff abide by this procedure. The clinical managers are accountable to their director for overseeing clinical records management within their directorate.

5.8 General Office Manager

The General Office Manager is responsible for the management of the paper medical records archive. The records archive will hold 'closed' files.

5.9 Staff Members who make entries to clinical records

Individuals are responsible for any clinical record that they create and must follow this procedure, and related procedures, in their handling of clinical records, particularly in

relation to accurate filing and tracking of records. Staff may only access records, and parts thereof, where they have a legitimate relationship with the data subject.

5.10 All Staff

All staff are responsible for keeping the clinical records that they handle confidential and only sharing information where there is consent to do so or required by law.

6 Procedures

Records are valuable because of the information they contain. However, information is only usable if it is correctly and legibly recorded in the first place, is then kept up to date, and is easily accessible when required. All records must be typed to ensure legibility.

6.1 Purpose of the Patient Record

The purpose of a clinical record is to facilitate the care, treatment and support of a particular service user. The record includes clinical notes, letters, summary reports, assessments (including risk assessments, standardized assessments), patients' drawings, formulations developed by clinicians and service users) All clinical records should be of a consistently high standard of accuracy, legibility and completeness. Records should include:

- Clinical notes containing a description of assessment and treatment sessions, and treatment plans
- Summary reports of assessment and treatment, risk assessments and safeguarding assessments.
- Relevant disclosures by the patient – pertinent to understanding cause or effecting cure/treatment.
- Facts presented to the patient.
- Correspondence and other forms of contact to and from the service user and other parties directly involved in the patient's assessment and/or on-going care.
- Patients drawings completed within sessions
- Formulations developed by clinicians and service users

Records should exclude:

- Unnecessary abbreviations, jargon, meaningless phrases and unsubstantiated speculation.
- Personal opinions regarding the patient (restrict to professional judgements on clinical matters).
- Process notes. These are detailed notes regarding clinical sessions written by some therapists for use in clinical supervision. Process notes should be anonymized, belong to and are the responsibility of the clinician and do not form part of the clinical record.
- Correspondence from complaints.

Note: if a record contains legal reports or other legal documentation, it should be stored in a separate marked section within the file and not with continuous clinical notes.

6.2 Record Keeping Standards

Clinical notes are an important component of the patient's record. An entry in the service user's clinical notes should be made, after each clinical contact relating to that service users care. This entry should be typed by the relevant clinician as soon as possible after this clinical contact has occurred. The entry should provide current information on the care and condition of the service user. Clinical Notes should:-

-
- Be factual, consistent, accurate and concise
- Be typed
- Should be validated and saved on the IDCR.
- Be accurately dated, timed
- Should be written in terms that the service user or carer will be able to understand, in the event of the service user requesting access to their clinical records.
- Be consecutive, as guided by the system.
- Provide evidence of the assessment, and the care or treatment planned, the decisions made, the care or treatment delivered and the information shared.
- Provide evidence of actions agreed with the service user (including consent to treatment and/or consent to share).

The standards for clinical record keeping are subject to annual audit and review/updating; the standards are shown at Appendix C. A related procedure sets out the arrangements for audit of record keeping.

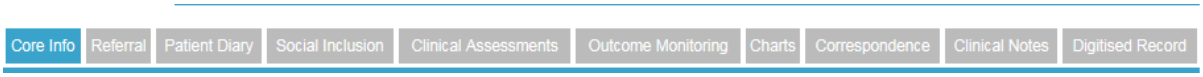
6.3 Procedures for Generating, Storing, Transferring and Destroying Individual Records

6.3.1 New Patient Registration

Service managers shall be responsible for ensuring that patients are registered according to the requirements of local systems and practice.

6.3.2 Creating a New Record

- Clinical administrators shall create a new IDCR on the electronic patient administration system; this IDCR shall contain specific tabs to ensure all information is easily accessible. Clinical System Tabs



All information is recorded and held electronically under the specific tabs on CareNotes, please see above list of tabs:

6.3.3 Checks to be followed to Avoid Creating Duplicate Records

Upon receipt of a referral, staff will check to see if the patient already exists on the system before adding them as a new patient. Once added to the system, the system carries out an automatic check against the National Spine for surname and DOB to establish the correct patient. If anything matches the data inputted, it notifies the user that they are about to create a duplicate record and appropriate action can then be taken.

6.3.4 Tracking of Records

All records are stored electronically and access rights are assigned at service level. Access of records is monitored.

6.3.5 Transfer of care to a new provider

This might take place when a contract has ended, for further information see appendix F.

6.4 Preservation, Storage and Destruction of current Paper Records

Existing paper files that are no longer in active use by a clinical team should be closed: an Archive Request Form[1] must be completed and sent together with the files to be archived to the General Office in a locked bag[2].

Older paper records are stored in the archive, managed by General Office staff. Portman Clinic staff manage their own archive.

Clinical and administration staff may request a file from the archive. The request must be by email. The file is retrieved from the archive, and, at the same time, a properly completed tracer card must be inserted into the stack to replace the file. Files are sent to the appropriate departments in lockable bags. When a patient with an archived paper file is re-referred, the previous paper file will be requested from the archive and will be scanned by into *CareNotes* under the digital information tab, so that the older information is available to staff involved in the re-referral.

After scanning, the paper file will not be returned to medical records for filing; it will be destroyed.

The Trust follows national guidelines in respect of the retention of medical records. A schedule detailing storage and destruction arrangements for medical records is available on the Trust's intranet and website appended to the Records Strategy. The Trust will keep any

[1] These are available on the Trust intranet

[2] This does not apply to the Portman who are responsible for their own archive in the Portman clinic

file which is subject to an ongoing complaint or similar action, until that complaint has been closed, if the complaint was raised and the end of the normal retention period.

Clinicians may have clinical reasons for keeping a file for longer than the retention period states, such cases should be discussed with the clinical superviser –if both agree that the record should be retained then this should be recorded in the notes and on the archive request form.

Archiving of old closed files takes place annually (during the summer) and is the responsibility of the General Office staff. The General Office staff select records for patients with whom there has been no contact for the number of years shown in appendix G, either as identified on the archive form, or by manual inspection. For retention purposes, the date of last contact shall be the date of the discharge letter. A list of destroyed or permanently archived files is compiled and retained electronically on the server. Files are placed in a confidential waste bin and passed to our contracted waste company who provide a certificate of destruction for Trust records. For records are held electronically the destruction date will be triggered by the discharge date on the system.

The above will remain in place until all paper records are destroyed or scanned for future use.

6.5 Group Records

An individualised summary of each patient's attendance at the group should be documented in that patient's 6 monthly review and closing summary.

6.6 Access to Personal Information contained in Health Records

The procedure for responding to a request for access to health records is set out at Appendix D.

6.7 Safeguarding records against loss, damage or unauthorised use

The confidential nature of health records cannot be overstressed and must always be borne in mind by those who have to handle such records.

Additional protection is in place for staff involved with the Trust in some way, close relatives of Trust staff, or people known to the public such as celebrities or politicians. See appendix E.

When incidents occur in relation to loss, damage or unauthorised access to either paper or electronic records, an adverse incident form must be completed and a formal investigation

launched into the incident. The incident must be reported immediately to the relevant line manager and report details of the incident via the Trust's Incident Reporting Procedure.

6.8 Additional guidance for health records and related records

6.8.1 Integrated Records

Integrated or joint care records create additional issues which must be resolved locally. This includes a means of attributing ownership and access to the records between all parties where there is a lawful basis to access the records. These arrangements may include:

- Nominating one organisation to own the record
- Separating the records so that each party retains their own information
- Each party keeps their own record but has access to the shared part of the other record

For each option, some form of patient consent is necessary to enable all parties to access information lawfully. An information sharing agreement is recommended as a mechanism for providing clarity and transparency on the standards that all participants must meet.

6.8.2 Complaints Records

Where a patient or client complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. See the Corporate and DET Records Procedure.

6.8.3 Adopted Persons Health Records

Notwithstanding any other centrally issued guidance by the DH or Department for Education, the records of adopted persons can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used.
Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure.

It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it was considered appropriate to do so, following the adoption.

6.8.4 Health Records of Transgender Persons

A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient. It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

6.8.5 Witness Protection Health Records

Where a record is that of someone known to be under a witness protection scheme, the record must be subject to greater security and confidentiality. It may become apparent (such as via accidental disclosure) that the records are those of a person under the protection of the Courts for the purposes of identity. The right to anonymity extends to medical records. For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person.

6.8.6 Asylum Seeker Records

Any service provided to any client must have a record. For reasons of clinical continuity or professional conduct, records for asylum seekers must be treated in exactly the same ways other care records. Where the asylum seeker is given a patient held record, the provider must satisfy themselves that they have a record of what they have done in case of litigation or matters of professional conduct.

7 Training Requirements

This procedure is available to staff via the Trust intranet. Local induction will address local record management.

Departmental managers are responsible for ensuring that staff in their area understand and follow records management procedures.

8 Process for monitoring compliance with this Procedure

Service Managers are responsible for ensuring compliance with this procedure. If a case file is untraceable or lost, an incident form must be completed and an investigation carried out.

All data loss investigations will be overseen by the Governance Manager and reviewed at the IG work stream meeting reporting to the CQSG.

See the Health Records Audit Procedure for the Trust's approach to records audit.

The Governance Manager will receive an annual report from the General Office Manager on the numbers of archived records which have been held for 20 or more years since last contact that have been destroyed as part of an annual weeding programme and will receive a report by exception if any risks are identified in this process.

The Governance Manager will report on records management and the Trust's compliance with the Records Management Code of Practice.

9 References

- . (2016). Records Management Code of Practice for Health and Social Care. London: Information Governance Alliance
- GMC (2001) Good Medical Practice. General Medical Council, London. http://www.gmcukorg/standards/default.htm HPC, April 2003
- Standards of conduct, performance and ethics: Your duties as a registrant. Health Professions Council, London. www.hpc-uk.org
- Nursing and Midwifery Council, January 2005. Guidelines for records and record keeping. Guidance -01-05, Nursing and Midwifery council, London. www.nmc-uk.org
- Public Records Act 1958

10 Associated documents[3]

- Clinical Governance Handbook
- Prescribing and administration of medication procedure
- Incident Reporting Policy
- Health Records Audit Procedure
- Records Retention Schedule
- Information Governance Policy
- Corporate and DET Records Procedure
- Selection of Records for Permanent Archive Procedure
- Data Protection Procedure
- Email procedure

[3] For the current version of Trust procedures, please refer to the intranet.

Appendix A : Equality Impact Assessment

Completed by	**Jonathan McKee**
Position	**Governance Manager**
Date	**13.7.16**

The following questions determine whether analysis is needed	**Yes**	**No**
Is it likely to affect people with particular protected characteristics differently?		X
Is it a major policy, significantly affecting how Trust services are delivered?	X	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		X
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		X
Does the policy relate to an area with known inequalities?	X	
Does the policy relate to any equality objectives that have been set by the Trust?	X	
Other?		

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then undertake the following analysis:

	Yes	**No**	**Comment**
Do policy outcomes and service take-up differ between people with different protected characteristics?		X	
What are the key findings of any engagement you have undertaken?			Na
If there is a greater effect		X	

on one group, is that consistent with the policy aims?			
If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?		X	
Will the policy deliver practical benefits for certain groups?	X		Will support care for all groups
Does the policy miss opportunities to advance equality of opportunity and foster good relations?		X	
Do other policies need to change to enable this policy to be effective?		X	
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 –seek advice from Human Resources (for staff related policies) or the Trust's Equalities Lead (for all other policies).

Appendix B : Process for Transportation of Hard Copy Records between locations

1.1 Request for original/copy patient records

Original paper or electronic records should never, unless under exceptional circumstances, be provided to other organisations outside of the Trust. If requests for records are received to supply original records, or copy records to patients or other organisations (e.g. solicitors) the request should be referred to the Director Quality who will refer to the Caldicott Guardian, Medical Director and/or trust solicitor as required

1.2 Staff requiring transporting patient paper records should follow the below procedures:

Should staff require taking a set of notes with them for a meeting off site, client/patient appointment in a location other than where the notes are stored, or (exceptionally) to complete a piece of work at home/alternative location due to deadline then the following guidelines should be followed:

- consider if it is at all possible to manage the situation without the records
- consider whether just anonymised extracts of the records would be sufficient, e.g. can a code number be used rather than names?
- consider whether just part of the records can be taken rather the complete file
- If the above not possible the following risk reduction measures should be employed when transporting records:

  a) carry as limited an amount of information possible

  b) carry information on an encrypted memory stick and/or encrypted trust laptop if possible

  c) if paper files are to be transported:

  - Small files small files these should be carried in strong sealed manila envelopes with a fully completed address label on the front (standard address labels will be marked '*PRIVATE AND CONFIDENTIAL'* and addressed to the relevant clinician /Clinical Director in the trust at the Tavistock Centre. The Trust will supply pre-printed labels for these envelopes.

  Note: it is an offence to open a sealed addressed envelope that is addressed to someone other than yourself, unless you have express permission, also it is anticipated that if an addressed envelope is found a reasonable person would put it in a post box)

- Large files these will be carried in grey strong plastic legal file transfer bags, which will also be sealed and addressed as above

d) for transport for bulk documents eg files for Court, these should be transported as above (in sealed containers) in a 'Court bag' eg black wheelie briefcase or rucksack designated for the purpose of transporting documents; this reduces the risk of

documents being muddled up with other non-confidential papers etc that may be in the personal bag of a member of staff

In all cases a log of the file/papers removed from 'base' must be maintained at the site the file is usually held, the person removing and returning the documents should sign them both out and in.

Appendix C: Standards for record keeping treatment

Directorate	Stage in Treatment	Target/Time	Record content standard: individual records
All	All stages All written clinical records	After each contact	• All notes, letters or summaries are typed or written legibly (preferably in black ink because it photocopies well, should case note copies be needed • Each case note entry are dated and signed. • The full patient name and file number are on every page of a report/summary • The date when the report/summary was written or typed is on every page • The signature and printed name of author of each report / summary is recorded. • The profession of the author is stated except on letters to clients/families *(in some situations this may be considered inappropriate)* • All telephone messages stored in patient's files are signed, dated and timed with the patient's name clearly stated
All	During Assessment	ASAP after each session	• As a minimum a brief written entry in record of assessment with date and signature • If patient does not attend a note is to be made in the record of this fact with reason if known (e.g. CBP)
All	Complete assessment	Within 3 weeks of end of assessment	• Assessment forms Specified in the Clinical Governance Handbook and there Trust assessment template, (under 18 or 18+ as appropriate), with all section so the pro-forma completed • Summary should be signed and dated by the author

			• The summary should be validated by the lead clinician if clinician is a trainee
All	Completed assessment	Within 4 weeks of the completed assessment date	Letter to GP and referrer (if different) Content: The communication describing the assessment process should: • Be written in letter form (i.e. not be a set of bullet points). • Include the patient's name, current address and date of birth. • Give the date of the first session. • Give the date of the original referral. • State the number of times the patient has been seen so far. • Give an outline of the main presenting problems * • Give a formulation of the patient's difficulties * • State the likely length and frequency of treatment. • State the Level of Care Programme Approach (as appropriate) and the degree of any risk the patient may pose to themselves or others.
All	During Treatment	ASAP after **each** session	• As a minimum a written entry after each attendance containing brief note of nature and content of session and commenter any changes to circumstances, or changes to risk, or disclosure • If relevant a record should be made of any eternal agencies alerted following session • If patient does not attend a note is to be made in the record of this fact with reasons if known (i.e. DNA, CBP)
All	Termly summary	Patients of have been in treatment for 2 or more months at term end	Treatment review prepared on Trust assessment pro forma, (under 18 or 18+ as appropriate) with all section so the pro forma completed • **Summary should be and dated by the author** • **The summary should be validated by the lead clinician if clinician is a trainee**

All	Termly	At end of each term	Updating letter to GP and/or referrer as appropriate This should be in letter form and contain: • The patient's name, current address and date of birth • The date of the previous letter sent to the referrer • The regularity with which the patient attended the Clinic • The main issues arising from the treatment • The progress of the treatment (e.g. if it has to continue or an end date) • Any change in degree of risk the patient poses to themselves or others and any change in Care Programme Approach Level.
All	Closing Summary	Within 28 days of completion of treatment	Closing summary prepared on Trust closure pro forma. (under 18 or 18+ as appropriate) with all sections for the form completed • Summary should be signed and dates by the author • The summary should be counter by the lead clinician if clinician is a trainee
All	At Closure	Within 1 month of Closure	Closure letter to GP and for referrer containing: This should be in letter form and contain: • The patient's name, current address and date of birth • The date of the original referral • The length of time the patient was seen and the frequency of sessions • The patient's condition on termination (clinical outcome and current formulation) including a note of any residual areas of difficulty, or risk and where appropriate, possible actions should there be a need • An indication of the patient's use of treatment and their benefit. • The availability of re-referral in the future • When the patient is continuing in treatment with another agency a note of this plus where appropriate, their level on that agency's CPA

Directorate	Stage in treatment	Target time	Record content standard: GROUP case records
All	All		Each patient being seen in a group has an individual file containing all patient specific data including: • Assessment • Assessment summary on Trust template • Correspondence • Termly summaries on Trust template • Closure summary on Trust template • Letters to GP/referrer (Post assessment, termly and at closure
All except Portman	Group sessions	Before first group session	A group file will be maintained for each group • For patients attending group sessions, there clinical entry in each patients individual record for each clinical contact. This may be a standard clinical entry regarding the group session, cascaded to each patient record. Such standard entries would not contain personal information regarding group members. • However if there are significant issues relating to specific group members arising in a group session (eg regarding risk) then this should be specifically documented in that individual's care record (and not the care records of other group members)

Appendix D : Responding to a request for access to health records

Background and Introduction

This procedure provides direction to staff about the provision of access to health records for patients and their representatives. This procedure has been written in line with the ICO guidance on access to health records. Patients have a right to the information in their records, which is not the same as having the right to a copy of their records.

Requests can be made on paper or by email.

1.0 Receipt of the request for Disclosure

1.1 All requests will be handled by the Access to Clinical Records Officer, or a deputy

1.1 All requests must be received in writing signed by the applicant, a legally appointed representative of the applicant, or in the case of a child, by someone who holds parental responsibility for the child.

1.3 If the patient is asking to review the records, this request will be passed to the relevant clinician who will consider the request and make arrangements to meet with the patient

1.4 If the patient or his legally appointed representative is asking for copies of records to be supplied the verification and disclosure process detailed below is to be followed.

2.0 Verification of the identity of the data subject

2.1 The Trust has a legal obligation to ensure that it does not breach any data subject's confidentiality. All reasonable steps must be taken to ascertain the identity of the data subject to ensure only the relevant information is disclosed.

2.2 The patient or their legally appointed representative will be asked to provide information to enable the trust to identify the relevant records this will include;

- Name of patient
- Date of birth
- Address registered at the time of contact
- Hospital No /NHS number
- Name of clinician seen

- Approximate dates of contact with the trust

2.3 Verification of Identity

The requestor will be required to provide evidence of their identity (and evidence of their authority to request disclosure if not the patient)

List A
Requestors will be asked to supply a copy of one of the following to support their application:

- Valid passport
- EU photo driving license. Driving licenses that do not have a photo are not acceptable
- EU/ELEA National Identity Card
- Northern Ireland Voters Card (with photograph)
- Firearms or shotgun license (with photograph)

List B
If the data subject cannot provide one of the above, they will be required to supply two documents from list B:

- Benefits or State pension notification letter
- Current UK non-photo driving license
- Blue disabled drivers pass
- All other current signed passports with valid UK Visa not listed above
- UK Birth Certificate (under 18s only)
- National Insurance Card (under 18s only)
- Medical Card/Certificate (under 18s only)

2.4 Verification of Address

List C
The requestor will be required to provide evidence of address in the form of a photocopy of one of the following:

- Bank, Building Society or Credit Union statement (we do not accept statements printed off the internet)
- Current UK non-photo driving license (only if it is not been used as proof of identification)
- Utility Bill/Utility Statement or Certificate/Letter from a supplier of utilities dated within the last 3 months
- Local authority tax bill/council tax bill for current year
- Benefits or pensions notification letter confirming the right to benefit (only if it has not been used as proof of identification)

Prospective requests will not be accepted until the Trust has satisfied itself as to the identity of the requestor.

3.0 Confirmation of authority for those acting on behalf of others

In addition to the information required in section (a) above, those acting on behalf of others will also need to supply written authority from the prospective subject, or an explanation of the circumstances why this is not possible (e.g. parent of a child) , and proof of their identity. Requests received from statutory agencies (e.g. the police or HMRC) or a personal representative (e.g. solicitors) should be accompanied by a signed letter of authority to disclose.

4.0 Details of what is being requested

In addition to verifying identity, the administrator should liaise with the requestor to find out which records they are requesting. For patient requests, we will ask for the reason for disclosure to see if we can assist the patient, however the patient is not legally obliged to tell us the reason for their request.

- Why the information is being requested
- Approximately when they attended the Trust
- Which department were they seen in and name of their clinician if known

5.0 Process for providing access

5.1 Details of the request are sent by the administrator to the relevant senior clinician who should review the record and advice on disclosure.

5.2 If there may be grounds for withholding all or part of the record (see section 6 below) the clinician should consult with the Governance Manager who will provide advice on disclosure.

5.3 The clinician will advise on the format of information to be supplied, e.g. whether photocopies are made or whether the information could be supplied in a different format.

6.0 Grounds for withholding access

Before the patient's health record is released, an appropriate health professional should ensure that they have checked the record and considered if allowing access would result in either of the following:

Could result in serious harm to the physical or mental health condition of the patient, or of any other person.

or

Would disclose information relating to, or provided by a third person (not a health professional), who had not consented to that disclosure.

If either of these applies then the health professional may deny or limit access to the record, there are other unusual circumstances when requests may be declined, contact the Governance Manager for further information. In addition, if the application is for access to a deceased person's record and the record contains information that the deceased person expected to remain confidential then it must remain so.

There is no legal obligation to advise applicants of the grounds on which information has been withheld and, if the fact that all or part of the records are withheld may cause distress to the applicant, there is no obligation to notify the applicant that records have been withheld.

7.0 Responding

7.1 The Trust has a maximum of 40 days in which to respond to requests; this time starts when the requirements in sections 2, 3, and 4 have been satisfied.

7.2 If disclosure is agreed the administrator should arrange photocopy and dispatch of the records, which must be sent recorded/special delivery, or collected in person from the Trust.

7.3 Access Log

A log will be kept by the administrator to record how the Trust is complying with the request.

8.0 Fees

The Trust will waive fees for patients who request access to their records. For requests via third parties, eg from a solicitor or private practitioner, disbursements are charged as follows:-

Health records held totally on computer: A minimum charge of £10 will be charged for pages printed of A4 size at ten pence, and twenty pence for any page other than A4, per printed page, up to a total maximum £50 charge. Where records can be transferred securely electronically, then a flat charge of £50 will be made.

Health records held in part on computer and in part manually: A minimum charge of £10 will be charged for pages printed of A4 size at ten pence, and twenty pence for any page other than A4, per printed page, up to a total maximum £50 charge.

Health records held totally manually: A minimum charge of £10 will be charged for pages printed of A4 size at ten pence, and twenty pence for any page other than A4, per printed page, up to a total maximum £50 charge.

A requestor has three months in which to pay these charges, if no payment is forthcoming, then the request will be deemed to have been withdrawn.

9.0 Correcting a Record

9.1 If, after accessing the record, the patient feels that information recorded on their health record is incorrect then they should be advised to discuss the situation with the health professional in an attempt to have the record amended. If the matter is not resolved they should be advised of the current complaints policy and procedure as outlined in the Complaints Procedure.

9.2 Statements of professional opinion cannot be changed. The Trust suggests in line with good practice that the patient is allowed to include a statement in their record that they disagree with specific parts of their record. The patient could further complain to the Information Commissioner, who may rule that any erroneous information is rectified, blocked, erased or destroyed, or they may seek legal independent advice to pursue their complaint.

Appendix E : Star Case Management

This Appendix is intended to provide guidance on the practice, principles and ethics underpinning the handling of star cases. This includes matters concerning the storage and protection of star case data, as well as who will have access to it.

Allocation of star case status

The status of 'star case' is usually decided at Intake by a panel of senior clinicians. Typical reasons for allocation of this status include staff involved with the Trust in some way, close relatives of Trust staff, or people known to the public such as celebrities or politicians.

If part way through treatment, it is thought that a case needs to become a star case this decision will be made by the senior clinicians in the clinical team meetings.

All new cases should be reported to the Clinical Governance Office.

Electronic Systems

All star cases should be stored "locally" on electronic systems which will mean that they are not connected to the national spine. All star case names should be entered as initials rather than full names The initials should be entered into the first name field and 'STARCASE' should be entered into the surname field.

For example, Ann Person would be entered as: - AP STARCASE

Paper Records

All patient labels should have initials in the place of full names. This includes the labels identifying the file, tracer cards, and labels attached to any paperwork such as outcome monitoring forms. All forms given to the patient should be pre-filled out with initials and a Trust ID (labels or handwritten), to discourage the patient from filling out their own name. Storage and Access

Paper files will be kept locked in a star cases filing cabinets and stored locally. Access to the files will be requested via team managers. Only the clinicians directly involved in the patient's care (any clinicians seeing the patient, plus their supervisor if necessary) and the lead administrator for the service should have access to star case paper records. An audit log developed by Informatics will enable monitoring of the access to electronic records on the Outcome Monitoring System.

Supervision and Teaching

Star cases may be discussed in clinical meetings only if names or particulars of the case do not reveal the patient's identity. If cases cannot be discussed in clinical meetings supervision with a senior staff member should be arranged.

Research and Publication

The use of star cases data with regards to outcome monitoring research will be the same as for other cases as data is not presented on the individual level and any quotes are always anonymised.

Administration

Each Lead Administrator has administrative responsibility for their team's star cases, therefore the rest of the team administrators will not need to access the paper or electronic records. In case of leave or sickness, the senior clinician to whom the case has been allocated will have responsibility for its administration.

Data breaches

Any access of a star case by any person for any reason but for the proper purposes of case management is a breach of the Data Protection Act and must be reported as an incident for which there may be disciplinary consequences. This not only applies to unauthorised persons, but also to authorised persons for unauthorised purpose.

Appendix F : The management of records during the acquisition or divestment of services

Introduction

Once a contract ends, any service provider still has a liability for the work they have done and as a general rule at any change of contract the records must be retained until the time period for liability has expired.

To ensure the continuity of service provision upon termination of the contract arrangements will be made in the interests of patients. After the contract period has ended; the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also be a consideration to identify the legal entity which must manage the records.

Where the content of records is confidential, for example care records, it may be necessary to inform the individuals concerned about the change. Where there is little impact upon those receiving care it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes may require individual communications or obtaining explicit consent. Although the conditions of the DPA may be satisfied in many cases there is still a duty of confidence which requires a patient or client (in some cases) to agree to the transfer.

It is important to highlight the importance of actively managing records which are stored in offsite storage. This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and privacy impact assessments are conducted on the offsite storage providers. The table below summarises some possible scenarios and, for each option, patient consent and an information sharing agreement or a contract may be required to share the information.

Characteristics of new service provider	Fair processing required	What to transfer	Sensitive records
NHS provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign such as signage or posters located on premises	Entire record or summary of entire caseload	na

Non NHS provider from same premises and involving the same staff. This may be a merger or regional reconfiguration.	Light – notice on appointment letter explaining that there is a new provider. Local publicity campaign involving signage and poster and local communications or advertising.	Copy or summary of entire record of current caseload. Former provider retains the original record	na
NHS provider from different premises but with the same staff	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Former provider retains the original record	na
NHS provider from different premises and different staff	Moderate – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider	Individual communications may not be possible so consent of current caseload may need to be sought before transfer. It may not be possible to transfer the record without explicit patient consent so in some cases no records will be transferred
Non NHS provider from different premises but with the same staff	High – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider	
Non NHS provider from different premises and different staff	High – a letter informing patients of the transfer with an opportunity to object or talk to someone about the transfer.	Copy or summary of entire record of current caseload. Orphaned records must be retained by the former provider	

Duties and responsibilities

The transferring organisation has a responsibility to ensure that there are appropriate governance structures in place in the receiving organisation(s) before they transfer any information. The receiving organisation should, as a minimum, have assigned Senior Information Risk Owner responsibilities, have an information governance lead (or equivalent), and have a documented Information Governance Framework. All organisations that process personal information relating to NHS service users or staff should also be completing and publishing an annual IG Toolkit assessment and should have assigned Caldicott Guardian responsibilities. The IG Toolkit provides clear guidance on information governance requirements and on the roles and responsibilities that need to be covered.

Process

a) *Planning*

As soon as is practicable organizations will wish to develop an action plan[2] to outline procedures for destruction, transfer or archival of information. Early planning will help organisations to manage the risks arising during transitions and allow them to:

- identify potential issues at an early stage;
- utilise existing expertise within the organisation;
- understand the resources available to carry out transition related work;
- seek legal and good practice advice where necessary;
- check that Data Protection notification/registration is updated to reflect any new or changed functions;
- identify what information needs to be shared and with whom;
- minimise the impact on those functions which are to transfer, and
- liaise and negotiate with receiving organisations, archives and government bodies.

b) Creating an inventory

In order to effectively manage transition, organisations should produce an information inventory[3] outlining details about the information they hold and how they will handle this information through the transition. Organisations that have already mapped their information flows and have developed a comprehensive information asset register will be better placed to do this and these should form the basis of this exercise (refer to requirements 9-308 and 9-604 of the Information Governance Toolkit for further information). Inventories should contain details about:

- which records are currently held;
- where these records are;
- whether the records are currently active;
- the format records are held in and the equipment needed to read them;
- the appropriate department or contacts with responsibility for the records;
- how old records are;
- what the future of the functions to which the records relate to is;
- the decision for archival/destruction/transfer of record;
- responsibility and mechanism for transferring/destruction of records;
- what information is being shared and with whom.

c) Files closed before the termination or start of a contract

Files of cases closed prior to the start or end date must stay with the provider of that service at the time. Where it is not practicable to separate out inactive records from similar active records then the public interest will justify the transfer of all the records to the new body. Where this involves personal data appropriate steps need to be taken to prevent records being viewed by individuals who do not need to see them, e.g. access controls and/or logical deletion of the inactive records.

d) Personal data security

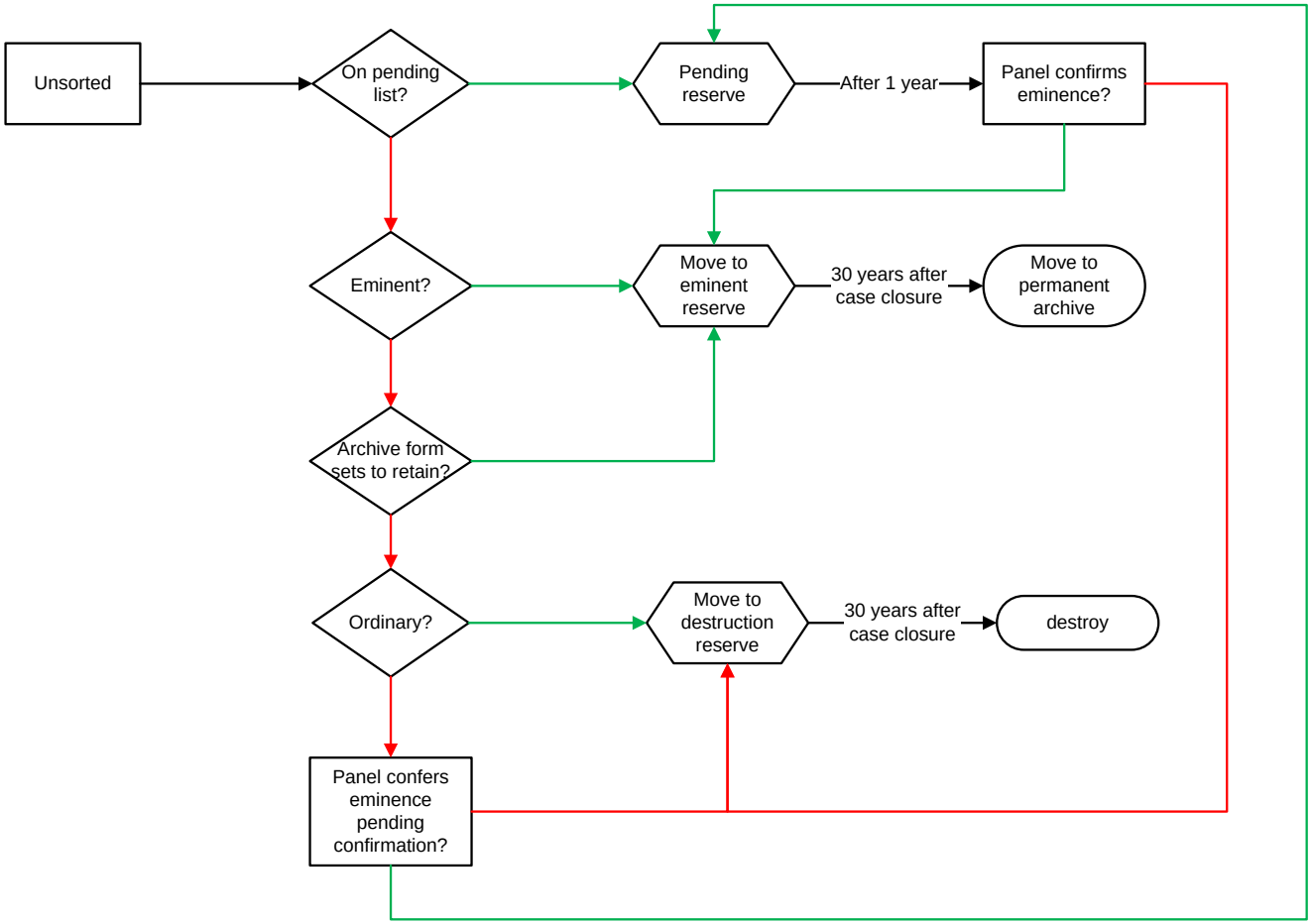
Throughout the transition, organisations must ensure that they adhere to Information Governance (IG) principles. Particular attention must be paid to the handling of identifiable and confidential information, such as that held in health or personnel records, as this information will require extra consideration when archiving, destroying or transferring.

All health records must be passed to an appropriate responsible body before an organisation is dissolved. No personal information, particularly health records, should be left without an appropriate data controller.

Where the information associated with a function includes confidential patient records it is essential that the transfer is tightly managed, the receiving organisation is working with the NHS Information Governance Toolkit and demonstrating a satisfactory level of performance and that there is a communications plan for informing the patients concerned about the change.

Where a change is internal to the NHS, the staff involved are largely the same and patients are unlikely to notice significant change, appropriate communications might be a short information notice being included in the next appointment letter or other communication. Where a change is more significant, e.g. an NHS service transferring to a private sector supplier, it may be necessary to write to each patient to explain the change and who to contact with any concerns and to do this in advance of any transfer.

Appendix G : the selection of clinician's records for permanent archive



Selecting clinician's records for permanent retention