HPFT

Care Records Management Policy

This policy gives guidance to staff on the management of Care Records

HPFT Policy

Version	10
Executive Lead	Executive Director – Innovation and Transformation
Lead Author	Head of Information Rights and Compliance
Approved Date	23/05/2018
Approved By	Information Management & Technology/Information Governance Group
Ratified Date	23/05/2018
Ratified By	Information Management & Technology/Information Governance Group
Issue Date	31/05/2018
Expiry Date	31/05/2021
Target Audience	All staff who have access to care records

Document on a Page			
Title of document	Care Records Management Policy		
Document Type	Policy		
Ratifying Committee	IM&T Senior Managers Meeting		
Version	**Approval Date**	**Review Date**	**Lead Author**
10	23/05/2018	31/05/2021	Head of Information Rights and Compliance
Staff need to know about this policy because -	This policy outlines how clinical information should be stored and archive guidance for care records		
Staff are encouraged to read the whole policy but I (the Author) have chosen three key messages from the document to share:	• The policy outlines which documents should be kept in their original format and which can be scanned and then confidentially destroyed; • The policy outlines the Trusts business continuity plan for when the EPR is unavailable; • .This policy contains the archiving guidance for care records		
Summary of significant changes from previous version are:	Complete review of policy (incorporating the Clinical Information Filing Policy) Reformatting to new template Inclusion of text message guidance		

Contents Page

PART 1 – Preliminary Issues

From 25th May 2018, the EU General Data Protection Regulations (GDPR) comes into effect. This is being incorporated within domestic legislation, which will become the new Data Protection Act (DPA). Until the new Act receives Royal Assent, this policy will continue to refer to either the GDPR or the more generic term of ‘Data Protection Legislation’. For further information, please see the Trust’s Information Governance Policy

1. Introduction

The Care Records Management Policy sets out Hertfordshire Partnership University NHS Foundation Trust’s (hereafter referred to as the Trust) commitment to ensure that all health and social care records are effectively and lawfully managed.

The Trust seeks to meet the *Department of Health’s core standard* for the level of quality for all organisations providing NHS care. The policy is compatible with the requirements of the Department of Health guidelines issued by the Caldicott Committee 1997 and the governmental and legal requirements set out in Appendix 2.

2. Purpose

This policy must be read by all health/social and administrative staff who have access to care records and associated documentation. The policy sets out the main requirements for the management of care records within the Trust.

The Policy is a working document intended to reflect best practice throughout the Trust. It will be updated accordingly to reflect any changes.

Staff must be compliant with all Trust Policies and follow the specific recording requirements detailed within them e.g. Discharge, Care Co-ordination, Complaints and Incidents Procedures.

The term ‘care records’ applies to electronic and paper records and refers to all health and social care information pertaining to the service user, including their:

- medical case notes
- nursing care plans
- CPA documentation
- treatment plans
- correspondence and other similar documentation

It includes any records held as visual or audio recordings, e.g. video and X-rays. This policy outlines the expectations of the Trust for all staff to use electronic patient records (EPR) to support clinical practice.

It encompasses the partnership arrangement within the Trust and is compatible with the policies of Hertfordshire County Council Adult Care Services and Children Schools and Families Service.

i. The Purpose of Care Records

Care records are created and maintained in order to share relevant information appropriately between professionals and to:

- Provide contemporaneous, factual, accurate, comprehensive and concise information concerning the assessment, care and treatment of a service user, and associated observations relating to that person's care.
- Provide a record of any problems that arise and the action taken in response to them.
- Provide a record of all the health and social care interventions undertaken by the Trust staff, including those seconded from other agencies and the service user and carer's response.
- Provide a record of physical, psychological or social factors that may affect the care/treatment needs of the service user.
- Provide a record of the sequence of events and the reason for decisions and interventions made by Trust staff including those seconded from other agencies.
- Provide information which will facilitate communication between staff and there by enable continuity of care.
- Provide information which will support multi-disciplinary care.
- Provide information that will support clinical effectiveness, audit and Health or Social Care research.
- Provide a baseline against which progress can be measured.
- Provide evidence of negotiated care and understanding of the actions agreed between service user or a relative/carer and the health or social care worker.

Where NHS services are provided under contract to the NHS or are being planned or provided with other agencies, the procedures and guidelines set out in this document should be followed.

The Trust is working to a single record for every service user and the use of the EPR will help achieve this national requirement. All information for service users will be collected and stored electronically. However, there is still a requirement to keep certain legal documents in their original format e.g. Medication charts. In general, once most information has been typed, attached or scanned onto the EPR, there is no need to print it out and keep a paper copy indefinitely.

In the event that the EPR becomes unavailable, the Trust business continuity report should be used (please refer to section 9).

3. Definitions

A record is a structured document that contains information, in any media, (including electronic, audio and visual) which has been created or gathered as a result of any aspect of work of NHS employees.

See full glossary in Appendix 4

4. Duties and Responsibilities

The electronic patient record (EPR) is intended to be the ‘primary record’, to replace paper files in the day to day management of service user information. It is the main source of information sharing in the clinical environment.

Each member of staff is individually accountable for updating and maintaining the records of service users on their caseloads, according to their professional role.

a. Duties of the Organisation

The Trust is committed to providing accurate data returns based on the information recorded in the EPR. The quality of this data contributes to the Trust’s performance and it is imperative that all staff assume responsibility for ensuring information is complete, accurate and up to date. (Please refer to the Data Quality Policy).

The EPR will therefore be considered as the most up to date and accurate record available.

The Trust’s Information Security, Information Risk and Email, Internet and Intranet Policies give detailed instructions relating to the security of the Trusts information systems and must also be read in conjunction with these guidelines.

b. The Information Management & Technology (IM&T)/Information Governance (IG) Programme Group

The IM&T/IG Programme Group will operate as a sub-group of the executive team feeding back to the Integrated Governance Committee to ensure sufficient focus is maintained on IM&T and IG issues. The group is accountable to the Trust Executive Board and is responsible for the development and review of the Trust's policies on the management of records (electronic and paper).

The Group works to ensure that the Trust, through its service areas, implements the records management policies and provides guidance on the development and review of local policies and systems.

c. Management responsibility

The Chief Executive and Senior Managers of the Trust are accountable for records management within the organisation and have a duty to make arrangements for the safekeeping of the records.

The Caldicott Guardian is responsible for approving and monitoring national/local guidelines and protocols on the handling, sharing and management of confidential patient information.

The SIRO is an executive Board member who is familiar with information risks and provides the focus for the management of information risk at Board level. He/she must provide the Board with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted for by the organisation.

Managers of services have responsibility to ensure compliance within their areas, making sure records management issues are discussed in supervision and that the Mental Health Services Data Set and key performance targets around records keeping are met. Please refer to the Data Quality Policy. It is an expectation that managers and professional leads are up to date with the EPR system and supplementary reporting procedures and use them to support clinical supervision.

Managers are responsible for maintaining the security of care records in general and for ensuring access permissions for the electronic patient record are appropriate and upheld. They are also responsible for authorising a record to be identified under an alias in accordance with the Alias Procedure available on TrustSpace.

Anyone who records, handles, stores or otherwise comes across patient information has a common law duty of confidence to people accessing Trust services. Such a duty will continue even after the death of an individual.

d. Individual responsibility

Each member of staff is individually accountable for the records of service users on their caseload. All clinicians providing treatment and care for service users are responsible for inputting their own information into the EPR to update their contacts and clinical details.

Administrators and medical secretaries have specific responsibilities to support clinicians within the process; these responsibilities may vary from team to team. Local management should ensure teams are aware of the processes to be followed.

Individuals should make sure:

- The record can be accessed.
- The record can be interpreted.
- It is possible to establish who created the document, during which operational process and how it relates to other records.
- The record can be trusted.
- The record can be maintained through time.
- It is accessible and meaningful in the right format, to those who need to use it.
- There is no unnecessary duplication of care records.
- Any occurrence of duplicate records are immediately reported to the records management /EPR system support team (via the ICT Service Desk)

Individual health and social care professionals are responsible for:

- the content and accuracy of the records they make

- the security and confidentiality of the records in their care
- that information is provided to service users where appropriate to do so.
- the supervision of support staff or others if this role is designated.
- in meeting the standards of their professional organisation

Health and social care professionals are accountable for the entries made by students and unqualified workers under their supervision and should confirm clinical notes to validate the information recorded within 5 working days. Training is available for unqualified staff to assess their competencies to enable them to confirm their own notes.

Health and social care professionals have a duty to:

- keep up to date, and adhere to, relevant legislation and national and local policy relating to information and record keeping.
- keep up to date on best practice for health/social care records and communication practice standards
- be proficient in the system they use to record and communicate health and social care information

Personal details contained in the record must be checked for accuracy and updated accordingly each time the service user attends for an appointment or when changes are known:

- Name
- Address (incl. postcode)
- NHS Number
- Date of Birth
- Contact telephone
- GP details
- No. of dependent children

Details should be confirmed by the receiving member of staff prior to the appointment and any discrepancies amended in the EPR.

Procedures must also be in place for collecting and updating additional data that is required to support the mental health services data set (MHSDS) process. This includes:

- Marital status
- Ethnicity
- ICD10
- CPA tier/level
- Care co-ordinator

Please refer to the Data Quality Policy.

e. Care Co-ordinators

Care Co-ordinators have additional responsibility for managing the process to ensure records are complete and meet the Mental Health Service Data Set (MHSDS) requirements.

f. Medical Staff

Medical staff are supported in their use of EPR by medical secretaries and team administrators who are responsible for:

- booking and confirming appointments
- typing reports and letters in the system
- scanning and attaching relevant information etc.

Medical staff are expected to be proficient in the use of EPR and to access the system to retrieve information and update the medical record. They are responsible for ensuring that the following information is put onto the EPR:

- entering and confirming/saving/authorising clinical notes/case notes
- including ward round and CPA information (where they are the service user's care co-ordinator)
- authorising letters
- updating the medication record
- tracking paper files in the file location on the EPR
- Recording relevant accurate diagnosis in the form of an appropriate ICD10 code.

g. Administrators/Secretaries

Administrators/secretaries have a responsibility to support the clinical team to ensure the care record is accurate and complete. They should expect to receive an appropriate level of instruction from practitioners, who are ultimately responsible for the content of the record and all data quality.

CPA Administrators and MHA Administrators have specific responsibility for maintaining these functions for the team and in doing so, creating and updating the appropriate documents within the EPR. However, it is the Care Co-ordinator who is responsible for providing the necessary information to the administrators.

Administrators/secretaries are responsible for:

- Where appropriate, searching and locating all service user records[1] on receipt of a new referral
- Where appropriate updating existing EPR details and registering new service users onto the system
- creating the file location to reference and track all service user records.
- checking basic data (name, address, contact telephone number and GP) when a service user attends for an appointment
- identifying gaps in the record and inform the relevant clinician as appropriate
- They may also be asked to collect and update the system with information about ethnicity and other data set requirements.
- Identifying duplicate records and notifying the EPR Team via the ICT Service Desk

The following is subject to local implementation.

h. Inpatient Admissions

Inpatient staff are responsible for:

- creating an inpatient episode and a file location document on the EPR
- recording clinical progress and ward round information
- updating relevant and accurate ICD10 diagnosis and medication records, leave, absence and discharge planning
- ensuring the care record is accurate and complete during the service user's admission to hospital and on discharge which includes a discharge summary.

Ward round notes must be added to the EPR, either directly into an appropriately titled clinical note. (Please refer to section *5.2* naming files).

[1] the 'historical' paper record in use prior to the EPR and the secondary paper record (if applicable) used to support the EPR

PART 2 – What needs to be done and who by

5. Records Keeping Standards

Care records are not the property of any individual health or social care professional, or of the service user or carer. They are the property of Hertfordshire Partnership University NHS Foundation Trust on behalf of the Secretary of State for Health.

The Introduction to The National Archives' *Records Management: Standards and Guidance, adopted by the Department of Health,* document states:

"A systematic and planned approach to the management of records within an organisation, from the moment the need for a record to be created is identified, through its creation and maintenance to its ultimate disposal ensures that the organisation has ready access to reliable information. An organisation needs to maintain that information in a manner that effectively serves its own business needs, those of Government and of the citizen, and to dispose of the information efficiently when it is no longer required."

Additionally, effective monitoring of clinical care with high quality systems for clinical record keeping and collection of relevant information is one of the main components of Clinical Governance."

5.1 Clinical Recording

i Record Content

All care records must clearly identify the service user to whom they refer and include:-

- NHS number
- Service user's full name or known as and any known aliases
- Postcode and full address (use postcode look-up facility to insert address)
- Accommodation status
- Telephone number(s)
- Date of birth
- Gender
- Civil Partnership/Marital status (unless service user declines to give this information)
- Next of kin for service users with a Learning Disability
- Named carer where appropriate
- Parent or guardian where appropriate
- Number of dependent children
- Advocate where appropriate
- Details of General Practitioner
- Diagnosis/ICD10 Code
- Employment
- Ethnicity (unless service user declines to give this information)

- First language if not English (with details of need for interpreter)
- Communication needs if there is sensory loss, e.g. signing
- Disability (unless service user declines to give this information)
- Religion where appropriate (unless service user declines to give this information)
- Sexual Orientation (unless service user declines to give this information)

This is not a comprehensive list. Personal details must be checked for accuracy with service users and carers at every appropriate opportunity.

Clinical notes must be entered at the time the care is provided (within the standard of 2 working days). Where this is not possible and there is a significant delay in recording the information, an explanation should be added at the start of the note, giving the reason for the delay and the date and source of any original notes taken.

A clinical note is completed to ensure reference is made to relevant scanned documents or attachments.

Records are created with the involvement of the service user or their carer wherever possible.

Some services may attach a photograph of the service user for identification purposes. The service user's consent must be sought before taking a photograph.

For further information please refer to the: Audio/Visual Recordings of Service Users, the use of One Way Screens and the use of Closed Circuit Television (CCTV) within Wards/Units (Policy, Guidance and Standards)

Each document must include a header with service user's name, date of birth, NHS number and person responsible for the individual's care.

The care record must contain a designated place for the recording of hypersensitivity reactions and other information relevant to professionals involved in the care of the service user e.g. Advance Decisions. Alerts are categorised to inform about risk to the service user and others.

The Care Plan/Wellbing Plan/Care Programme Approach/Person Centred Plan is readily identifiable.

Relevant copies of Mental Health Act/legal documentation is readily identifiable.

Records must be recorded in English, clearly, legibly and in a printable format if required for access to records purposes.

Alterations to a clinical note are acceptable however, the original entry can still be viewed in version history and audit trail will be created.
Please contact the Business Application Support Team for further information/assistance.

All entries must be accurate and up to date.

Clinical notes and reports must be saved by the clinician at the time of writing. If notes are entered by a secretary or non-registered professional member of staff, they should be checked and authorised by the authorising clinician/supervising staff within 5 working days. Team leaders/clinical supervisors may delegate the entry of notes/reports to non-professionally registered members of staff working in clinical roles without additional authorisation being required for each entry, if the non-professionally registered member of staff has been assessed as competent to do so.

Jargon and abbreviations must not be used.

All information should be clear and unambiguous, factual, consistent and accurate**.** Relevant, non-factual entries e.g. conclusions or opinions may be recorded and should be indicated as such. Meaningless phrases, irrelevant speculation or offensive comments about the service user, their relatives, or other individuals must not be used.

Please refer to the Information Commissioner's Data Protection Good Practice Note – *"How does the Data Protection Act apply to professional opinion?"* This is available on Trustspace.

Telephone contacts and relevant emails should be recorded in the record as a clinical note.

All information that originates from within the Trust, e.g. notes, reports, assessments, etc., should be in the EPR; copies of information held in a contingency must be available within the EPR.

ii Observation Charts

To reduce the amount of administration time spent scanning, the observation sheets are to be kept in a separate file and summarised in the EPR at the end of each shift. The folder containing the observation sheets should be added to the file location in the EPR. Observation charts form part of the service user record and therefore the same retention and disposal guidelines to a care record apply.

iii Daily Food and Fluid Chart

The daily food and fluid charts can be kept with the observation charts. A clear divider should separate the forms and the file should be labelled appropriately. An entry must be made in the EPR to indicate that a daily food and fluid chart has been completed. This can be summarised in a sentence as a clinical note (in the EPR) at the end of each shift. As above, the same retention and disposal guidelines apply.

iv Prescription Charts

Prescription charts should be scanned onto the EPR and checked to ensure they are a true and legible copy of the original. The original prescription chart must be kept and filed appropriately within the unit, reference to the location of the original must be recorded in the file location on the EPR

v Scanning Information

Some staff have expressed concerns that a scanned document will not '*stand up'* in court if required as evidence[2]. Part 1 of the Department of Health's Code of Practice on Records Management confirms that scanning is an acceptable practice within organisations.

The NHS Litigation Authority (NHSLA) also clarified that scanning and the destruction of the original paper record, is acceptable as long as the following standards are met:

- The retention of the records (as per Part 2 of the Records Management Code of Practice) must be adhered to.
- A full audit trail is required to identify when the original paper record was scanned.
- The scanned copy is complete and legible and a true copy of its original.

Please note: Scanned documents must be kept to a minimum because they impact on the performance of the EPR and in most cases documents in their entirety are not needed e.g. case notes could be created to contain relevant information as opposed to a full document being scanned. Scanned documents must be added to the EPR as a .pdf document (not .gif or.jpeg) to prevent clogging up the system.

If the scanned image is *not* complete and legible, the original should be filed in referenced in a clinical note.

Handwritten notes must not be scanned as they are often very difficult to read and in some cases illegible.

The following documents can be scanned with the original(s) being shredded (unless stated otherwise):

- **Referral letters**
- **Clinical reports from other organisations** that relate directly to the service user's secondary mental illness *(all other reports should be referenced in the EPR and where appropriate, a summary provided in the clinical note.*
- **Investigations/path lab results** (If not received electronically)
- **Received correspondence** directly relating to the service user's spells e.g. solicitor's letters.

Particular attention should be given to the reports described below as they may not scan clearly onto the EPR (however all documents must be checked after scanning):

[2] Remember, Legal documents (e.g. Mental Health Act, child protection and consent to treatment papers) need to be retained in their original format because of legal requirements. These documents are scanned and attached in the EPR, for ease of access, with the originals filed in the appropriate section of the service user's contingency file.

- **X- rays**
- **Ultrasound Scans**
- **ECG Print Outs**
- **CT Scans**
- **ECT Print Outs**

All other information must be entered and updated directly into the EPR. This includes:

- **Clinical/case notes**
- **Diagnosis/ICD10**
- **CPA**

vi Recording incident information in the Electronic Patient Record (PARIS or PcMIS)

In addition to completing a Datix form the staff member reporting the incident must make a contemporaneous factual accurate comprehensive entry of the incident description and actions taken in the EPR referencing the Datix web reference number generated at the time of reporting. See Incident and Serious Incidents Requiring Investigation Policy

vii Text Messaging

Pagers/text messages must not be used to convey service user information unless the service user has specifically consented to this service. This consent **must** be documented on the EPR. Any text messages that are received *from* or *sent* to a service user must be recorded as a clinical note. These messages will become part of the clinical record and should be recorded as such.

5.2 Naming Files

Naming conventions are standard rules to be used for naming both electronic files and folders. Using the Trust's naming convention will help to identify documents more quickly. The following rules must be followed when entering documents onto the EPR.

a) *Specific* information should be recorded when naming a document e.g. describe the content of the document. This should not just be a repeat of the folder name.

b) *Logical* information should also be captured e.g. the date and name of the person who created the document. The date must be the date the document was created and *not* the date it was entered onto EPR.

c) Each file must have:

- a unique name to each document
- a meaningful name which closely reflects the record's content

- express elements of the name in a structured and predictable order
- locate the most *specific* information at the beginning of the file name and the most *logical* at the end.

d) Documents should be named using the following convention to ensure that documents are in date order and are easy to locate in electronic form:

- Date in the format YYYY MM DD
- Document title – (containing version number if applicable)
- Authors initials in brackets
- Leave spaces between each entry e.g. 2018 04 26 Care Records Management Policy V1 (SW)
- Please note: The use of dots and slashes can change the format of the document and should therefore be avoided.

5.3 Entries by Service Users

As part of the service user's participation in the care process, they may wish to write about their experiences e.g. following rapid tranquillisation. These notes should be created on separate sheets and scanned onto the EPR. The notes should be signed and dated by a member of staff (the EPR will create a permanent audit trail).

5.4 Entries by other agencies

All integrated services should use the same health record.

There must be a single record for all relevant staff to access. Where there are additional paper files (e.g. historical notes) these must be referenced using the file location document on the EPR. Please refer to Paris User Guide.. See also Section 7.2 Transferring Paper Records and 8.2 Tracking Records.

5.5 Mental Health Act Administration (MHA) and Legal Documentation

Original Section 17 leave forms must be retained within the unit. The unit must ensure the original is scanned to the EPR. When the Section 17 form has expired a diagonal line must be drawn through the form and subsequently scanned to the EPR following which it may be destroyed.

All original legal MHA documentation must be sent to the MHA office at Kingsley Green who will scan the documentation to the EPR. The ward/unit must retain copies of legal MHA documentation within the service user paper file until no longer required prior to sending the originals to the MHA office.

Certain other documents **must** be retained in their original format as a legal requirement. These documents should be scanned and attached in the electronic record for ease of access, with the originals filed in the appropriate section of the service user’s contingency paper record. For example:

- Child Protection documents
- Consent to Treatment
- SAP Documentation signed by Service User/Carer
- Prescription Charts, Transfer/Discharge Forms for medication

5.6 Alerts/Warnings

An alert/warning is used to inform, any of the following (including but not limited to):

- an advance decision is in place
- 'Child looked after'
- Child subject to a protection plan
- Information sharing restriction
- Personal Safety
- Risk of Allegation
- Adult is subject to safeguarding
- Violence

Alerts should be created in the EPR and consideration should be given as to the risk to the individual and others.

The first Principle of the Data Protection Law states that the processing of information must be fair and lawful. Alerts should be based on a specific incident and/or a particular concern of a professional and not a general opinion of an individual. In order to be fair to the service user, they should be informed that an alert has been added to their record. There may be cases whereby informing the service user that an alert has been placed on their record will not be considered to be in their best interest for example, if a service user is considered 'violent' and an alert is placed on the record to reflect this, telling the service user may increase the risk of further violence. The care co-ordinator/lead professional must record why the decision not to inform them of the alert was taken. All decisions must be made on a case by case basis.

Reviewing Alerts

Data Protection Law states that personal information should not be kept longer than necessary. Alerts entered into the EPR will be reviewed when a risk assessment is reviewed/updated. The risk assessment should state the need for an alert as part of the risk management plan.

Alerts must not be left on the EPR without being reviewed and a reason given as to why the alert is still relevant. Alerts should be reviewed as part of the CPA review as a minimum and more frequently as part of the service user's care review by the multi-disciplinary team.

The alerts will however remain on the service user's care record and form an 'alert history' for future reference.

You may also refer to the Data Protection Good Practice Note on 'The Use of Violent Warning Markers' issued by the Information Commissioner's Office.

5.7 Audit

Audit is part of the risk management process and audits will be undertaken to assess the quality of record keeping standards to ensure an on-going programme of improvement. The audit should be multi-professional. The toolkit is separated into three areas:

- Structure, content and presentation of the contingency record and its effectiveness as a contingency file when the EPR is not available
- Data collected and stored on the EPR (and in line with the records keeping policies)
- General records Management

The Trust's records management processes are monitored by the following national standards:

- CQC Standards Regulation 17
- Information Governance Toolkit
  - Confidentiality & Data Protection
  - Clinical Assurance
- NHS Litigation Authority Risk Management Standards
  - Health records Management standards: 1.1.7; 2.1.7; 3.1.7
  - Health records keeping standards: 1.1.8; 2.1.8; 3.1.8

A copy of the Care Records Management Audit League table is available on Trustspace.

User login ID and password creates the electronic record signature. It is essential that each person making an entry in a record can be traced using their unique identifier, e.g. electronic password.

Managers should regularly use reports available from SPIKE to ensure staff are complying with the standards set.

The outcome and recommendations of the records keeping audits will be reported to the:

- The IM&T/IG Programme Group
- Managing Directors of Strategic Business Units (SBU)
- Service Line Leads
- Managers of local teams
- Operations Committee

The Information Rights and Compliance Team will follow up the records keeping audits with service areas and individual teams in order to improve performance and meet the standards outlined in this policy. Action plans will be developed for the team manager to take forward.

6. Security

Everyone has the right to expect their care records to be maintained under the strictest security and that the information contained within them will remain confidential between the service user and the Trust, for the sole purpose of carrying out its core business.

All staff employed by the Trust, whether on permanent or short term contracts, are expected to abide by the Trust's confidentiality and data protection policies. They are responsible for their own code of conduct as indicated by their professional organisation.

They must have and use their own unique log in ID. Passwords must not be shared or the EPR accessed on behalf of another member of staff at any time. Users must always close down all records and log out of the system immediately after they have finished their work.

Passwords and User ID's are issued following the completion of a 'Computer System Access Request' (CSAR) form which is completed by the appropriate manager, on line via the intranet to the ICT Service Desk. This will form part of the recruitment process for new employees, to enable training to be completed during induction.

When access needs changing the Computer Systems Access Amendment form (CSAA) must be completed on line to facilitate staff movement from one team to another.

There is a separate procedure for solicitors, auditors and other agencies requiring access to care records. They must only view records under the supervision of a senior member of staff. Please refer to the guidelines for 'Authorised Visitor Access' which is available on Trustspace.

At no time should a visitor (professional or otherwise) be given direct access to the electronic record using a member of staff's password. This contravenes all confidentiality, information sharing and Caldicott principles.

For further information on security issues please refer to the Information Security Policy.

7. Access to Information Recovery of the EPR

The EPR is intended to provide 24 hour access to service user information. If the system is unavailable for maintenance purposes, at least 48 hours' notice will be provided to all users, so that the 'Computer Access and Recovery Procedure' can be implemented.

All information recorded about a service user during the system downtime must be transferred to the EPR as soon as it is functioning. For guidance on how to do this, refer to the Computer Access and Recovery Procedure available on the intranet.

If you are unable to view information that you have created, call the Business Application Support Team via the ICT Service desk, do not re-enter.

Service users must not be given a password or access to the EPR system. However, good practice is to explain to the service user what information will be recorded. This can be particularly useful during care reviews. However, some service users may disagree with what is recorded even if it is factually correct. The detail should still be entered in the clinical note, recording the service user's conflicting views where appropriate. Please refer to the Protection and Use of Service User Information Policy .

Formal requests for access to care records by the service user or their representative should be made in writing to the Information Rights and Compliance Team.

7.1 Storage/Filing

Records should be stored chronologically, the most recent records accessible first.

Storage arrangements must allow for retrieval on a 24 hour/7 day arrangement in areas where there are emergency admissions. **(Please refer to the Trust's Care Records Archiving Procedure – Appendix 5)**

Information printed from the EPR should be confidentially destroyed using the confidential waste bins once it is no longer required – after updating the EPR with any changes. Handwritten notes and messages can also be destroyed once the information has been transferred to the EPR. Please see section 8.4 Destruction of Records.

There must only be one electronic record for a service user. If duplicate records are identified in the system the Business Application Support Team must be notified immediately via the ICT Support Desk so the records can be merged.

7.2 The Transfer of Care Records

This section covers the transfer of care records by courier or mail as either paper records (e.g. the 'historical' paper record – the paper record used prior to the implementation of an EPR), or electronic media e.g. CDs or microfilm and the electronic transfer of care records via email.

Records in Transit:

- Any portable equipment taken off premises or paper records containing person identifiable or other confidential information must not be left in cars or any other unsecure location and must be used only by authorised persons. Password control must be strictly maintained.
- If paper records are delivered to another location they should be enclosed in envelopes or secure bags/wallets and sealed for transfer.
- Records that may be damaged in transit should be enclosed in suitable padding or containers.
- For larger quantities, records should be boxed in suitable boxes or containers for their protection.
- Each transit container (box or envelope) should be addressed clearly and marked confidential with the senders name and address on both back and front of the transit container (box or envelope).
- Records should be packed carefully into vehicles to ensure that the movement of the vehicle will not damage them.
- Vehicles must be fully covered in order that records are protected from exposure to weather, excessive light and other risks such as theft.
- No other materials that could cause risks to records (such as chemicals) should be transported with records.
- Safety of staff must be taken into account when transporting records.
- Records must be hidden from the public eye at all times.

7.2.1 Mailing records

There are various options for mailing records such as recorded delivery, registered mail etc. When choosing options staff should consider the following:

- Will the records be protected from damage, unauthorised access or theft?
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality of the records?
- Does the mail provider offer ‘track and trace’ options and is a signature required on delivery?

7.2.2 Transferring Paper Records

The ’file location’ in the EPR must be used to record all existing paper records relating to a service user. If the location of the record changes e.g. it is transferred to another unit, the file location must be updated. The ‘referring’ team is responsible for updating the file location field in the EPR. The ‘receiving’ team must then update the file location with further ‘specific’ details of where the record will be stored e.g. in locked filing cabinet in Room 401.

Please note: when transferring records from one team to another, you can overwrite or add detail to the entry concerned, do not create another entry as this will look like there are duplicate records.

Instructions on how to use this facility is in the PARIS User Guide which is available on the intranet.

7.2.3 Emailing Records

When emailing patient identifiable information, staff must establish whether the recipient of the e-mail can receive the information in a secure manner. Patient information has to be encrypted. Corporate e-mails (nhs.net emails) are automatically encrypted by the system.

Corporate email relates to Hertfordshire Partnership University NHS Foundation Trust (HPFT) sending to the following organisations (please note this list is not exhaustive):
Hertfordshire Community NHS Trust (HCT),
Hertfordshire County Council (HCC).
East & North Herts Clinical Commissioning Group CCG (ENHCCG)
Herts Valleys Clinical Commissioning Group CCG (HVCCG)
Central Eastern Commissioning Support Unit CSU (CECSU)

If both parties have access to the EPR, record the information in the service user's care record and make contact by telephone or notification to direct the person to view the appropriate entry.

Guidance on the use of e-mail when sending person identifiable or confidential information is available on Trustspace, please refer to the E-mail, Internet and Intranet Policy .

7.2.4 Transfer of care records to another team within the Trust

When referring a service user to another team e.g. inpatient services, the referring team is responsible for updating the 'location field' in the EPR to enable the receiving team to view the record. This must happen as part of the transfer process, before the service user is seen at the new location.

If the 'historical' paper record is also transferred, the referring team is also responsible for updating the 'File location' field in the EPR (see PARIS User Guide on Trustspace)

7.2.5 Reporting mechanism

Care records must be stored in such a way that whether the record is currently in use or has been transferred to an archive/storage facility, there is a robust tracking system that:

- Identifies the person responsible for the care record if it is removed.

- Provides details of the expected date of return (where appropriate)
- Has an alert mechanism if the expected date of return is not met.
- Has the capacity to enquire if the care record is not returned by the due date.

7.2.6 Risk Management

It is the health professional's decision based on clinical judgement and risk assessment whether or not to see a service user in the absence of their care record.

7.2.7 Procedure for non-availability of a record

Following the request for a care record which cannot be found, the person who is responsible for providing the record should follow the procedure below.

- Make a thorough local search which includes double checking the tracking system to confirm it cannot be traced.
- Check the record has not been misfiled, is awaiting filing or in the case of an electronic record has been recorded incorrectly on the computer. Check any known aliases as the record may have been registered under a different name.
- Enquire whether a copy of the required record is available in another location e.g. progress notes of the health professionals involved.

If the above is not successful a report should be made to the line manager and for Mental Health Services, the Directorate Manager.

If the notes are found in the short term, action should be taken to prevent a reoccurrence. If the notes are unavailable in the long term, the Untoward Incident/Accident Procedure (via Datix) should be instigated by the person who discovers they are permanently lost. Please refer to the Learning from Incidents Policy.

If the record is not available following a request by the service user or their representative for access to records, a letter of apology should be sent following the HPFT Complaints Procedure.

Refer also to Section 9.d.iii Accidental destruction of records.

7.2.8 EPR system unavailable

Please refer to the Computer Access and Recovery Protocol which is available on Trustspace.

7.2.9 Monitoring of the protocol and review

Statistics regarding lost or unavailable care records will be monitored yearly by the Trust IM&T/IG Programme Group. Requests for more in-depth audits will be made by the group as appropriate. Teams should carry out local audits on a quarterly basis.

8. Preservation, Retention and Destruction of Service User Records

This section sets out the minimum retention periods for care records and gives advice on the long term storage of care records, the selection process of records for destruction and destruction methods.

- Each service must define a responsible person who works in conjunction with the Information Rights and Compliance Team with regard to the preservation, retention and destruction of care records.
- Each service area has a legal requirement to store records including 'historical' and contingency records for a statutory period of time.
- Nursing, medical and other records e.g. AHP records are filed together or referenced when the service user is discharged from inpatient care.
- All service areas with 'non-active' service user records must follow the Trust's Care Records Archiving Procedure which is available on Trustspace.
- Joint records i.e. those between Hertfordshire County Council and the Trust, are archived, stored and destroyed by the Trust following the Retention and Destruction Schedules.

8.1 Archiving and locating "Historical" Paper records

Professionals involved in the care of a service user should have access to all information relating to the individual. This may mean looking at information recorded in the 'old' paper record dating back some years. It is essential the whereabouts of these records are recorded on the EPR system.

Record storage methods must:-

- be secure to prevent breaches of confidentiality i.e. kept in locked filing cabinets or a locked room.
- not compromise the physical safety of service user, staff or visitors
- be safe from damage from fire, damp, water e.g. in fire proof cabinets, stored off the floor, stored at a temperature between 13^{o}C and 18^{o}C, stored at a humidity of between 45%-65%.
- ensure electronic storage media is safe from damage which may corrupt the media e.g. strong magnets will damage video/audit tapes.

8.2 Tracking Paper Records

The "File Location" in the EPR must be used to record all existing paper records relating to a service user. This will include any historical paper records relating to an individual as well as those in use prior to the implementation of an

EPR and the contingency record. It will help to create a ‘virtual’ single record for each of our service users.

The manager of each unit must be aware of where records are archived/transferred and by what method. It is essential that a ‘tracking’ system is in place to ensure that if the records are required for any reason at a later date, they can be traced. The ‘file location’ on the EPR system should be used to track the historical paper record relating to a service user (see relevant EPR training manual/user guide for details on how to use the file locations). This includes transferring records to the Trust’s approved off-site storage contractor when sending records to be archived for medium to long term storage.
(See also 7.2.ii Transferring Paper Records)

When using the Trust’s approved off-site contractor (see the Trust’s Archiving Procedure) the service must ensure that a process is in place to review and arrange for disposal of old records in line with Trust policies, Department of Health guidelines and in compliance with the Public Records Act.

8.3 Standards for the Electronic Archiving of Records

8.3.1.1 The technical issues of electronic archiving of records need to be addressed on a case by case basis.

8.3.1.2 The archive medium must be one which is forward compatible (will not become obsolete with the introduction of new technology).

8.3.1.3 The paper record must be retained when:

8.3.1.3.1 there is a reasonable probability that the service user will be re-referred or re-admitted.

8.3.1.3.2 there is a likelihood of any complaint or legal action requiring the disclosure of documents in the care record. Care records for an individual should be risk assessed to ascertain whether this is a possibility in the future.

For legal admissibility purposes, digitisation of records should follow an agreed and documented process. This should cover:

- the software and hardware used
- the media e.g. CD, DVD, microfiche to be used and the format of the digital records on the media.
- the format must be an accepted industry standard.
- The media must be "read only"

8.3.1.4 Format and content of the audit log. As a minimum it should record:

- Date and time digital record created.
- Name/identity of operator
- Care records digitised
- Number of copies created.

Note that the audit log will form part of the supporting evidence for legal admissibility.

8.3.1.5 Each care record should be contained in a separate, clearly identified, electronic folder. If more than one disc is used each disc should be clearly labelled.

8.3.1.6 There should be a master copy and a working copy for use when access is required.

8.3.1.7 The master and copies must be clearly labelled.

8.3.1.8 The retention and disposal date must be the same on all copies and marked on each copy.

8.3.1.9 An audit log of all access to the master copy must be maintained. This will include creating working copies and accessing the care records.

8.4 Destruction of Records

A system for the destruction of files beyond their retention date should be set up, thus ensuring unnecessary records are not kept past their statutory period unless there is a particular reason e.g. legal and also to keep storage space down to a minimum.

The selection of records for destruction/review at the end of the retention period should take place where possible in consultation with the relevant health/social care professional.

Destruction of electronic, paper and microfilm records must be in a manner which ensures continued confidentiality.

Paper or microfilm records should be ‘cross’ shredded either on site if the unit has an appropriate shredder or by the licensed contractor approved by the Trust.

The contractor provides lockable bins delivered directly to the unit for staff to fill with any confidential material, staples and paper clips do not need to be removed. When the bins are full the contractor will collect them in a secure vehicle for industrial shredding.

A certificate of destruction specifying the exact weight of the content of the bin will be issued to the site once the content has been shredded.

Records must not be placed in clinical waste bags for incineration.

Electronic media such as CDs or DVDs should be destroyed by physically breaking them in two.

Please note: A log of destroyed records must be retained by the manager and a copy sent to the Information Rights and Compliance Team (please refer to the Care Records Archiving Procedure for a log sheet).

When sending records for archiving to the Trust's approved off-site storage provider, it is a requirement to record the destruction/review date. When a file/box of records has met its destruction/review date, the relevant team manager will be contacted to review the records and confirm if they can be destroyed. A destruction certificate will be issued.

8.5 Retention Schedule for Health and Social Care Records

All NHS records are public records under the terms of the Public Records Act. For details of retention periods for non-health/social care records refer to the Trust's Corporate Records Management Policy.

Dates should be calculated from the end of the calendar year of the last date of entry.

8.5.1 Minimum retention periods for Health/Social Care Records

These are based on the Department of Health & Social Care recommendations[3].

Full information is given in Records Management Code of Practice.

8.5.2 Decisions to increase the Retention Period

It is important that decisions to increase the retention period take account of the care needs individual to the service users, and of future research and audit requirements.

Reasons for the retention of records beyond the periods recommended by the Department of Health & Social Care will include:

- Care related to 'whole-life' issues such as learning disability, multiple development disorder
- Unusual diagnoses or treatments
- Treatment within research programmes

[3] https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

- Planned audit programmes
- A care history which has included formal complaint and/or litigation

Where the care team has made a decision that records are to be retained, the front cover of any historical paper records must be stamped, using a red ink pad. The stamp should state the name of the Trust, the words **'Do Not Destroy'** and be signed and dated by either a consultant or senior manager within the service. The decision should be reviewed at 5 yearly intervals and a review date written in the stamped area.

An alert on the electronic record must also be created.

8.5.3 Accidental Destruction of records

If an accident happens and records are damaged beyond restoration e.g. due to a water leakage, the following action is advised:

- Check which documents have exceeded their retention period and dispose of these. Details of retention periods can be found on the intranet.
- Contact the Head of Information Rights and Compliance immediately with details of the damaged records; it may be possible to send these records off to an external contractor for restoration work.
- List the names of the service users whose files cannot be saved and where possible the title of the documents and dates so there is a record of what has been lost. This information needs to be attached to the new file or an existing main file.
- For current service users, the document may be replaceable from another source, e.g. copies of reports/assessments in the main service user file or copies saved on computers.
- Depending on how the damage occurred, put in place action to prevent a reoccurrence.

9. Business Continuity

A contingency plan must be in place should the EPR become unavailable so staff can access *specific* service user information to enable care to continue. For most teams, this will be a combination SPIKE reports printed or stored on an encrypted USB memory stick.

The reports will contain the demographic information for each service user (along with alerts, GP details and carer details), the care plan/wellbeing plan and risk assessments.

Please note: The business continuity report is only to be used when the EPR is unavailable and should **not** be used as a day-to-day reference source

Business continuity reports should be run once a week as a minimum (or as often as your service requires).

The reports use SPIKE to pull information directly from the EPR system, Paris. The essential information that will be displayed has been deemed necessary to provide short term emergency care to service users in the event that the EPR becomes temporarily unavailable. As this is a live report, the accuracy and amount of information available on the report will solely rely on the quality of data entered on Paris.

This updated report style contingency is quick and easy to maintain, will increase valuable clinical time and improve the robustness of the backup information we hold about service users in the event of an IT outage.

Please refer to the SPIKE User Guides on Trustspace for futher information.

10. Training / Awareness

Course	For	Renewal Period	Delivery Mode	Contact Information
Care Records & Confidentiality Training	Managers and Clinicians	Every 3 years	E-learning	In order to obtain OLM e-learning login details please contact the Learning & Development Team: Learning@hpft.nhs.uk
Information Governance/Data Security Awareness	All staff	Annually	E-learning Classroom	
EPR Training	All staff			

11. Embedding a culture of Equality & RESPECT

The Trust promotes fairness and RESPECT in relation to the treatment, care & support of service users, carers and staff.

RESPECT means ensuring that the particular needs of ‘protected groups’ are upheld at all times and individually assessed on entry to the service. This includes the needs of people based on their age, disability, ethnicity, gender, gender reassignment status, relationship status, religion or belief, sexual orientation and in some instances, pregnancy and maternity.

Working in this way builds a culture where service users can flourish and be fully involved in their care and where staff and carers receive appropriate support. Where discrimination, inappropriate behaviour or some other barrier occurs, the Trust expects the full cooperation of staff in addressing and recording these issues through appropriate Trust processes.

Access to and provision of services must therefore take full account of needs relating to all protected groups listed above and care and support for service users, carers and staff should be planned that takes into account individual needs. Where staff need further information regarding these groups, they should speak to their manager or a member of the Trust Inclusion & Engagement team.

Where service users and carers experience barriers to accessing services, the Trust is required to take appropriate remedial action

Service user, carer and/or staff access needs (including disability)	(a) All service users (carers/advocates) should be kept informed that information is being recorded, why it is being recorded and who it may be shared with at their first appointment or soon after. (b) If they are not fluent in English, the services of an interpreter should be sought. The specific needs of people with impaired hearing or a learning disability, and those of young people, should be met. The Trust policy on "Communicating with Diverse Communities" provides further guidance. .
Involvement	As per (a) above. Service users can request access to their information under section 7 of Data Protection Legislation via a formal subject access request.
Relationships & Sexual Orientation	Explicit consent must be sought from the service user before any information from the care record is shared with nearest relatives, families, partners or carers.
Culture & Ethnicity	See (b) above.
Spirituality	When this policy is followed, the Trust can be sure that all health and social care records are effectively and lawfully managed. It will have the same effect on all groups of people.
Age	When this policy is followed, the Trust can be sure that all health and social care records are effectively and lawfully managed. It will have the same effect on all groups of people.
Gender & Gender Reassignment	When this policy is followed, the Trust can be sure that all health and social care records are effectively and lawfully managed. It will have the same effect on all groups of people
Advancing equality of opportunity	When this policy is followed, the Trust can be sure that all health and social care records are effectively and lawfully managed. It will have the same effect on all groups of people

12. Promoting and considering individual wellbeing

Under the Care Act 2014, Section 1, the Trust has a duty to promote wellbeing when carrying out any of their care and support functions in respect of a person. Wellbeing is a broad concept and is described as relating to the following areas in particular:

- Personal dignity (including treatment of the individual with respect);
- Physical and mental health and emotional wellbeing;
- Protection from abuse and neglect;
- Control by the individual over day to day life including over the care and support provided and the way in which it is provided;
- Participation in work, training, education, or recreation;
- Social and economic wellbeing;
- Domestic, family and personal;
- Suitability of living accommodation;
- The individual's contribution to society.

There is no hierarchy and all should be considered of equal importance when considering an individual's wellbeing. How an individual's wellbeing is considered will depend on their individual circumstances including their needs, goals, wishes and personal choices and how these impact on their wellbeing.

In addition to the general principle of promoting wellbeing there are a number of other key principles and standards which the Trust must have regard to when carrying out activities or functions:

- The importance of beginning with the assumption that the individual is best placed to judge their wellbeing;
- The individual's views, wishes, feelings and beliefs;
- The importance of preventing or delaying the development of needs for care and support and the importance of reducing needs that already exist;
- The need to ensure that decisions are made having regard to all the individual's circumstances;
- The importance of the individual participating as fully as possible;
- The importance of achieving a balance between the individuals wellbeing and that of any carers or relatives who are involved with the individual;
- The need to protect people from abuse or neglect;
- The need to ensure that any restriction on the individuals rights or freedom of action that is involved in the exercise of the function is kept to the minimum necessary.

13. Process for monitoring compliance with this document

Action:	Lead	Method	Frequency	Report to:
Care Records Management Audit (internal)	Head of Information Rights and Compliance	The audit looks at the EPR and its interaction with the Trust's Standard "Secondary" Paper Record Folder as well as the records management and data quality.	Annually	IM&T/IG Programme Group, Practice Governance and Caldicott Guardian

13.1 Responsibilities for conducting the monitoring/audit

There will be yearly audits of the quality of record keeping standards to ensure an on-going programme of improvement (also refer to 8.3). The Information Rights and Compliance Team will follow up the records keeping audits with service areas and individual teams in order to improve performance and meet the standards outlined in this policy. Action plans will be developed for the team manager to take forward. The Information Rights and Compliance Team will monitor the progress of the action plan on a half-yearly basis. Any concerns will be raised at the IM&T/IG Programme Group and taken forward by the appropriate service manager.

The Record Keeping Audit Toolkit can be found on Trustspace.

PART 3 – Associated Issues:

14. Version Control

Version	Date of Issue	Author	Status	Comment
V3	18 Jan 2007	Head of Records & Access to Information		Updated policy to reflect the move toward electronic patient records. Protection & Use of Service User Information and Formal Access Requests now separate policies.
V3	19 Mar 2007	Head of Records & Access to Information		Information relating to CareNotes added
V3	17 April 2007	Head of Records & Access to Information		ICO Use of Violent Warning Markers added. Updated naming documents. Controlled drugs Note B (Legal Requirements) added. Policy proforma added.
V3.1	23 July 2007	Head of Records & Access to Information		Amendments made to policy after comments from staff Updated Appendix , with amended Data Quality Supervision Guide
V3.2	10 Oct 2007	Head of Records & Access to Information		Amendment made to Appendix 9 to reflect recent changes in line with Mental Capacity Act.
V3.3	31 Oct 2007	Head of Records & Access to Information		Amendments made to Appendix – Confidential Database Protocol Add Appendix – Clinical Coding

				Protocol Updated to reflect Foundation Trust status
V4	20 Nov 2007 30 April 2008	Head of Records & Access to Information Head of Records & Access to Information		In light of meeting with CNST assessor: Make reference to the audit template in 8.3 Audit. Describe how actions will be taken forward from the audit, including, how, who and by when. Describe how this policy will be monitored through audits, changes to national legislation, department of health guidelines, NPfIT. Add paragraph to retention and disposal schedule re: how to dispose of confidential documents. Relevant changes made by ICT Dept
	6 May 2008	W&ODG		Agreed by Group Approved by the Group
V5	3 August 2009 10 September 2009	Head of Records & Access to Information Head of Records & Access to Information	Superseded	Annual review Separated appendices to make policy smaller. All appendices are available on the intranet and referred to in this policy. Email contributors: To update sections. Sections have been in line with responses. Confirmation email sent to IG & R Group for final

	8 October 2009 12 November 2009 26 January 2010 20 April 2010			comments on policy. Agreed at WODG on the proviso that the policy is checked for Alison Ryan’s input and is agreed by EIA. Agreed at EIA subject to feedback. Changes made as requested. Ratified by Executive Team
V6	1 February 2011	Head of Records & Access to Information		Sent to IG&R 9/12/10. Not ratified as not quorum. Circulated to IG&R members via email week commencing 17/1/11 for ratification.
V6.1	21 July 2011	Head of Records & Access to Information	Minor change	Amendment to 7.3 reflecting changes to the information security policy re: transporting patient identifiable/confidential information.
V6.2	6 September 2011	Head of Records & Access to Information	Minor change	Make reference to Records Keeping audit toolkit in 9.1. Make amendments to Section 5 – Training Strategy to ensure mandatory is explicit to managers and clinicians. Add Introduction to IG Training. Refer to presentation slides on TrustSpace.
	16 Feb 2012	Head of Records & Access to Information	Extended	It was agreed at the IG & R Group to extend the current version of this policy for 6 months

				because of the changes to internal processes. The IG policies will be mapped to ensure there is no duplication.
	10 May 2012	Head of Records & Access to Information	Change	Reviewed process for 'alerts' to be included in next revision of policy.
V7	July 2012	Head of Records & Access to Information	Annual Review/Approved by IG&R Group 16/08/2012	Policy put into new format
V8	10th March 2014	Head of Information Management and Compliance	Annual Review/Approved by IM&T/IG Programme Group	
V8.1	4th September 2014	Head of Information Governance & Compliance	Superseded	Change in practice in managing prescription charts (see page 13). Original must not be destroyed. Change in Practice requested and approved by DTC and MSC (July 2014)
V9	25th March 2015	Head of Information Management and Compliance	Superseded	
V9.1	25th March 2015	Head of Information Management and Compliance	Superseded	Amendments to appendices
V9.2	16th August	Head of Information Management and Compliance	Superseded	Amendments to appendices
V10	31st May 2018	Acting Information Governance Manager	Current	Complete review with the incorporation of the Clinical Information Filing Policy

15. Archiving Arrangements

All policy documents when no longer in use must be retained for a period of 10 years from the date the document is superseded as set out in the Trust Business and Corporate (Non-Health) Records Retention Schedule available on the Trust Intranet

A database of archived policies is kept as an electronic archive administered by the Policy Coordinator. This archive is held on a central server and copies of these archived documents can be obtained from the Policy Coordinator on request.

16. Associated Documents

- Archiving Procedure (Service Users Care Record)
- Archiving Procedure (Business and Corporate)
- Compliments, Concerns and Complaints Policy & Procedure
- Computer Access and Recovery Protocols
- Corporate Records Management Policy
- E-mail, Internet and Intranet Policy
- Information Risk Policy
- Information Security Policy
- Information Governance Policy
- Information Sharing Protocol between HPT and HCC
- Learning from Incidents
- Protection and Use of Service User Information policy

The above are available on the Trust Policy Website.

17. Supporting References

The following documents were used in the writing of this policy:

- General Medical Council, "Confidentiality: Protecting and Providing Information, September 2002:
- NMC, "Guidelines for Records and Record Keeping". August 2004
- Guidance on the Keeping and Management of School Nursing Records, WHHT School Nursing Service 2004
- Health Records & Communication Practice Standards for Team Based Care, NHS Health Records and Communication Practice Standards Group 2004
- Department of Health Records Management Code of Practice
- The NHS Care Record Guarantee, NHS Care Records Development Board 2005
- Guidance on the Data Protection Act 1998, Eastern Region, July 2000
- Interagency Information Exchange Guidance Note, Hertfordshire Social Services, March 2000
- "Protecting and Using Patient Information", A Manual for Caldicott Guardians, Department of Health, 1999.
- Data Protection Good Practice Note – The Use of Violent Warning Markers

18. Comments and Feedback

The following people/groups were involved in the consultation:

Policy Coordinator
Head of Information Rights and Compliance
Service Development Manager (EPR)
Associate Director of Information Management and Technology
Information Governance Manager
Senior Information Governance Officers
IM&T Managers Group
IM&T/IG Programme Group
Head of Medicines Management

Appendices

Appendix 1 – CQC Standards Regulation 17

Appendix 2 - The Legal Framework

Appendix 3 - Definitions of Therapeutic Notes

Appendix 4 – Glossary

Appendix 5 – Care Records Archiving Guidance

Appendix 1

Care Quality Commission
Fundamental Standards and Regulations

Regulation 17 - Good Governance

What the provider could do to meet the requirements

The provider has systems and processes to assess and monitor and improve the quality and safety of service provided and these are continually reviewed to ensure they remain fit for purpose; fit for purpose means systems and processes enable the provider to identify where quality and safety are being compromised and take appropriate and timely action in response to issues

Records relating to service users care and treatment are created/amended, stored and destroyed in accordance with current legislation and guidance, they are complete, legible, and accurate and every effort to ensure they are updated without delays.

Records must be kept secure and only accessed, amended or destroyed by persons authorised to do so.

Individual service user records are fit for purpose and can be accessed by authorised persons.

Individual service records should accurately record all decisions taken in relation to care and treatment.

Decisions taken on behalf of a service user due to lack of capacity must be recorded and provide evidence that these have been taken in accordance with the requirements of the Mental Capacity Act/Mental Health Act.

Appendix 2

The Legal Framework

This policy encompasses requirements of the Acts of Parliament listed below, Common Law, the Department of Health Circular 1999/053 (For the Record – Managing Records in NHS Trusts and Health Authorities), elements of the requirements of the Clinical Negligence Scheme for Trusts (CNST) and the National Health Service Litigation Authority (NHSLA) Controls Assurance Standards, the requirements of the Care Programme Approach (CPA) and the requirements within the codes of practice of the professional bodies which regulate the registration of staff employed within the Trust.

- The Freedom of Information Act 2000
- The Abortion Regulations 1991
- The Access to Health Records Act 1990
- The Caldicott Committee Report 1997
- The Crime and Disorder Act 1998
- Data Protection Legislation
- The Human Fertilisation and Embryology Act 1990
- The Human Rights Act 1998
- The Mental Health Act 1983
- The NHS Venereal Diseases Act 1974
- (NHS Trusts Venereal Disease Direction 1991)
- The Public Records Act 1958 (All NHS records are public records under the terms of the Public Records Act.)

The rights of clients are set out in:

1) The Data Protection Legislation
2) Health Service Guidance, HSC (1999) 053 "For the Record"
3) The Access to Health Records Act 1990 - in respect of the records of deceased persons.
4) The Civil Procedure Rules 1999
5) The Human Rights Act 2000

Appendix 3

Definitions of Therapeutic Notes

If the practitioner needs to keep supplementary records (that identify the patient) to which access by the service user is limited or withheld; the other members of the health care team must be able to access this information on a need to know basis.

Details of such information would be likely to include that, which in the opinion of the responsible health/social care professional and their manager would be likely to cause serious harm to the physical or mental health of the person if disclosed. This might also include social care records, or where the record relates to or has been provided by an identifiable third party, unless that third party consents to the disclosure.

Therapeutic notes (see below for examples) must be included in the care record. However, it may not be practical to type or attach detailed notes of every session, so the following procedure is agreed:

1. The clinical note should commence with a description of the context for the meeting / contact, i.e. an Assessment, a Consultation, a Therapy Session, and¸ the nature of the context, i.e. Routine, Acute, etc. Such that the reader of the note understands why you are meeting with the client, and the clinical context for the meeting or contact, e.g. “Seen routinely for 6/12 DBT sessions”, “Seen at short-notice for urgent review of safeguarding issues relating to……”.

2. An appropriately concise description of the clients’ current mental state, including any issues of concern, risk & safeguarding, change in mental state etc, reported use of medication(s) etc, where these exist.

3. An appropriately concise description of the major topics and issues discussed in the meeting / contact.

4. Where a particular therapeutic model(s), or a particular assessment process is employed the note should contain an identifying reference to these, e.g. “Seen for Psychotherapy / Interpersonal Therapy / Cognitive-Behaviour Therapy / Applied Behavioural Analysis / Neuropsychological Assessment etc”.

5. The note should define any contact with a third party and any related sharing of information which arises out of the meeting / contact. This should also describe the involvement / agreement (or otherwise) of the client in that third-party contact / sharing of information.

6. The note should describe any actions arising out of the meeting / contact, including those relating to actions agreed with the client.

7. If additional recorded material, e.g. test materials, handwritten notes, communications from the client or carer are generated in the course of the

meeting / contact then a reference to where these can be accessed is required. This does not apply to process notes (see below).

8. The note should conclude with a concise description of any action points arising out of the meeting / contact, including the time and date of the next planned contact with the client (if appropriate).

9. The length and detail of the clinical note will obviously depend upon a number of variables relating to the context of the meeting. However, the recording requirement should tend towards the minimum, keeping in mind the issues raised in this document, and not be exhaustive. The purpose of clinical notes should not be confused with that of process notes which are described more fully below.

Process Notes

Process notes are notes written by a therapist for clinical supervision purposes only, to contribute to reflective practice. Process notes may contain information regarding therapists' personal reflections and reactions to particular situations and are not service user identifiable. They therefore do not form part of the clinical record.

Members of staff who write process notes:

- Must ensure that the service user is not identifiable
- Must not keep process notes within the care record

Notes which contain other information such as the examples given below are not process notes but are part of the care record and should be treated accordingly.

Examples of information which should form part of the care record and are ***not*** process notes:

- Detailed notes of work carried out with a service user
- Rough notes of a session with a service user if no other record is made. A report written using information from the rough notes is not a complete record of the sessions, so the notes must be kept
- Therapy notes containing thoughts and decisions regarding clinical outcomes

Psychological Tests

- If psychological tests are administered, the test administered should be summarised in a clinical note on the EPR
- Details of the date the test was carried out, and the full name of the test should be included in the entry

- The entry should make reference to the fact that the full test is filed in the ‘secondary paper record’.
- The paper record should be logged on the ‘records locator/file locations’ document on the EPR.

The test should have the service user’s name and date of test administration, and will be subject to the formal ‘access to service user information’ procedure under Section 7 of Data Protection Legislation.

Appendix 4

Glossary

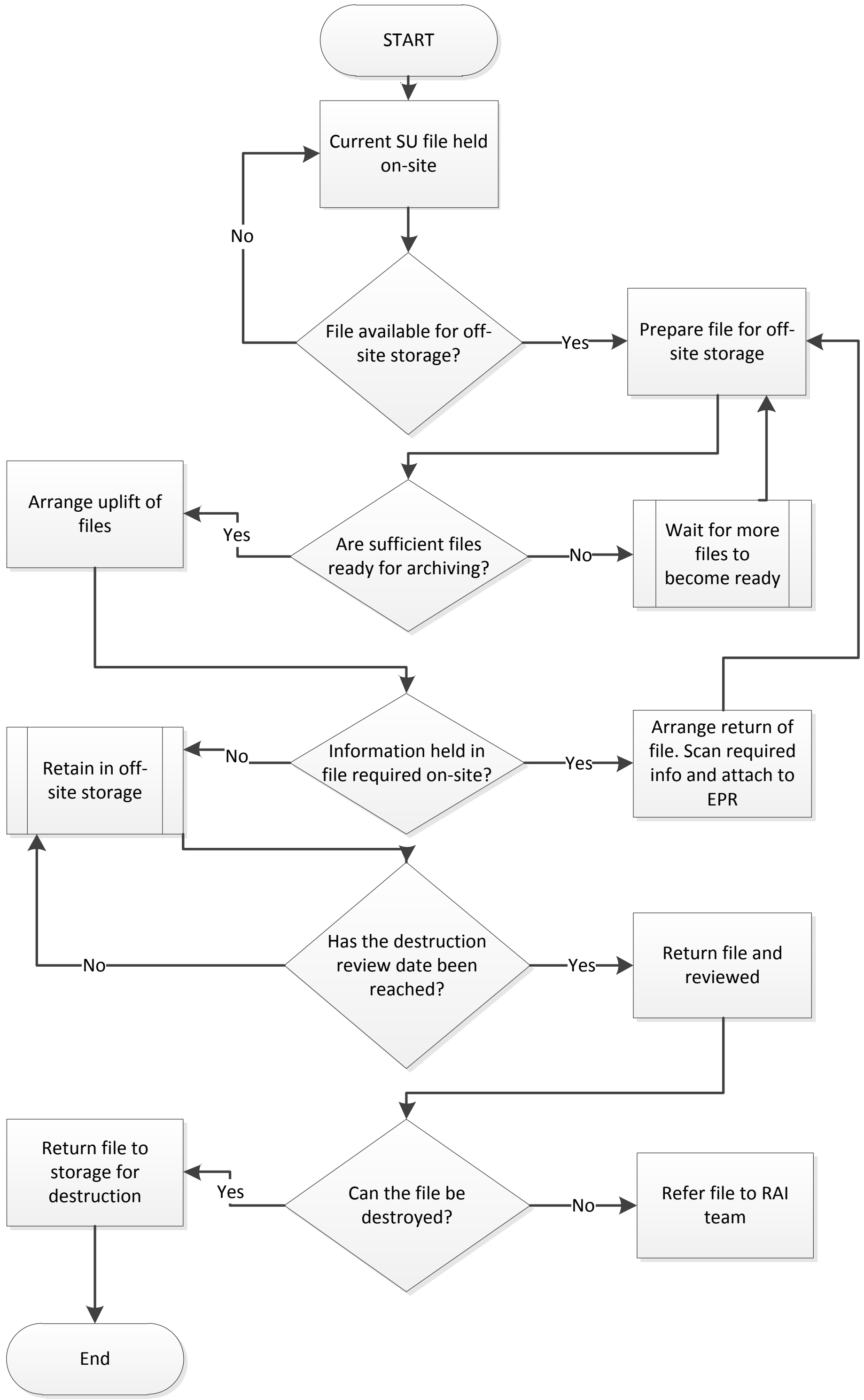
STANDARD

Adult Mental Health	AMH
Allied Health Professional	AHP
Care Programme Approach	CPA
Care Programme Approach Needs Assessment	CP2
Care Programme Approach Care Plan	CP3
Child and Adolescent Mental Health Service	CAMHS
Crisis Assessment and Treatment Team	CATT
Did Not Attend	DNA
Electro Convulsive Therapy	ECT
Electronic Patient Record	EPR
Freedom of Information Act	FOI Act
General Practitioner	GP
International Classification of Disease	ICD10
Integrated Recording Information System	IRIS
Information Management and Technology	IM&T
Information Technology	IT
Mental Health Act	MHA
Mental Health Services Data Set	MHSDS
Mental Health Services for Older People	MHSOP
Single Assessment Process	SAP
Specialist Learning Disabilities Service	SLDS
SMI Register	Seriously Mentally Ill Register
Therapeutic Notes	Psychologist’s descriptive notes about a patient’s therapy session

Appendix 5

Service Users Care Record Archiving Guidance

Process of this guidance


START
Current SU file held on-site
File available for off-site storage?
No
Yes
Prepare file for off-site storage
Arrange uplift of files
Yes
Are sufficient files ready for archiving?
No
Wait for more files to become ready
Retain in off-site storage
No
Information held in file required on-site?
Yes
Arrange return of file. Scan required info and attach to EPR
Has the destruction review date been reached?
No
Yes
Return file and reviewed
Return file to storage for destruction
Yes
Can the file be destroyed?
No
Refer file to RAI team
End

The Rights & Compliance Team is available to offer advice and assistance regarding any archiving issues units or teams may have (see section 9).

1. Introduction

This procedure covers the archiving of Service User's (SU) Care Folders only. Other procedures are available for the archiving of information other than Service User care records.

The Trust is working to a single record for each service user; the use of the Electronic Patient Record (EPR) will help achieve the National Programme for Information Technology (NPfIT) national requirement. All information for service users will be collected and stored electronically except where there is a requirement to keep the originals of specific documents. In general, once information has been typed, attached or scanned into the EPR, there is no need to keep a paper copy.

SU Care Folders should be archived with the Contractor following the discharge, transfer or death of the service user. Older volumes of a record can also be archived to reduce pressure on storage space within Trust offices.

The following workflow describes the basic stages in the management of SU Care Folders.

2. Purpose

Responsibilities

Responsible Managers

The Responsible Manager will be responsible for the quality of the archiving carried out on records owned by the unit or team, including the quality of data held within the unit/team and on RESTORE Document Management Database. This position will ensure that all the records selected for storage are unique and relevant to ensure compliance with legislation.

It is their responsibility to ensure that there are sufficient Record Administrators to carry out this procedure and to act as authorised contacts with the Contractor. Changes in Record Administrator or unit/team location must be alerted to the Information Rights & Compliance Team (IR&CT) as soon as possible so that the Contractor can continue to provide the contracted service.

Managers are responsible for ensuring that use of the contract is cost effective. Activity relating to their team/unit(s) must be monitored to ensure that records are effectively managed and storage costs kept to a minimum.

Invoices will not be sent to the manager for payment approval. The IR&CT will monitor the invoices monthly in order to identify high usage following which the invoices will be approved for payment by the Head of Information Rights & Compliance.

Record Administrators

Record Administrators are responsible for the accurate processing of their unit/team's records, ensuring that the information held on RESTORE Document Management Database is up-to-date and complete. This is an authorised role where the Information Rights & Compliance Team will train an employee to process records.

A Record Administrator is nominated by the unit/team's Responsible Manager as the main contact for liaising with the Contractor and the IR&CT on archiving issues. Up to two Record Administrators can be nominated to process records on behalf of a unit/team. Where necessary, the Responsible Manager can nominate him/herself as a Record Administrator.

Requests for services (for example, the recall of boxes or files from the Contractor) will only be accepted by the registered Record Administrator(s). Such requests will only be approved by the Contractor on line; Emails, fax and/or telephone requests will not be accepted. Each team will be allocated a unique identifier which must be quoted on all correspondence with the Contractor and the IR&CT. If confirmation of the unit code is required, please contact the IR&CT.

The Contractor

The Contractor is the only provider of archiving services to the Trust; use of other storage providers is not acceptable.

The Trust's contract with The Contractor is for the following service:

- Secure storage of all SU Care folders stored off-site
- Secure retrieval of individual records to specified Trust sites/locations only
- Secure collection of individual record from specified Trust sites/locations only
- Management of total storage volume to provide a cost effective solution
- Provision of RESTORE Document Management Database, an online service between supplier and the Trust to enable service requests and database queries
- Provision of a system for indexing and cataloguing all records stored off-site

The contractor does not own HPFT records but has contractual responsibilities under Data Protection and Freedom of Information legislation for the records.

Information Rights & Compliance Team

The Head of Information Rights & Compliance is the Senior Manager responsible for managing the contract. IR&CT will:

- Provide training for the Record Administrators and Responsible Managers
- Oversee adherence to this procedure
- Authorise new and amend access to the Contractor service

- Accredit the use of a particular contractor and deal with possible security issues that may arise
- Monitor aspects of the archiving process and storage contract to ensure that issues (such as excessive costs and poor management) are resolved

3. Process

Definitions

- **Box number** – The storage ID used by the Contractor to identify the box in which the SU Care folders are stored. The IR&CT will issue each team with their own unique number relevant to their service; this number will be prefixed by a letter. CAMHS will be C, Learning Disabilities and Forensic will be L, Mental Health will be M and Corporate will be B. The Records Administrators within each team will be responsible for entering the relevant box number after the service code. This will enable teams to keep the same number regardless of where they are based and should they ever be relocated.
- **Destruction review date** – The date at which the SU Care folder is due to be reviewed
- **File Locations** – Part of the EPR on Paris used to track SU Care folders
- **File number** – The storage ID used by the Contractor to identify the SU Care folders. The format will be the same as for box number above; RESTORE will enter the file number after the box number
- **RESTORE Document Management** Database – The Contractor's online service, allowing SU Care folders to be managed whilst off-site. Access is controlled by personal password. By using the database, Record Administrators will be able to monitor the movements of the stored files for their unit/team(s). It will also provide an audit trail of the Trust's transactions which can be used as evidence of appropriate record management. For this reason, RESTORE Document Management Database is the **only** means of requesting the Contractor's services
- **Historical interest** – SU Care folders which might be considered to have historical interest must fall into one of the following categories:
    - The service user is/was a notable person
    - The care received by the service user became or lead to a precedent in the Trust's policies or procedures
- **Legal records** – Documents within the SU Care folder which must kept in their original format (e.g. Mental Health Act or Child Protection documents; Consent to treatment and SAP documentation signed by service user/carer; Prescription Charts)
- **Recall** – The part of the procedure that covers the request and return of SU Care folders by the Contractor from off-site storage

- **Records Locator** – Part of the EPR on Care Notes used to track SU Care folders
- **Requestor** – A Trust employee, Records Administrator, who requires information in storage for the purposes of continuing Trust business.

- **Review process** – The task of reappraising the status of a SU Care folder for possible disposal, carried out by a HPFT employee with sufficient understanding of the information to carry out the process
- **SU Care folder** – The physical file containing documents relating to the care management of **one** service user.
- **Transit listing** – The document created by Record Administrators to evidence the SU Care folder uplift to the Contractor
- **Responsible Manager** – For the purposes of this procedure, the term 'Responsible Manager' refers to the manger with direct responsibility for the records owned by the team or unit
- **Unit code** – The code used by the Contractor to identify the unit/team that owns the SU Care folders.
- **Uplift** – The part of the procedure that covers the collection and removal of boxed SU Care folders by the Contractor to off-site storage
- **Volume** – A numbered part of the SU Care folder where more than one file is required to hold the information to be archived
- **Weeding** – The task of removing those documents or duplicates of documents produced as part of normal working processes. This includes papers that contain no significant operational or evidential value, as well as those already available on the EPR

On-site storage of SU Care records

Whilst on-site, SU Care folders must be held securely in locked filing cabinets or locked archive rooms. Please refer to the Care Records Management Policy for detailed information on managing SU Care folders on-site.

Records Locator (CareNotes Only)

All SU Care folders must be recorded on the Records Locator on the EPR. This contributes to the virtual, single record for each of our service users and enables the Trust to locate all the information on the service user efficiently.

The Records Locator must record each volume of the SU Care folder. Whilst on-site a volume entry will show the following:

- Reference number – volume number, as recorded on the folder cover
- Location – name of site
- Owner – name of unit/team, as recorded on the folder cover
- Start – date the volume was opened, as recorded on the folder cover
- End – [blank]
- Microfiched? – No
- Notes – Hospital number, where appropriate

File Locations (Paris Only)

All SU Care folders must be recorded on the File Locations on the EPR. This contributes to the virtual, single record for each of our service users and enables the Trust to locate all the information on the service user efficiently.

The File Locations must record each volume of the SU Care folder. Whilst on-site a volume entry will show the following:

- File ID – volume number, as recorded on the folder cover
- Date Created – date the volume was opened, as recorded on the folder cover
- File Type – e.g. paper
- Description - hospital number, where appropriate
- Location – name of site
- Team – name of unit/team
- Status – e.g. active/closed
- Due Destruction Date – leave blank

Decision to Archive

Archive storage should only be considered when:

- the service user has died
- the service user has been discharged or transferred from the unit and is not likely to return
- the folder of a current service user contains only legal records which are not required on a day to day basis
- the service is no longer delivered by HPFT because the service user has relocated
- the service is no longer delivered by HPFT due to organisational changes
- information that is not legible once scanned to the EPR

Records can only be sent to the Contractor if they meet the following criteria:

- Cost effectiveness – the cost and service levels provided by the Contractor must be considered to ensure that use of the service is appropriate. Records that may be required within a short time may be more efficiently stored on-site. See Appendix 1 for a list of the Contractor's charges.
- Retention – records that will be destroyed within a short period (i.e. less than 12 months) are more cost effectively stored on Trust premises. The cost of the service prohibits its use for short-term storage.

Preparing SU Care folders for archiving

SU Care folders which have been selected for archiving must be prepared by a Record Administrator.

Paper copies of documents held on the EPR must be removed and destroyed using the confidential waste facility. Typed, non-legal documents must be scanned and retained on the EPR provided that the images are checked to ensure legibility and accuracy against the original. The folder should contain only legal documents and those not suitable for scanning.

No information will be uplifted for scanning without the Contractor receiving prior consent from the IR&CT.

All documents must be securely held in a folder or in a ring binder. Plastic sleeves or elastic bands must not be used to secure bundles of paper as these disintegrate and could compromise the integrity of the records. Archive ribbon or envelopes should be used to hold the record together.

For service users who have accessed more than one team/unit, on discharge the key /primary worker or named person must collect the records pertaining to that individual making *one complete record* and removing any duplicated information. The complete record can then be prepared for archiving.

SU Care folder front cover

The information shown on the SU Care folder's front cover is used by the Contractor to index each file. Where the Contractor cannot locate the specified information, the file will be returned to the unit as not acceptable.

The front cover must contain **all** of the following information:

- The service users' surname and first name
- The service users' date of birth
- The service users' NHS number
- The volume number
- The start and end dates for the volume
- The reason for the folder's closure, i.e. discharge, death, transfer, current
- The unit/team owning the folder
- The destruction review date for the folder

Where a folder is re-used, the information on the front of the folder must be permanently covered. The front cover template must be attached to record the up to date information.

Destruction Review Dates

Setting a destruction review date enables the SU Care folder to be managed effectively. It is not an automatic date of destruction, but a date at which the folder will be reviewed for disposal. Using a standard period of time following the folder's closure enables the Trust to comply with statutory requirements.

The Care (Health) Records Retention and Disposal Schedule provides the retention periods for Service User records. The length of time depends on the status of the SU Care folders:

Reason for archiving	**Retention period**
the service user has died	8 years from the date of death
the service user has been discharged from the unit	20 years from the date of discharge

the folder of a current service user is full	20 years from the folder’s closure date
the service is no longer delivered by HPFT	20 years from the folder’s closure date

Destruction review dates must reflect the specific date on which it is calculated. There is no need to round the dates on to the start of the following year for SU Care records.

Records Locator (CareNotes Only)

The Records Locator must record the movement of SU Care folders. Whilst preparing a folder for storage the entry will show the following:

- Reference number – volume number, as recorded on the folder cover
- Location – name of site
- Owner – name of unit/team, as recorded on the folder cover
- Start – date the volume was opened, as recorded on the folder cover
- End – **date the volume was closed, as recorded on the folder cover**
- Microfiched? – No
- Notes – ‘**in preparation for archiving’**, hospital number, where appropriate

File Locations (Paris Only)

The File Locations must record the movement of SU Care folders. Whilst preparing a folder for storage the entry will show the following:

- File ID – volume number, as recorded on the folder cover
- Date Created - date the volume was opened, as recorded on the folder cover
- File Type – e.g. paper
- Description - **date the volume was closed, as recorded on the folder cover,** ‘**in preparation for archiving’**, hospital number, where appropriate
- Location – name of site
- Team – name of unit/team
- Status – e.g. active/closed
- Due Destruction Date – destruction review date, as recorded on the folder cover

Uplifting SU Care Folders to archive

Once sufficient SU Care Folders have been prepared for archiving the Record Administrator can begin the uplift process.

Only standard boxes provided by the Contractor can be used. Orders **must** be placed using RESTORE Document Management Database. Requests made by telephone, email or fax are not acceptable and will be refused by the Contractor.

Records Locator (CareNotes Only)

The Records Locator must record the movement of SU Care folders. When the folder has been prepared for uplift and shortly before the uplift has taken place, the folder entry will show the following:

- Reference number – **box number identified on the transit listing**
- Location – **the Contractor**
- Owner – name of unit/team, as recorded on the folder cover
- Start – date the volume was opened, as recorded on the folder cover
- End – date the volume was closed, as recorded on the folder cover
- Microfiched? – No
- Notes – '**Uplifted to archive on [date of uplift]'**, hospital number, where appropriate

File Locations (Paris Notes)

The File Locations must record the movement of SU Care folders. When the folder has been prepared for uplift and shortly before the uplift has taken place, the folder entry will show the following:

- File ID – **box number identified on the transit listing**
- Date Created – date the volume was opened, as recorded on the folder cover
- File Type – e.g. paper
- Description - date the volume was closed, as recorded on the folder cover, '**Uplifted to archive on [date of uplift]'**, hospital number, where appropriate
- Location – **the Contractor**
- Team – name of unit/team
- Status – e.g. active/closed
- Due Destruction Date – destruction review date, as recorded on the folder cover

Boxing folders

As each folder is added to the box, a Transit Listing for the box must be prepared. This is used as the tracking system whilst the boxes are in transit.

To comply with health and safety requirements, do not overfill boxes. Each box should weigh no more than 12kg, even if this means that it will not be full. This is not a specific limit but a guideline within which the average person can safely handle the box. Above this, it may still be safe, although a risk assessment will be required.

No more than 99 SU Care folders can be placed in one box. Records should be stored in an upright position (either on the spine or the front) but not laid flat.

Preparing the boxes

A label must be attached to one of the smaller ends of the box (not the lid) to summarise the contents and indicate which unit/team it belongs to.

The box number **must** follow the format C100, M200, L300 or B400/001 to enable the box and folders to be indexed and managed.

To identify the destruction date for the box, find the SU Care folder with the latest destruction review date and repeat this on the End of Box label. All boxes **must** have a destruction date.

Example of a completed End of Box label:

C	1	0	0	/	0	0	1

Address: 15 Forest Lane Kingsley Green Harper Lane Radlett Herts WD7 9HQ 01923 289 050	**Number of Records**: 36

Destruction date:

0	5	/	1	0	/	2	0	2	0

Contact: A N Other (Operational Services Manager) / An.Other@hpft.nhs.uk

The box lid must have written in marker pen the initials **FE** (File entry) and the **unit code** in letters no smaller than 10 cm (4 in) high. Without this the Contractor will not be able to index each file and store the box correctly. Unit codes are available from the Information Rights Assistants in the IR&CT.

When a box has been packed, it must be sealed with 2 plastic security seals used to secure the lid to the box on either side. This can be done by threading a plastic security seal through a hole in the box lid, out through a hole in the box side and then secured.

These seals are an important element of the security of the SU Care folders whilst in transit. They should be broken only by the Contractor when the box contents are about to be indexed.

Requesting uplift

Once the records have been boxed they are ready for uplift to the Contractor. Each collection by the Contractor is charged.

Uplifts **must** be placed using RESTORE Document Management Database. Requests made by telephone, email or fax are not acceptable and will be refused by the Contractor. The Contractor will only return folders to addresses authorised by the IR&CT.

Boxes will be collected directly from the Record Administrator. If the Record Administrator is unable to be present during the uplift, the name of a nominated person must be sent, in advance, to the Contractor and will be accepted for a single uplift.

When collecting the boxes for uplift, it is essential to bear security in mind. Until the time of uplift, the boxes should be protected in an appropriate manner.

In every case, the Record Administrator and Contractor’s driver must sign the Transit Listing for each box uplifted. Once signed, this should be sent to the IR&CT.

The Contractor is committed to indexing every box or SU Care folder within 5 working days (but will aim to complete this task within 48-72 hours) of receiving the box. Following this date, the Record Administrator will be able to check that the folders have been received and indexed correctly on RESTORE Document Management Database. Any queries with time-delays or indexing quality should be promptly referred to the IR&CT.

Recalling SU Care records from archive

A SU Care folder may be required by a care professional for review if the information is not held on the EPR. Most information will be immediately available from the EPR. Recalling folders from storage results in an additional cost to the Trust and it is imperative that all recalls can be justified. Any request for service that appears to the Record Administrator to be either incorrect or an attempt at inappropriate access must be notified to the IR&CT Team for investigation.

Requesting recall of folders

Recalls must be requested using RESTORE Document Management Database which is available at all times. Request made by telephone, email or fax are not acceptable and will be refused by the Contractor.

Costs can be efficiently managed if the delivery of recalled files is arranged at the same time as uplifts, thereby reducing transport charges (appendix 1).

The Contractor will only return folders to addresses authorised by the IR&CT. Any request for service that appears to the Contractor to be either incorrect or an attempt at inappropriate access will be notified to the IR&CT for investigation.

Delivery of folders

When a SU Care folder is returned it will be taken by the Contractor to the reception desk at the registered address. The Record Administrator will be contacted by reception staff and required to collect and sign for delivery. The number of SU Care folders must be checked before delivery is accepted. The IR&CT must be contacted if a SU Care folder is seriously damaged or any documents unaccounted for.

If the Record Administrator is unable to be available for the delivery, the name of a nominated person must be sent, in advance, to the Contractor and will be accepted for a single recall.

When an older file is recalled and found to have documents which can be scanned for the EPR, the Record Administrator will need to arrange for this to happen and return to storage the folder containing legal documents only.

Records Locator (CareNotes Only)

The Records Locator must record the movement of the folder. As soon as the folder is on-site, the Record Administrator must amend the entry to show the following:

- Reference number – box number identified on the transit listing
- Location – **name of site**
- Owner – name of unit/team, as recorded on the folder cover
- Start – date the volume was opened, as recorded on the folder cover
- End – date the volume was closed, as recorded on the folder cover
- Microfiched? – No
- Notes – '**Recalled for use by [name of care professional] on [date of recall]'** , hospital number, where appropriate

Following uplift to storage, the Records Locator must reflect the new location of the file.

File Locations (Paris Only)

The File Locations must record the movement of the folder. As soon as the folder is on-site, the Record Administrator must amend the entry to show the following:

- File ID – box number identified on the transit listing
- Date Created – date the volume was opened, as recorded on the folder cover
- File Type – e.g. paper
- Description - date the volume was closed, as recorded on the folder cover, '**Recalled for use by [name of care professional] on [date of recall]'**, hospital number, where appropriate
- Location – **name of site**
- Team – name of unit/team
- Status – e.g. active/closed
- Due Destruction Date – destruction review date, as recorded on the folder cover

Following uplift to storage, the File Locations must reflect the new location of the file.

Returning folders to archive

The SU Care folder must be returned at the same time as a scheduled uplift. Uplifts must be requested using RESTORE Document Management Database which is available at all times. Request made by telephone, email or fax are not acceptable and will be refused by the Contractor.

Any request for service that appears to the Contractor to be either incorrect or an attempt at inappropriate access will be notified to the IR&CT for investigation.

Destruction review of SU Care records

All records will be disposed of in accordance with the Care (Health) Records Retention and Disposal Schedule.

The Information Governance Team will run a report from RESTORE Document Management Database bi-monthly to identify records and boxes due for a destruction review.

Reviewing folders

All records will need to be reviewed by the Lead Clinician at the end of their retention period (8 years following the date of death and 20 years following the date of transfer or discharge). If it is decided that the record needs to be retained for historical reasons, the care record should be marked accordingly and transferred to a Public Records Office. The record will then be retained for a further period of 100 years.

Where the reason for the folder's storage has been given as 'current', the Record Administrator must check the EPR to identify the current status of the service user and the destruction review date recalculated.

All other folders must be recalled from the Contractor and arrangements made for their review, where possible in consultation with a relevant care professional. The Record Administrator must check the EPR Records Locator/File Locations for other volumes for the same service user. Where other volumes are found the IR&CT must be alerted so that these can be reviewed at the same time.

The destruction review decision for each folder will be one of the following:

- To destroy the record as it no longer has administrative, legal of financial value to the Trust and is not of historical value
- To transfer the ownership of files that have historical value only

Where folders might be considered of historical interest, the IR&CT must be contacted for guidance.

Requesting folder destruction

Where records are to be destroyed, the Responsible Manager will identify the SU Care folders for destruction to the Contractor.

The Contractor will send a Request for Documents to be Destroyed form to the Responsible Manager, seeking authorisation to destroy. When this is returned with appropriate signatures in place, the Contractor will proceed to destroy the records as requested. The unit/team must send a copy of the Documents to be Destroyed form to the IR&CT.

Where the Responsible Manager has not responded to the Request for Documents to be Destroyed form within 5 weeks, The Contractor will notify the IR&CT for follow-up with the unit/team as a matter of urgency.

The Contractor will send the completed Document Destruction Advice to the IR&CT. The SU Care folder will be indicated on RESTORE Document Management Database as 'destroyed'.

Records Locator (CareNotes Only)

Whether the SU Care folder is destroyed or transferred on the grounds of historical interest, the Records Locator must record the movement of the folder.

Following the completion of the Request for Documents to be Destroyed form the Record Administrator must amend the Records Locator as follows:

- Reference number – **box number identified on the transit listing**
- Location – **the Contractor**
- Owner – name of unit/team, as recorded on the folder cover
- Start – date the volume was opened, as recorded on the folder cover
- End – date the volume was closed, as recorded on the folder cover
- Microfiched? – No
- Notes – '**Sent for destruction on [date sent]'**, hospital number, where appropriate

Following a decision to retain the folder for historical purposes, the Information Governance Team will amend the Records Locator as follows:

- Reference number – **box number identified on the transit listing**
- Location – **name of archive**
- Owner – name of unit/team, as recorded on the folder cover
- Start – date the volume was opened, as recorded on the folder cover
- End – date the volume was closed, as recorded on the folder cover
- Microfiched? – No
- Notes – '**Transferred to archive on [date sent]'**, hospital number, where appropriate

File Locations (Paris Only)

Whether the SU Care folder is destroyed or transferred on the grounds of historical interest, the File Locations must record the movement of the folder.

Following the completion of the Request for Documents to be Destroyed form the Record Administrator must amend the File Locations as follows:

- File ID – **box number identified on the transit listing**
- Date Created – date the volume was opened, as recorded on the folder cover
- File Type – e.g. paper
- Description - date the volume was closed, as recorded on the folder cover, '**Sent for destruction on [date sent]'**, hospital number, where appropriate
- Location – **the Contractor**
- Team – name of unit/team
- Status – e.g. active/closed
- Due Destruction Date – destruction review date, as recorded on the folder cover

Following a decision to retain the folder for historical purposes, the IR&CT will amend the File Locations as follows:

- File ID – **box number identified on the transit listing**
- Date Created – date the volume was opened, as recorded on the folder cover
- File Type – e.g. paper
- Description - date the volume was closed, as recorded on the folder cover, '**Transferred to archive on [date sent]'**, hospital number, where appropriate
- Location – **the Contractor**
- Team – name of unit/team
- Status – e.g. active/closed
- Due Destruction Date – destruction review date, as recorded on the folder cover

Contacts

RESTORE Plc	Records Administrators to contact RESTORE via the RESTORE Document Management Database.
Information Rights & Compliance Team	IM & T Department 99 Waverley Road St Albans, AL3 5TL 01727 804956

Appendices

Appendix 1

The Contractor’s charges from 11th May 2018

Collect New and Putaway Box	£0.50
Collect New and Putaway File RESTORE to enter details from record on Filetrak system	£N/A
Collect Exist and Putaway Box	£0.50
Collect Exist and Putaway File	£0.50
Pick & Deliver Box	£0.50
Pick and Delivery File	£0.50
Pick & Shred Box	£1.50
Pick & Shred File	N/A
Perm Out Box	£1.50
Perm Out File	N/A
Flat Pack Standard Size	£1.00
Empty Shredding Bin Per Kg	N/A
Shredding Sacks & Tags	N/A
Flat Pack B3 Size	£1.30
Express Trip Charge (Delivery within 2 hours)	£60.00
Trip Charge as Same Day (before 5pm)	£22.80
Trip Charge as Next Day (before 5pm)	£22.80
Storage (Monthly) Box Size 1	£0.17
Storage (Monthly) Box Size 2	£0.19
Storage (Monthly) Box Size 3	£0.21
Storage (Monthly) Box Size 4	£0.24
Storage (Monthly) Box Size Small	N/A
Scan on Demand per Sheet	£0.04
Scan Preparation per File	£5.00
Rental (Monthly) Shred Bin 240L	N/A

Appendix 2

NHS NUMBER

Please note: The Electronic Patient record is the primary record and has the most up to date information

SURNAME: (Block Letters)
MR/MRS/MISS/MS

FIRST NAME: (Block Letters)

DOB:

CONFIDENTIAL

Users of this file are reminded that information of a confidential nature concerning service users which they may obtain during the course of their duties must not be disclosed without authorisation

Not to be removed without authorisation from

(Unit Name and Directorate)

The Care Record must be transported in a secure manner
which maintains Service User's confidentiality

Last year of attendance label

SURNAME: (Block Letters)
MR/MRS/MISS/MS

FIRST NAME: (Block Letters)

DOB:

REASON FOR CLOSURE: (delete as appropriate)
DISCHARGE / DEATH / TRANSFER

DESTRUCTION REVIEW DATE:

VOLUME NO: ________

FROM: ______________

TO: _________________

Appendix 3

End of box label

				/			

Address:	**Number of Folders:**

Destruction date:

		/			/	2	0		

Contact:

				/			

Address:	**Number of Folders:**

Destruction date:

		/			/	2	0		

Contact:

Appendix 4

Transit Listing

Box number:							
				/			

Unit/team name and address:	Unit Code:	Date & time of uplift:
	Authorising Manager:	Record Administrator's name:

Service User's name, date of birth and NHS number		Number of volumes
01		
02		
03		
04		
05		
06		
07		
08		
09		
10		
11		
12		
13		
14		
15		
Box destruction review date:		

Contact on behalf of Cintas (driver):	**Contact on behalf of HPFT:**
Print	Print
Sign	Sign

Appendix 5

CERTIFICATE OF DESTRUCTION (Health)

I certify that these records have exceeded their recommended minimum retention period in accordance with Department of Health Clinical Information (Health and Social Care Records) Guidelines as per Hertfordshire Partnership University NHS Foundation Trust Management of Care Records Policy and Procedure and are no longer of Historical value'

These records have been destroyed under confidential conditions on: ....

Authorising Manager's Name: ……………………………………. Signature ………………………………………...

Description	Number of Records Destroyed	Date From	Date To

Appendix 6

1. Introduction to Summary Care Records

A Summary Care Record (SCR) is a centrally held electronic record which contains information about the medicines a patient is prescribed, allergies and any adverse reactions to medicines.

Having this information stored in one place makes it easier for healthcare staff to treat patients in an emergency, or when their GP practice is closed. The information is automatically updated from the GP electronic records at regular intervals (often nightly).

Only healthcare staff involved in a patient's care can see their Summary Care Record.

Those who look at a Summary Care Record need to:

- be directly involved in the patient's care;
- have a Smartcard with a chip and pass code

Healthcare staff will only see the information they need to do their job, and they will ask permission every time they need to look at a SCR. If they can't ask, for example if a patient is unconscious or lacks capacity for any other reason, they may look at a SCR without permission. If they do this, they will make a note on the service user's PARIS record to say why they have done this.

In exceptional circumstances it will be appropriate to look at the SCR prior to meeting a patient, e.g. before an emergency home visit. This should be clearly documented on PARIS, disclosed to the patient and the reasons for having done so explained.

Healthcare staff should recognise that the SCR is an information resource to help guide the clinical care they provide (in the same way GP referral letters or lists of medication are sources of information).

2. Initial / Trust Decisions

The initial roll-out of SCR viewing will be to Single Point of Access staff, Medicines Management / Pharmacy staff and medical staff across the Trust. These are areas where the clinical benefit is clear and interest has been expressed. In some teams, it will be appropriate for administrative staff in a supporting role to have SCR viewing access. This will be established on an individual basis and reviewed as the roll-out progresses.

The functionality will also be available to other teams / staff who can demonstrate that the use of SCR would be beneficial in adding value to clinical care.

There are SCR Viewing Request pro-formas:

Appendix One (1) - CIS – Create New User

Appendix Two (2) - CIS Position Assignment and Modification)

These forms need to be completed and returned to:
For Medics:

Dr Paul Bradley – paulbradley@nhs.net
Tel: 01442 283464

For all other staff:

Workforce Intelligence Team – hpft.workforce@nhs.net
Tel: 01707 253874

The assessment criteria are detailed in Appendix three (3).

3. Local Decisions

Once a request to view SCR has been approved, the team / service need to ensure the following aspects are discussed:

a) Identification of an Information Asset Owner

This is essential for any information system within the Trust. An IAO would be the senior manager (e.g. Service Line Lead or Medical Lead) who can make decisions and take responsibility for decisions about granting access to the SCR.

b) Identification of an Information Asset Administrator (team manager/consultant)

This is also essential for a team; the IAA should be team managers / medical consultants and be able to assist staff members with queries about the system of viewing SCRs.

c) Who requires the facility to view SCR within the team?

The Service Line Leads / Medical Leads (IAO) and Team Managers (IAA) would need to discuss which staff members would benefit from the facility to view SCRs; the staff members must need the facility in line with the responsibilities of their job role. It is also important to consider the likelihood of the staff member using the facility, the benefit to clinical care and the functioning of the team within the Trust.

It is likely to be beneficial for medical staff of all grades who deal with medication on a day to day basis, either in clinic, whilst on-call or on admission to inpatient wards. Junior doctors joining the Trust will frequently have a Smartcard which can be activated for the period of time they will work in the Trust using the Position Assignment and Modification form.

Team Managers will need to keep a record of staff who have access to the SCR (to be approved by the Service Line Lead) and any changes reported to the Workforce Intelligence Manager/ Registration Authority Manager to ensure their smartcard records are up to date.

4. Approval

Each staff member within the department will need a Smartcard issued or additional codes added to their existing Smartcard to enable the facility to view SCR. The appropriate RA forms (Appendix one and two) will need to be completed and returned to:

For Medics:

Dr Paul Bradley – paul.bradley@hpft.nhs.uk

Tel: 01442 283464

For all other staff:

Annabel Gobin - Workforce@hpft.nhs.uk

Tel: 01707 253874
For further information, you can refer to the Registration Authority Policy on TrustSpace.

5. Guidance & Training

All staff members given the functionality to view SCRs are recommended to undertake training via an e-learning module. The training module has been developed using an e-learning training package produced by the Health and Social Care Information Centre. Available here:

https://www.e-lfh.org.uk/programmes/summary-care-records/

6. Clinician accessing patient record and verifying the Legitimate Relationship (LR) themselves

Each user requiring access to the SCR self-claims an LR which supports subsequent accesses for up to 5 days for that user alone. An IG Alert is generated whenever a record has been accessed without service user consent. This is referred to as ‘Emergency Override’. These occasions will be investigated by the Information Rights & Compliance Team and reconciled with Paris entries to confirm the service user's attendance.

If accessed after 5 days a new self-claimed LR would need to be claimed and a subsequent alert would be generated for the Privacy Officer to view.

7. Monitoring and Compliance

The Information Rights & Compliance Team will spot check 10-20 notifications per month to ensure that no untoward access has occurred. As long as there is a legitimate reason for staff to be entering the SCR then, even if an alert is raised, there is nothing to worry about. The team will simply match up the alert with a corresponding entry on PARIS and close the alert.

If it is found that there is no legitimate reason for a record to be accessed, the staff member will be asked to explain their actions and further investigations will occur if the behaviour is inappropriate and the functionality of SCR is being abused. Staff members should be aware that inappropriate use will result in disciplinary action.

7.1 Viewing figures will be monitored:

NHS Digital (formally The Health & Social Care Information Centre) will provide viewing figures on a weekly basis; these include details which can be linked down to individual staff using the system. The RA Manager will be able to monitor viewing. Those departments / staff members that are not using the viewing functionality over a six to twelve month period will be reviewed and if justified, have the functionality removed.

This monitoring will be used to ensure that in line with statutory requirements staff members only have access to information they require in line with their job role and ensure that risk can be reduced where possible with staff not being able to view more than necessary.

7.2 Information Asset Owner/ Administrator validation:

The Workforce Intelligence Manager/RA Manager will ask teams / departments asked to validate the lists of their staff who have access to SCR.

The team manager (IAA) can carry out the validation work but the Service Line Lead (IAO) must give final approval. It is essential that checks are made to ensure the staff members on the list still require access to view SCR.

Appendix 8

CIS – Create New User

- Part 1 of the form is to be completed by RA Sponsor and smartcard applicant,
- Applicants must sign terms and conditions in Part 2 of this form before a smartcard can be issued.
- Once Part 1 and Part 2 are completed a meeting needs to be arranged with the RA Manager or RA Agent, they will complete the ID check in Part 3.
- Applicants must present proof of identity as per the Identity Checks at NHS Employer Standards at the face to face meeting with the RA Manager or RA Agent. RA must capture a photograph of the individual.

Please complete the following details in BLOCK CAPITALS:

Part 1: To be completed by applicant and RA Sponsor

Applicant Personal Details			**(Please complete all fields as fully as possible in BLOCK CAPITALS)**
Title: (e.g. Dr, Mr, Mrs, Miss etc.)		Date of Birth: (Mandatory)	
Given Name: (Mandatory)			
Middle Names:		Preferred name:	
Family Name: (Mandatory)		Previous family names:	

Applicant Identifiers (Mandatory)	**(At least one Identifier must be completed)**
NI number:	
Passport number:	
Driving licence number:	
Applicant Contact Details	**(Please complete all fields as fully as possible)**
Telephone number:	
Mobile number:	
Email:	
RA Sponsor (Mandatory)	
RA Sponsor Name:	
RA Sponsor UUID(12 digit number on front of smartcard):	
RA Sponsor Signature:	
Date:	
Applicant (Mandatory)	
Applicant Signature:	

Date:	

Part 2: To be complete by applicant

By signing this declaration, I, the applicant:

1. agree to provide any additional information and documentation required by the Registration Authority in order to verify my identity;

2. confirm that the information which I provide in this application is accurate. I agree to notify my local Registration Authority immediately of any changes to this information;

3. agree that the Smartcard issued to me is the property of the NHS and I agree to use it only in the normal course of my employment or contract arrangement;

4. agree that I will check the operation of my Smartcard promptly after I receive it. This will ensure that I have been granted the correct access profiles. I also agree to notify my local Registration Authority promptly if I become aware of any problem with my Smartcard or my access profiles;

5. acknowledge that I will keep my Smartcard private and secure and that I will not permit anybody else to use it or any session established with the NHS Care Records Service applications. I will not share my Passcodes with any other user. I will not make any electronic or written copies of my Passcodes (this includes function keys). I will take all reasonable steps to ensure that I always leave my workstation secure when I am not using it by removing my Smartcard. If I lose my Smartcard or if I suspect that it has been stolen or used by a third party I will report this to my local Registration Authority as soon as possible;

6. agree that I will only use my Smartcard, the NHS Care Records Service applications and all patient data in accordance with The NHS Confidentiality Code of Practice (as available on the **www.dh.gov.uk** site) and (where applicable) in accordance with my contract of employment or contract of provision for service (which ever is appropriate) and with any instructions relating to the NHS Care Records Service applications which are notified to me;

7. agree not to deliberately corrupt, invalidate, deface, damage or otherwise misuse any NHS Care Records Service applications or information stored by them. This includes but is not limited to the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality.

8. acknowledge that my Smartcard may be revoked or my access profiles changed at any time without notice if I breach this Agreement; if I breach any guidance or instructions notified to me for the use of the NHS Care Records Service applications or if such revocation or change is necessary as a security precaution. I acknowledge that if I breach this Agreement this may be brought to the attention of my employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution);

9. agree that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Smartcards for the NHS Care Records Service applications. The Registration Authority is not responsible for the availability of the NHS Care Records Service applications or the accuracy of any patient data.

10. acknowledge that I, or my employer, shall notify my local Registration Authority at any time should either wish to terminate this Agreement and to have my Smartcard revoked e.g. on cessation of my employment or contractual arrangement with health care organisations or other relevant change in my job role; and

11. acknowledge that these terms and conditions form a binding Agreement between myself and those organisations who have sponsored my role(s). I agree that this Agreement is governed by English law and that the English courts shall settle any dispute under this Agreement.

Applicant Signature:	
Date:	

Part 3: For RA Manager/Agent Use Only

Identity Verification (Mandatory) **(3 Forms of ID: 1 Photo ID + 2 Address ID OR 2 Photo ID + 1 Address ID)**				
Photo Identification	**Document No.**	**Country**	**Date of Issue**	**Date of Expiry**
Passport:			▨	
Driving Licence:				▨
Address Identification:	**Address 1**		**Address 2**	
Address ID Type: (Utility Bill, Electoral Register, etc.)				
Name of Company:				
Date of Issue:				

RA declaration

I confirm that the **Applicant** specified above can be issued a Smartcard. I verify the original document was seen and confirmed to be genuine in a face to face meeting with the applicant.

RA Name:		**RA Role:**	
RA UUID:		**Date:**	

Appendix 8

CIS – Position Assignment & Modification

- Must be completed by RA Sponsor
- All mandatory fields must be completed to complete this process.

Please complete the following mandatory fields in BLOCK CAPITALS:

User Name (Mandatory)	**User NI Number** (Mandatory)	**User Smartcard UUID number (12 digit number on front of smartcard. Leave blank if new user without existing smartcard)**

Team Name (Mandatory)

Position Name	**Add/ Remove**	**Reason for position assignment modification**	**Position Assignment Start Date***	**Position Assignment End Date**
367 Summary Care Record				

* If the dates are left blank the profile starts now and ends at the CIS default end date (10 years).

RA Sponsor declaration

I confirm the **Position** amendment(s) detailed in this form are correct and can be made to the user above.

RA Sponsor Name	
RA Sponsor Signature	
Date	

(Mandatory)

APPENDIX 3

Assessment Criteria Indicators:

- There needs to be a recognised need and a justified purpose for the request (e.g. improvements in clinical care can be recognised)
- The request must be signed by an appropriate manager

- The service must be willing to take responsibility for the provision (i.e. have IAOs and IAAs identified to make decisions and organise the day to day running)

Factors that would support the request to view further:

- The service request comes from an emergency and/or out of hours service.

- Evidence has been documented that this will improve compliance with regulatory and statutory requirements of the team.

Our Values

we are...	you feel...
Welcoming	✓ Valued as an individual
Kind	✓ Cared for
Positive	✓ Supported and included
Respectful	✓ Listened to and heard
Professional	✓ Safe and confident