Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: CP3
Issue number: 16.01

Health Records Policy

Lead executive	Medical Director & Caldicott Guardian
Authors details	Information Governance Lead/DPO

Type of document	Policy
Target audience	All CWP staff
Document purpose	Trust policy for management of health records, encompassing paper and electronic records

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 12 April 2021
Implementation date	April 2021	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM7	Code of confidentiality policy
IM6	Information (over arching) sharing policy
CP40	Safeguarding children policy
GR17	Freedom of Information Policy
IM1	Information Communications Technology (ICT) Acceptable Usage Policy (AUP)
GR41	Corporate records policy
CP19	Advance Statements
CP30	Do Not Attempt Resuscitation (DNAR) orders
CP24	CPR policy
GR1	Incident reporting and management policy
GR2	Health and safety arrangements and responsibilities
GR3	Risk management policy
GR25	Crisis Support Team
HR14	Guidance on accessing staff support and counselling service
GR33	Lone worker policy
CP10	Safeguarding adults policy
CP6	The Management of Challenging Behaviour, Violence and Aggression policy
CG1	Fraud, theft and corruption policy
MP10	Violence and Aggression Pharmacological Short Term Management (incorporating Rapid Tranquilisation) policy
CP25	Therapeutic observation for in-patients
GR4	Recording, investigating and management of Complaints policy / Concerns and Compliments.
CP5	Clinical risk assessment policy
	Clinical systems training guides available via clinical systems teams.
	Health Records Standard Operating Procedures

Document change history	
What is different?	1. Links refreshed 2. Page 7: 1.1 changes in medication should be recorded before the end of the working shift 3. Page 8: 1.1. information held on the electronic record must not be

	duplicated in the paper record. 4. Page 8: 2.1 clarification of legislation 5. Page 9: 2.2 changes in medication should be recorded before the end of the working shift 6. Page 10: 2.5 information held on the electronic record must not be duplicated in the paper record. 7. Page 10: 2.5 removed filing results in paper records 8. Page 11: 2.5 information placed in a paper record due to electronic systems being unavailable should be transferred to the electronic record as soon as possible 9. Page 20: 3.1 dual record keeping guidance 10. Page 21: 3.1 accessing scanned records on CSCAN
Appendices / electronic forms	Not applicable
What is the impact of change?	Not applicable

Training requirements	Select - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	None

Financial resource implications	None

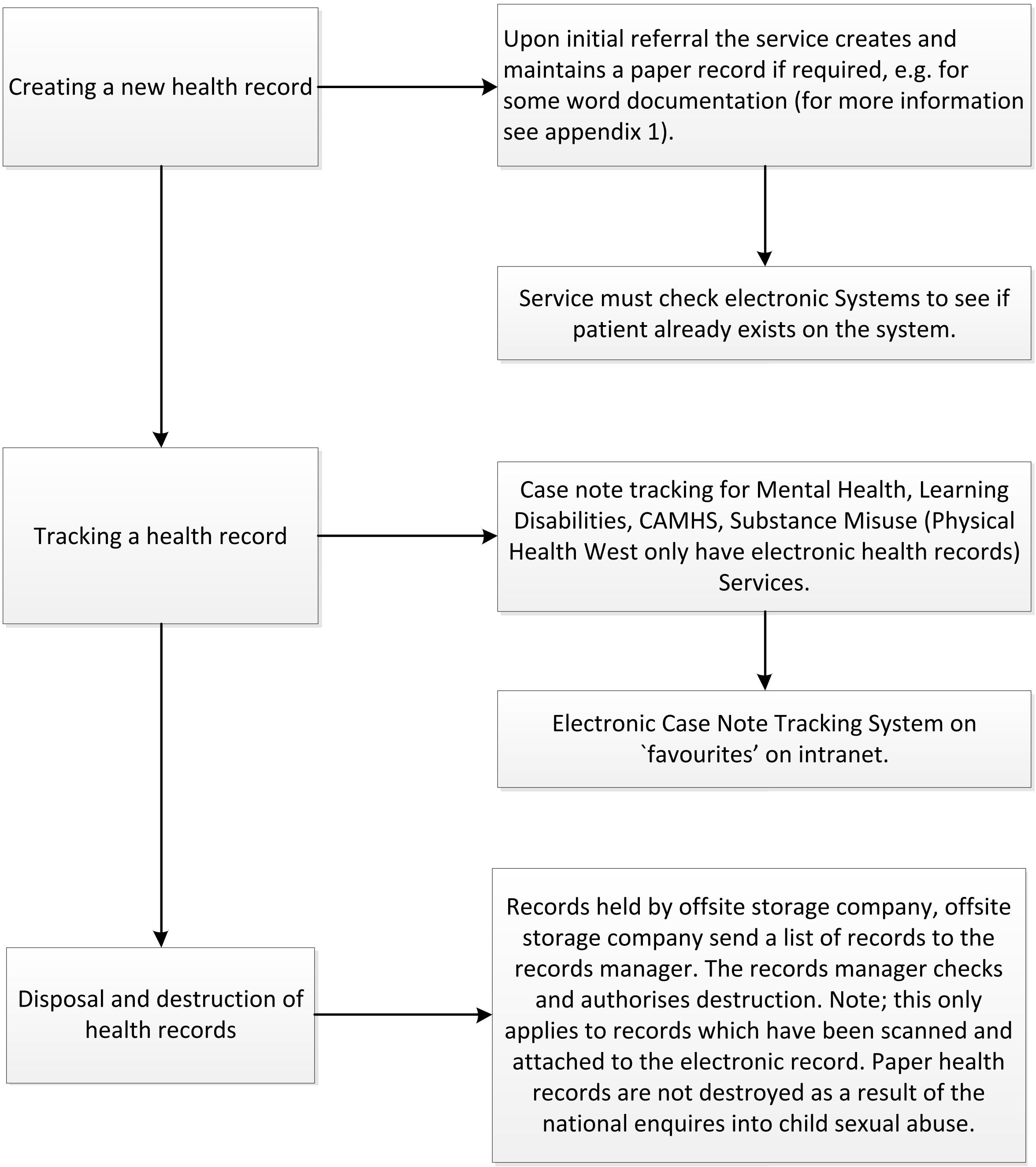
External references
1. Article 8 - European Convention on Human Rights; a persons right to be treated with dignity and respect and the need for maximum privacy through any invasive procedure 2. Mental Health Act Code Of Practice (2015) 3. Data Protection Act (DPA) 1998 plus the Information Commissioner's Office (ICO) guidance the DPA and use of violent warning markers 4. Secretary of State Directions to health bodies on dealing with violence against NHS staff (2003) and security management measures (2004) 5. Health and Safety at Work Act 1974 6. The Management of Health and Safety at Work Regulations 1999 7. Safety Representatives and Safety Committees Regulations 1977 (a) and 8. The Health and Safety (Consultation with Employees) Regulations 1996 (b)The Corporate Manslaughter and Corporate Homicide Act 2007. 9. GMC good medical records practice http://www.gmc-uk.org/guidance/ethical_guidance/13427.asp 10. NMC standards for record keeping https://www.nmc.org.uk/standards/code/ 11. Allied Health Professional Standards on Record Keeping 12. Independent Inquiry into Child Sexual Abuse NHS England records risk assessment best practice example BIP 0008:2008 British Standard on legal admissibility and evidential weight on scanned records

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
Not applicable		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	N/A	

Contents

Quick reference flowchart – Health records flowchart



Creating a new health record

Upon initial referral the service creates and maintains a paper record if required, e.g. for some word documentation (for more information see appendix 1).

Service must check electronic Systems to see if patient already exists on the system.

Tracking a health record

Case note tracking for Mental Health, Learning Disabilities, CAMHS, Substance Misuse (Physical Health West only have electronic health records) Services.

Electronic Case Note Tracking System on `favourites' on intranet.

Disposal and destruction of health records

Records held by offsite storage company, offsite storage company send a list of records to the records manager. The records manager checks and authorises destruction. Note; this only applies to records which have been scanned and attached to the electronic record. Paper health records are not destroyed as a result of the national enquires into child sexual abuse.

1. Introduction the review

This policy outlines national and Trust standards for health (clinical) records. The policy relates to both paper and electronic records. The electronic record is the primary health record and the paper `light file' is the secondary record. The paper record is used for documents which are not held electronically and as part of business continuity plans in the event of system down time. Further advice on any aspect of the enclosed policy can be gained from the Information Governance Lead/DPO. Records queries are logged by the Information Governance Lead/DPO and a log of records queries and responses can be found on the Information Governance section of the intranet.

Accurate health records are a tool of professional practice that should improve the care process for all patients. Good record-keeping can determine accountability; facilitate clinical decision making; improve patient care through clear communication of the treatment rationale; provide a consistent approach to team working; and help defend complaints or legal proceedings.

Making and keeping records is an essential and integral part of care and should not be seen as a distraction from its provision. These standards are to assist healthcare professionals to fulfil the expectations the Trust has of them, and to serve effectively the interests of patients and clients.

1.1 Explanation of terms

The following are definitions of terms used within this policy:

- **Health Record**

The Data Protection Regulation 2016/Data Protection Act 2018 describes the health record as personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status

- **Electronic record**

Within CWP the records held in dedicated electronic health records systems are the primary record and all issues reflecting changes in clinical risk or medication should be recorded in the electronic record before the end of a working shift.

- **Paper record**

Paper records are health records not initially recorded on electronic systems and include both handwritten records, and paper forms (such as rating scales and observation charts).

- **Paper Light Record**

Paper Light Records are paper records which only consist of the handwritten records and other paper forms that are not also recorded electronically, i.e. copies of letters and information held on the electronic record systems are not printed out for these records.

- **Basic record-keeping standards**

These are generic health record keeping standards that define good practice for health records and address the broad requirements that apply to all clinical record keeping.

- **Contemporaneous**

Contemporaneous records are made at the same time as the events they record.

- **Confidentiality**

Confidentiality is the duty to keep private or personal information safe and ensure that it is only used for the purposes for which it is given by those members of staff who are involved in a client's care.

- **Caldicott Guardian**

The Caldicott Guardian is a senior member of staff (usually one of the trust medical directors) whose duty is to ensure that patient information remains secure and is only used appropriately.

- **Access**

Access refers to the procedure by which the contents of the health record are examined, either by staff who are involved in the care of the client whose records are being looked at, or by others to whom the records are provided under the safeguards and procedures of the access to health records policy.

- **Dual record keeping**

Dual record keeping is where both electronic systems and paper records co-exist for a client within a service (for example, in the transition period when moving from paper to electronic systems). In these situations the electronic record will be the primary record for the client (as described above) information held on the electronic record must not be duplicated in the paper record.

- **Audit**

Audit is a process by which practice is checked against the standards set for that practice, so that the quality of the process can be measured and actions taken to improve the practice over time

2. Maintaining and improving the quality of health record keeping

2.1 Legal obligations that apply to records

The Trust has legal obligations relating to Health Records. This includes the General Protection Regulation 2016/Data Protection Act 2018, Access to Health Records Act 1990, Public Records Acts 1958 and 1967. In additional a number of professional bodies have issued guidance on maintaining good record keeping standards. A list of legislation relating to health records is listed below:

- Access to Medical Reports Act 1988;
- Access to Health Records Act 1990 (relates to deceased patients);
- Data Protection Regulation 2016;
- Data Protection Act 2018 (enshrines GDPR 2016 into UK law);
- Freedom of Information Act 2000.

Legal obligations that apply to health records will be reviewed on an annual basis or as a result of changes to the law. This will be completed by the Information Governance Lead/DPO and reported to the Information Governance & Data Protection Sub-Committee.

The **holder of the record** is the health service body by which, or on whose behalf, the record is held. The Trust holds our records on behalf of the Department of Health. **The records are not the property of individual healthcare professionals, nor of the patient or client.**

2.2 Process for making sure a contemporaneous record of care is completed

CWP expects accurate contemporaneous record-keeping in all formats regardless of how they are held, and will have an ongoing process of audit for record keeping. Health professionals involved in the patients care **should ensure** that the health record:

- Provides frequent, accurate, current, comprehensive and concise information concerning the condition and care of the patient against which improvement or deterioration can be judged;
- Includes assessments of the patient's condition and risk issues, risk assessments, diagnosis, care / treatment plans, ECT details, prescription sheet details, discharge arrangements;
- Includes details of factors (physical, psychological or social) that appear to affect the patient or client;
- Includes copies of the most recent care plan agreed with the patient;
- Includes records of treatments given (including prescriptions and ECT);
- Provides a record of any care issues that arise and the action taken in response to them;
- Records the chronology of events and the reasons for any decisions made;
- Clearly delineates between factual information and observations and opinion;
- Supports standard setting, quality assessment, audit and research;

- All issues reflecting changes in clinical risk or medication should be recorded in the electronic record before the end of a working shift;
- All entries must be made within 48 hours and electronic entries and documents must be confirmed/authorised/approved within 48 hours of creation in order to render them read only.
- The record of the care interaction between the health professional and patient should be recorded within the health record.

2.3 The importance of Effective Record Keeping

Effective record keeping is a means of:

- Communicating with others and describing what has been observed or done;
- Identifying the role played by the healthcare professionals;
- Organising communication and the dissemination of information among the members of the team providing care for the patient or client;
- Demonstrating the chronology of events, the factors observed and the response to care and treatment;
- Demonstrating the properly considered clinical decisions relating to patient care (if practitioners are deviating from NICE guidelines, reasons for doing so must be clearly recorded explaining the rationale for deviating, e.g. if prescribing differently to NICE guidelines);
- Ensuring that an opinion is not presented as a fact.

2.4 Principles of record keeping

Clear, accurate and legible records which report relevant clinical findings, decision making, information given to patients / carers, and any medication prescribed or other investigation or treatment, assist in the safe care and treatment of individuals.

Health records are to be maintained and structured appropriately so that clinical information is recorded in the right place to create a contemporaneous document which will:

- Determine accountability;
- Support effective clinical judgment and decisions;
- Show how decisions relating to patient care are made;
- Allow easier continuity of care;
- Promote better communication and sharing of information between members of the multi-professional healthcare team;
- Support patient care and communications;
- Support the delivery of services;
- Provide documentary evidence of services delivered;
- Identify risks, and enable early detection of complications;
- Help address complaints or legal processes;
- Support clinical audit, research, allocation of resources and performance planning.

For electronic records, the health records are kept within the appropriately secured electronic records systems.

For paper systems, the health records are kept in the appropriate section of the trust approved records file for that service. Paper records are held securely within designated secure storage sites within the trust and movements of paper records are electronically monitored using the trust's case note tracking database on the trust intranet, which is linked to the trust's Master Patient Index.

As keeping effective health records is an essential part of providing care to a patient, where a patient expresses the wish that no records are kept of their care, consideration would have to be given as to whether the patient was declining care and treatment. This should only occur after a full discussion of this with the patient.

2.5 Basic record keeping standards which must be used by all staff

The standards for record-keeping described below are consistent with the standards recommended by the professional bodies, and support the core values of the Trust. Examples of approved professional standards are found in the reference section of this document above.

As Cheshire and Wirral Partnership NHS Foundation Trust (CWP) provides services across mental health and physical health services, different electronic and paper record keeping systems will exist in differing areas of the trust. Within the trust, services should ensure that only one set of electronic and paper records exists for each service user for that service area.

Information held on the electronic record must not be duplicated in the paper record.

As a minimum, health records should be clear, legible documents that follow a logical and methodical sequence with clear milestones and goals for the record-keeping process.

Entries must:

- Be factual, consistent and accurate (all records);
- Be recorded as soon as possible after an event has occurred (within 48 hours), providing current information on the care and condition of the patient, recording if the notes are written some-time after the event, for paper records, if the date and time differs from that of when the records are written, this should be clearly noted under the signature, printed name and designation (in accordance with GMC good medical records practice, NMC standards and Allied Health Professionals standards);
- Record any advice given to patients e.g. advice to inform DVLA if unable to drive due to medication (all records);
- Be accurately dated, timed (ideally using the 24 hour clock system) and signed with the full name printed alongside each entry (paper records);
- Be written clearly, legibly and in such a manner that cannot be erased (this is best achieved by writing in black permanent ink) (Paper Records);
- Be consecutive, and filed in book order within each section (paper records);
- Be bound and stored so that loss of documentation is minimised (paper records)
- Be kept in manageable sized documents, by filing in a trust approved paper binder (paper records).

Staff must:

- Ensure that reports and results are seen, evaluated and signed by the practitioner before being scanned onto the patient's electronic record (electronic record) (see appendix 15 for scanning paper documents guidance);
- Where results are available via external electronic systems there should be a record of what has happened within the main body of the CWP electronic notes. If results are viewed at source this needs to be noted what this is, a comment should be then put into the patient's electronic record noting the review and outcome. Results may be printed off and scanned onto the patient's electronic health record for future reference. An audit trail of what has been done to support the clinical decision must be kept.
- Ensure that any unused legal forms are retained (e.g. Mental Health Act forms) and are clearly marked as "void" and stored within the patient records (paper records);
- Ensure that where entries are made by students and trainees who do not hold an NHS contract of employment, their entries should be read and countersigned by their Trust clinical supervisor (all records);
- Ensure that any notes dictated and typed in records should include the name and position of the practitioner, and should also be checked, corrected if necessary and signed or approved by the practitioner who dictated them (all records);
- Ensure that all items of appropriate "Minimum Data Sets" are recorded e.g. Mental Health Minimum Data Set (all records),

Ensure that where paper records are becoming too large, they are kept in separate volumes which are consecutively numbered in chronological sequence (paper records);The standards include the following restrictions:

- The use of abbreviations should be kept to a minimum, and where discipline-specific abbreviations are used for the first time, the term they are abbreviating should be written using the approved abbreviation lists which are approved by the Information Governance & Data Protection Sub-Committee. The list of approved abbreviations can be found on the intranet under Information Governance. (all records);
- Initials should not be used to identify staff involved in discussions – their names should be written out in full. Where more than one staff member is involved in a decision, the most senior professional present should be clearly identified (all records);
- Where any third party is involved in an incident, they should not be named in the care record, but the incident reported on the correct form (all records);
- Records of complaints and their handling are not to be stored in the main Health Record for that client, records of complaints should be held separately (all records);
- Records of incident investigations (including root cause analyses) are not to be stored in the main health record for that client; records of incident investigations should be held separately (all records),
- Erasers, liquid paper, or any other obliterating agents should not be used to cancel errors; a single line should be used to cross out and cancel mistakes or errors, and this should be signed and dated by the person who has made the error (paper records);
- Poly-pockets must not be used for storing sheets of paper in health records (paper records);

Good practice includes:

- Including contact details for medical staff seeing clients in in-patient settings (bleep or phone numbers) (all records);
- If clinicians use the phrase “See previous psychiatric history” they should specifically refer to the date of the assessment; (all records)
- Where there is no entry in the health record for a significant period the next entry should explain why (all records);
- All electronic communications relating to the care of a patient should be attached to the electronic health record , if electronic systems are not available, they may be printed off and placed into the paper health record e.g. e-mails between health care professionals or from/to the patient information placed in a paper record should be transferred to the electronic record as soon as possible ;
- Where e-mails are attached to the electronic systems, care should be taken to ensure that the content of these only includes information pertinent to the health record (electronic records),
- Where large gaps exist on pages within the paper record, a single line should drawn through the gap (paper records);

These standards should enable any record entry to be traced to a named individual at a given date/time with the secure knowledge that all alterations can be similarly traced; and on subsequent review any decision making can be justified.

Any individual making an entry into the health record should be aware that records are also made and kept in the event of being required by:

- The patient applying to have access to their own health records under Data Protection legislation;
- The patient’s solicitor for a third party litigation claim;
- Mental Health Act Tribunal;
- The patient’s solicitor in support of a clinical negligence claim against the Trust or another organisation;
- Individual staff to write a report for litigation claim;

- Individual staff to demonstrate that they have not been professionally negligent;
- The Trust for managing the incidents, claims and complaints processes;
- The Trust for conducting audits and research;
- The Trust for managing issues under Data Protection legislation.

2.6 Specific guidance

2.6.1 Advance Statements

As covered in the advance statements policy, advance statements that are provided by the patient **should** be attached to the health record, and the existence of the advance statement **should** be documented in the Alerts section of the records.

2.6.2 Recording consent to share information

The health records should record whether or not the patient has given consent for staff to make contact with their family / carers and other services involved in their care.

2.6.3 Recording change of gender and information regarding Transgender patients

Trans (Transgender) status forms part of an individual's history but is often irrelevant to why they are accessing services. For records of Transgender people:

- If there is any risk of ambiguity, clarify their preferred name and gender pronoun with the service user;
- Once a Transgender person has changed their name and gender all subsequent records must reflect this;
- It should be assumed that the service user is in receipt of a Gender Recognition Certificate – they should not be asked to provide this;
- Entries should only refer to Transgender status if clinically relevant to the immediate treatment and with the consent of the service user. This is most likely to be when recording their past medical/mental health history; relationship/family issues; and in relation to assessment and treatments for Gender Reassignment

To protect the special sensitivity of health records existing pre transition:

- There is a duty under the Equality Act 2010 not to disclose a Transgender persons previous status or identity to anyone including other members of staff without their consent;
- It is good practice to make a clinical summary of relevant events prior to transition, and to obtain the service user's consent before the use of this summary;
- Access to past health records with reference to previous gender should be restricted and take place only with the service user's consent.
- Placing an alert on the record stating that the patient has an old record quoting either the previous NHS number or the clinical systems number will not disclose the transgender person's previous status or identity on the new record but will enable clinicians to access clinically relevant information mitigating clinical risk to the patient.

The same duty of care applies equally to information obtained from other sources e.g. from other NHS Trusts, Social Services or Education records.

If further advice is required then please contact Trust's Equality and Diversity Co-ordinator

2.6.4 Record keeping for safeguarding purposes

Health records need to follow the principles outlined in the Safeguarding Children Policy and safeguarding adults policy. Records should include the issues identified; record the referral to the appropriate body and the outcome of the referral. Minutes of safeguarding meetings should be attached to the appropriate record, if the minutes record parenting issues then it will be appropriate to attach these to the relevant child's records.

2.6.5 Recording alerts in health records

Alerts should be used to bring to the urgent attention of staff, critical information in the event of an urgent / crisis situation e.g. safety of staff or others or legal requirements e.g. MAPPA.

For electronic records, a short description in the alert box should refer to a document within the electronic system for further detail. For Paper records, the alert box on inside front cover of records should contain short description of the alert and refer to the document within the record for more detailed information.
Information relating to adding a safeguarding alert for child and adult patients/clients are detailed in the Safeguarding Children and Safeguarding Adults policies. Domestic abuse / MARAC alerts will contain reference to MARAC conferences.

If the Trust receives information that a patient may be a serious threat to safety of the staff this should be recorded as described above on all electronic and paper records and the teams looking after the patient should be informed of this risk.

All alerts in health records should contain reference to where further details and information about the reason for the alert can be found within the health record and should be reviewed at appropriate intervals, so that the alert can be removed when no longer appropriate.

Note: alerts should not be used to record the patient's status regarding blood borne viruses.

2.6.6 Violent Patient Markers

2.6.6.1 Introduction

Under health and safety legislation, NHS bodies are accountable as employers for assessing the risks of violence to their employees and, if necessary, putting in place control measures to protect them. The development of a pro-security culture is integral to all strands of Security Management, including the tackling of non-physical assaults, as it underpins all other areas of generic action that follow. A pro-security culture amongst staff, service users, visitors and members of the public is one where everybody accepts the responsibility for security and the actions of a small anti-social minority who breach security will not be tolerated. In order to build a pro-security culture, it is essential that security awareness is communicated to all staff and members of the public that it is necessary that they should be vigilant and that they report all potential breaches of security.

This guidance document sets out the development of procedure clinical measures which include risk of CWP violence marker systems which all aim to:

- Provide an early warning for services of a particular individual or situation that represents a risk to them, their colleagues or other patients
- Provide security warnings and handling advice to services to avoid or minimise the risk
- Include a workable system for sharing marker information appropriately with all staff (both internal and external) who come face to face with the violent individual(s)
- Help reduce the number of violent incidents across the organisation

Where appropriate the Trust will co-operate with and work within the memorandums of understanding which have been agreed by the NHS and other national bodies. These include the National Patient Safety Agency, the Health and Safety Executive, the Police and the Crown Prosecution Service. The memorandums of understanding are not legally binding documents but agreed standards of practice which the professional bodies have signed up to.

It is intended that this policy will apply to all staff groups working across CWP health services. The policy relates specifically to incidents which contain;

- Physical or non-physical assaults [face to face, phone or electronic method]
- Intentional or unintentional acts of violence and aggression
- Acts committed by a patient or a patient's associate

- Incidents involving a dangerous animal.

2.6.6.2 Definitions

Senior Clinical Lead refers to the most appropriate senior staff i.e. Modern Matron or Heads of Operations

Consultant/Responsible Clinician refers to the most senior care team lead i.e. RC, Consultant GP or social worker
Non-physical assault: *'The use of inappropriate words or behaviour causing distress and/or constituting harassment.'* NHS Protect. (2012).

Physical assault: *'The intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort.'* NHS Protect (2012)

Unacceptable or inappropriate behavior: *any incident where a staff member feels, harassed, abused, threatened, bullied (not by a colleague), insulted in circumstances relating to their work or whilst they are at work.* The Health and Safety Executive (HSE).

Violent Patient Marker (VPM): *Is a visible electronic or paper marker applied to a care record to indicate a level of risk following an incident of violence associated with a particular service user or relative/next of kin*. NHS Protect. (2012).

Violence refers to *'Any incident, in which a person is abused, threatened or assaulted in circumstances relating to their work. This can include verbal abuse or threats as well as physical attacks.* The Health and Safety Executive (HSE).

2.6.6.3 Procedure

A key element of pro-security culture is to encourage staff to take an active part in maintaining a safe and secure environment within the Trust. It is important that the staff working for the Trust, are aware of the procedures in place to deal with security-related incidents and that they are fully aware of their statutory requirements within the workplace. Equally it is important that service users and visitors are fully aware of the standards of conduct expected of them and the sanctions that may follow if they behave unacceptably. Communication is an important aspect of engendering a pro-security culture, where the responsibility for security is accepted by all and a strong message communicated to the staff, patients and members of the public alike that non-physical assaults on CWP staff will not be tolerated.

The management of disturbed and violent behaviour frequently can involve interventions to which an individual does not or cannot consent to. It is therefore essential that CWP staff use interventions that are in accordance with best practice and the law. Failure of the Trust or individuals to act in accordance with guidelines i.e. law, both criminal and professional, may not only be a failure to act in accordance with best interest but in some circumstances have legal consequences.

Any intervention used to manage violence, aggression and challenging behaviour must be a reasonable and proportionate response to the risk it seeks to address. This policy does not replace the reporting of incidents to the police and all incidents must be reported in accordance with CWP policy (please see CP6 The Management of Challenging Behaviour, Violence and Aggression policy).

2.6.6.4 Incident process

When an incident occurs and is reported through CWP reporting systems there must be an appropriate level of escalating action by the senior clinician/line manager or consultant. Local action may involve the issuing of verbal warnings, the marking of a service users electronic record. Applying a VPM will normally be applied where the individual causing concern to CWP staff member is a service user, however equally this can be applied where the individual is a service users associate (e.g. friend, relative or guardian). Incidents of assault which involve clinical and non-clinical elements will equally be assessed for the implementation of a marker;

- Where it has been deemed following an incident that the service user lacks capacity a marker will only be applied to their electronic care record
- Where it has been deemed following an incident the service user/assailant has capacity a marker will be applied to their electronic care record and the acceptable behaviour agreement process will apply.

2.6.6.5 Factors to consider (refer to Appendix 1)
All clinical services have approved documentation for the assessment of risk and these tools must be referred to as part of the review process. There are specific risk factors that will be considered when determining whether a service users electronic care record should be marked, this will include the following:

- nature of the incident (i.e. physical or non-physical)
- degree of violence used or threatened by the individual
- injuries sustained by the victim (including psychological)
- the level of risk of violence that the individual poses
- the medical condition and medication of the individual at the time of the incident.
- whether an urgent response is required to alert staff
- impact on staff and others who were victims of or witnessed the incident
- impact on the provision of services
- history of any previous incidents and/or the likelihood that the incident will be repeated
- any time delay since the incident occurred
- the individual has an appointment scheduled in the near future
- whether staff are due to visit a location where the individual may be present
- whether the individual is a frequent or daily attendee (e.g. to a clinic or out-patients) or an in-patient
- whether staff may come into contact with the individual while working alone
- whether the incident, while perhaps not serious itself, is part of an escalating pattern of behaviour
- The use of a weapon in the incident

a) Reporting and investigating
It must be emphasised that the decision to issue a VPM on their electronic care record will be based on a specific incident which has been reported through CWP Datix reporting systems.

b) Decision-making process (refer to appendix 2)
The decision to implement any formal process post incident will remain with the clinical services e.g. senior clinician/line manager. CWP Safety & Security Lead will support the clinical services with the decision making process and also the management of review of any marker which is placed on the service users electronic records.

c) No decision reached on post action required
Post incident in circumstances where a decision for action cannot be agreed between clinicians the LSMS must be contacted for advice. In these circumstances the LSMS will have the overriding decision whether to implement or not any action.

2.6.6.6 Verbal Warnings
To demonstrate a reasonable approach to incidents all post incident verbal warnings must be undertaken in a timely and appropriate manner with all the persons involved and recorded into the electronic patient record. A service user has the right to be formally represented by an Advocate, family member or by CWP Patient and Carer Engagement Team. To ensure the safety of all persons the environment and support systems available must be considered by staff preparing to communicate to the offending persons.

a) Where a service user, relative or visitor is violent or abusive, a member of staff must explain to the service user what is and is not acceptable behaviour and he/she should outline what the possible consequences of any further repetition of unacceptable behaviour could be. A suitable member of staff should always witness this explanation.

b) Verbal warnings are a method of addressing unacceptable behaviour with a view to achieving realistic and workable solutions. They are not a method of appeasing a difficult service user, relative or visitors in an attempt to modify their behaviour, or to punish them, but instead to determine the cause of the behaviour so that the problem can be addressed or the risk of it reoccurring minimised.

c) It is important that all service users, relatives and visitors are dealt with in a demonstrable fair and objective manner. Every attempt should be made to de-escalate a situation that could potentially become abusive. Where de-escalation fails, the service user, relative or visitor should be warned of the consequences of future unacceptable behaviours. The incident should also be reported and recorded on the Datix incident reporting system.

d) Where it is has been agreed and deemed appropriate to approach a service user, relative or visitor in respect of their behaviour, this should, where practicable, be done informally, privately and at a time when all parties concerned are composed.

The main aim of the Verbal Warning process is twofold:

- To ascertain the reason of the behaviour displayed as a means of preventing further incidents or reducing the risk of them reoccurring; and
- Ensure that the service user, relative or visitor is aware of the consequences of his/her further unacceptable behaviour.

e) Verbal Warnings will not always be appropriate and should be only attempted when it is safe to do so with the relevant and appropriate staff present and if necessary this could involve the police where this has been previously agreed with them.

f) A meeting should be arranged and conducted in a fair and objective manner. A formal record should be made and maintained within the service users electronic care record.

g) Where the process has no effect and unacceptable behaviour continues, alternative action must be considered and acted upon. The use of Acceptable Behaviour Agreement letters could be used to support further action. (see CP6 Violence and Aggression policy for further support)

2.6.6.7 Electronic markers

a) **Placing a marker on records**
Following each incident of violence or aggression CWP staff must complete a Datix incident form. Each Datix incident is reviewed and categorized according to severity by the authorised senior clinician/line manager. At this point it will be assessed by locally the senior clinicians/line managers if it is appropriate to place a marker on a service users electronic care record.

b) **Access to service users records**
Any decision to implement placing a marker on service users electronic care record must only be done through the senior clinical lead/line manager within the service line or Care Team.

c) **Essential information**
Essential information which must be included on all markers;

- Who, or what the marker applies to
- A brief classification of the type of incident
- Date the marker is effective from
- Whether the service users /individual has been notified
- Essential and relevant handling information or advice to staff
- Date for review.

Additional information to help staff manage the risks may include:

- A brief description of the incident, e.g. physical or non-physical assault
- Information relating to an service users medical condition, treatment and care if relevant
- Advice that the individual should not be denied treatment and care
- Security warnings, specific areas of risk or trigger factors
- Actions for staff who work off-site or out of hours and/or a relevant contact in case of another incident (e.g., LSMS, security personnel or police).

d) **Applying the electronic record**

Following each incident of violence towards CWP staff the senior clinician/line manager must;

- Ensure that an electronic/paper marker is applied to the service users electronic care record.
- Ensure that the Consultant/Responsible clinician is notified as soon as possible post application of the marker being inserted onto the service users electronic care record.
- Ensure that the Care Team is made aware of the incident and agree the process going forward.
- Complete a new Datix incident form, detailing all actions

e) **Service users associate**

Where the incident was committed by a service users associate/next of kin and when a marker is also placed on the records of the service user with whom the violent individual is associated, the senior clinician/line manager must make clear whom the marker applies to, in order not to stigmatise the service user unfairly.

f) **Dangerous animals**

If an animal is involved in an incident (e.g. a dangerous dog) and the individual service user is responsible for the animal, their records should indicate this and include advice relating to the animal. To minimize future incidents the venue for clinical visits could be relocated to a safer environment.

g) **Notifying the service user and/or individual** (refer to appendix 4)

Where it is identified that the perpetrator of the violent incident had at the time had capacity the senior clinical lead within the service line will be responsible for sending a notification letter to the individual following the decision to place a marker on their electronic care record. This letter must be sent as soon as reasonably possible post incident.

In situations where the incident was committed by an associate of the service user, a letter should be sent to both the service user and the associate advising them of the action being taken. In the event that the associates address is unknown CWP staff must give the letter by hand the next time the associate has contact with CWP staff or service. A copy of the letter must be kept within the service users case notes.

Each individual must be made aware of what that information associated with a marker may be shared, with whom, and for what purpose. The information contained within the marker may be shared with other health professionals in compliance with Data Protection legislation.

h) **Decision not to notify**

The ICO guidance *'Data Protection Good Practice Note - The use of violent warning markers'*, which recommends not notifying the individual in the following situations:

- Where informing the individual may provoke a violent reaction and put staff at further risk
- Where notification of a marker may adversely affect an individual's health.

If there is an immediate risk to CWP staff from any individual as a result of receiving a letter notifying of a marker being placed on their electronic care record staff must assess the need of informing the police for support. CWP Safety & Security Lead must also be contacted for advice. All action taken must be fully documented into the service users electronic care record.

i) **Supporting the victim**

CWP Safety & Security Lead can be contacted by the individual affected or by the senior nurse/line manager for support and advice. Also for further advice on staff support please refer to the *'Guidance on accessing staff support and counseling service (HR14)*'.

j) **Process**

Once an electronic marker has been applied to the service users electronic care record by the senior clinician/line manager the Consultant/Responsible Clinician [or senior care lead] will be responsible for;

- Ensuring the regular review of the suitability for the continued use of the marker on the service users electronic care record
- Ensuring that all referring agencies are made aware of all violent patient markers which may have been applied.
- Ensuring that all persons are made aware of the decision to remove the marker on the service users electronic care record
- For receiving all marker information from the commissioning body or other providers and for relating all known risks to the appropriate clinical team.

k) **Reviewing a marker**

The Consultants and/or Responsible Clinician [or senior care lead] will be responsible for;

- Reviewing each marker placed on the service users electronic care record
- Agreeing a date for the review of the marker
- A Care Team discussion is held which involves the review of the incident leading to the marker being placed on the service users electronic care record
- Involving the service user or Advocate/Nearest relative in all decision concerning the marker

l) **Review Criteria**

When reviewing the marker the Care Team must consider the same criteria as when the marker was first placed on the electronic care record following the incident e.g.:

- The severity of the original incident and the impact on the staff member
- Any continuing risk that an individual may pose
- Any further incidents involving the individual
- Any indication that the incident is likely to be repeated
- Outcome of further investigations
- Any action taken by other agencies, e.g. police or the courts
- Other developments since the original incident

m) **Outcome of review notification** (refer to Appendix 5).

The service user will be informed by their Consultant and/or Responsible Clinician of any review date of the marker, this includes the decision to remove any VPM.

n) **Handling complaints** (please refer to the Complaints policy GR4).

All complaints about a decision made to place a marker on their electronic care record made by the service user and/or other must be referred through CWP complaints process.

o) **Data Subject Notices**

Under the Data Protection legislation the individual whose electronic care record have been marked has the right to issue a 'Data Subject Notice' to the data controller (the health body) to prevent information sharing which would cause unwarranted damage or distress.

2.6.6.8 Information sharing with external agencies

Data Protection legislation allows all information which is related to the protection of the public can be passed on without the individuals consent. All concerns and arising issues relating the sharing of information must be shared with CWP Records Officer.

2.6.6.9 Audit, review and monitoring

Following the decision to apply a VPM the senior clinician/line manager must complete a new Datix incident form, detailing all actions.

2.6.6.10 Contacting the Police

(please refer to the Management of Violence and Aggression policy CP6).

Emergencies - CWP staff have a duty to maintain safe environments and to safe guard the wellbeing of vulnerable others. When a situation arises where it is believed that this duty of care is compromised and cannot be maintained i.e. control is lost, staff must contact the police.
When a situation arises which involves significant threats to others or imminent threat by use of a weapon staff must also contact the police immediately. These situations will require a rapid police attendance and staff must dial (9)999, giving exact location and stating that an emergency response is required.

Non-Emergencies - For all non-emergency situations where there is no significant loss of control but still requiring a police attendance staff must contact the police using the numbers stated below. These types of situations would be to ask for a police presence in order up hold the law or to carryout CWP policy i.e. missing service user. In situations in which staff are reporting an alleged assault but do not require a police attendance this must be clearly stated when giving details in order to obtain a police incident number. By making clear to the police this action will avoid unnecessary attendance at CWP premises by the police.

Police should be contacted via:

- 101 **(Non-emergency only)**
- 999 **(Emergency only)**

2.7 Information held on shared drives

For technical reasons, some clinical areas use shared drives to store electronic documents about clients, which have not been attached to electronic Health Record systems (specifically the electronic patient record, but this may also apply to all systems). In some cases these are work in progress or drafts, but in others may just be documents that administrative staff have not attached to the system. Staff should be aware that what is viewed on the electronic system and paper record may not be the whole record and administrative staff in clinical areas should be contacted to locate any additional information. If information is held on a shared drive an alert should be placed on the electronic health record stating this.

2.8 Recording the death of a patient

When a patient dies the appropriate member of staff, i.e. the person who is informed about the death, should ensure that both the paper and electronic records note the date of death. Staff must contact the clinical systems team to ensure that all Trust systems are checked to record the death of the patient.

2.9 Record keeping in private establishments

If Trust health professionals visit patients who are receiving care in a private setting, then they should make detailed entries into the private establishment's health records for the patient. Trust records should not be left in private establishments (or any establishment which is not part of CWP) for the purpose of recording visits. The private establishments have a separate legal duty to maintain their own records.

2.10 Standards / Key Performance Indicators

Standards and Key Performance Indicators against which this policy will be monitored include the Data Security & Protection Toolkit, CQC Standards and the Guidance on Record Keeping Standards produced by the professional and academic bodies of the various health professionals working within the Trust. These will be reviewed at least annually, or when new guidance is issued to ensure that the policy and audit of the policy is up to date.

2.11 How the organisation trains staff in line with the training needs analysis

Employees will be provided with training to enable them to meet the expectations of the Trust as described within this policy and to ensure compliance within the legal framework and national guidance. This will form part of the trust's Essential Training requirements and will be monitored through the Education Department. Training requirements for staff are detailed within the mandatory employee learning policy.

2.12 Monitoring compliance with the policy

2.12.1 Audit

By auditing health records and acting on the results, the Trust will assess the standard of record-keeping. This will allow the Trust to identify any areas where improvements can be made.

The Information Governance & Data Protection Sub-Committee will ensure that a comprehensive audit of health records is performed on an annual basis, measuring compliance against the standards of this policy and that an action plan is produced to tackle issues identified. This will be reported through the mechanisms described above to ensure that the actions identified are completed.

See appendix 13 for the current audit tool.

3. Management and administration of health records

3.1 How a new record is created

For a number of years the electronic record has been the primary patient record across all services. Wards currently use a paper light file for documents not yet held electronically and for emergency/ contingency situations in the event of system down-time, e.g. when there are system upgrades.

The paper light file should therefore not be used as the primary means of documenting paper history sheets or storing letters. If a paper history sheet is created for a patient, e.g. for practical reasons when seeing a patient in the community in the absence of a mobile device, this documentation **must be scanned in and attached to the patient's electronic record as soon as is practically possible**.

This is to ensure that critical clinical information about a person's care and treatment can be accessed by the wider care team. Once attached to the patient's electronic record, the paper version **should be disposed of** confidentially. Dual records, where both electronic systems and paper records co-exist for patients, must not be created. CQC have previously advised the Trust that they consider **dual records to be a risk.**

Where services are using electronic health records, a new record should only be created by staff after checking that no previous record exists for that client within the electronic system. Where a service has full electronic records there is no need to create a paper record. Where a paper record does not exist for a patient this can be shown on the case note tracking system by entering `0' against number of volumes and a comment may be entered onto the tracking system.

The current electronic records in use within the Trust are as follows:

System	Where used
Dedicated systems	
CareNotes	Adult mental health, Learning Disability Services, CAMHS.
EMIS-Web	Physical Health West (PHW)
PCMIS	Primary care mental health – West, East and Central Cheshire
Choose & Book	To access referrals
Summary Care Record	Tracing NHS/Patient details

System	Where used
Additional systems currently in use – Physical Health West (PHW)	
Liquid logic	Re-ablement and crisis re-ablement
Adastra	GP Out of Hours Service
Oracle	PHW– health visiting, district nursing, SALT therapists, evening/ night nurses
Cheshire Care Record	Available Trust wide via a link on the patient's electronic health record
C-SCAN	Drive available to authorised staff which holds scanned copies of historical records

For details of how to create a new record please follow the relevant electronic systems manuals.
Note: C-SCAN which is a separate drive holds scanned copies of historical paper health records. Adopted children's files are held in a separate file within CSCAN. Please refer to the standard operating procedure for accessing records via CSCAN. To access records which have been scanned contact the usual administrative staff who will have access to the scanned files and will be able to email them to staff. To preserve server space avoid attaching scanned files to clinical systems as the scanned files are already held within the network.

3.2 Storage and security measures

The following principles apply:

- Health records should be kept securely and access to them should be controlled on a 'need to know basis';
- Rooms in which paper health records are stored should be locked whenever they are left unattended. The records must however, be accessible 24 hours a day (e.g. by security);
- It is acceptable to store paper health records on open racking, as in most records libraries, providing that the room/building is secure;
- When paper health records are transferred between departments they should be sent in a sealed envelope or container. They should only be carried by Trust-authorised personnel;
- A patient's health records should not be handed to anyone who is not authorised to have access to them;
- Health records should never be left unattended in public areas. If a stranger is seen looking at patient's health records, check their identity and ensure they have the authority to handle health records.

3.3 How health records are tracked when in current use

The movement of paper health records throughout the trust is monitored and logged on the Case Note Tracking system, linked to the Trust Master Patient Index on the Trust Intranet. The process records the movement of records, by checking out each individual volume of paper records being taken from one location and recording their safe arrival at their destination. Reports of tracking are done for the Information Governance & Data Protection Sub-Committee and discussed as a standing agenda item. Staff should see appendix 7 for further details.

3.3.1 Missing records

When a service finds that paper records are missing extensive searches should be undertaken. If the records are still not in the location expected on the case notes tracking system, they should fill in a DATIX incident form to record the incident. The Information Governance & Data Protection Sub-Committee will monitor all reports of missing records.

3.4 Carriage of Paper Health Records off site

Healthcare professionals may need to take patient's health records from the team base / department, to facilitate seeing patients in community settings. Only those records required for this purpose should be removed for the minimum practical time. The paper records must be checked out of the team base using the Case Note Tracking system and then checked in on their return, so that their location is always known.

When a healthcare professional is not starting their working day from their team base / department, the required records may be removed at the end of the preceding working day.

When a healthcare professional is not returning to their team base / department at the end of their working day, the records should remain in a secure case in the safest location available until their return.

Records should be stored and carried in a secure case, and kept out of public view when transporting them. Records left in cars should be kept in a locked boot or covered luggage area and car alarms used when fitted. If health records are being kept out of the team base overnight, they should be kept in the secure case overnight in the most secure location possible, ensuring that others do not have access to them.

When in the community, ideally, only those records for the patient(s) to be seen in the current building should be taken in. The remaining records should be left in the car out of view. However, if it is considered that it would be safer from a theft and / or risk management point-of-view to take all records in to the building, then these should be taken in and should not be left unattended at any time.

3.5 Sending health records by post

If health records are sent via the external postal system, they should be sent recorded delivery and recorded in the electronic Case Notes Tracking system. A check should be made to ensure their safe return. Robust envelopes should be used. A note should be fixed on to return the records, including the name, title and full postal address of who the records should be returned to and by what date if appropriate.

3.6 Process for closure of paper records

Some services have reached the decision to go completely paperless. When this decision is reached the paper record must be closed with a record of the date of closure. It is good practice to upload a summary of the paper record to the electronic record. An alert should also be created on the electronic record that a paper record exists. See appendix 8 for flow chart for closure of paper records. See appendix 9 for sample of summary of paper records used by Starting Well team.

3.7 How health records are archived and retrieved from storage

Some areas of the Trust have limited space to store archived records and therefore send records to off site storage facilities. Services must keep a log of which records have been sent to off site storage companies either on the electronic case note tracking system or for Physical Health West services on appropriate form (SR10). The offsite storage company has a responsibility for the provision of a retrieval and storage service. The transport and retrieval arrangements comply with national legislation and policy. Please see appendix 10 and appendix 10a for the processes of archiving and retrieving records from both internal and offsite storage facilities.
Note: Physical Health West Child Health Services hold scanned child health records which are accessible on a separate shared drive which is accessible by all staff who need access to those records. This process is covered by a separate Standard Operating Procedure.

3.8 Process for retention, disposal and destruction of records

NHS health records are ‘public records’ as outlined in the Public Records Acts 1958 and 1967. The health records of individual patients will not normally be preserved permanently, other than by way of samples. The Trust will select and deposit samples in agreement with local record offices, which have suitable facilities and are prepared to house such records. Those health records selected for permanent preservation should be transferred to a place of deposit appointed by the Lord Chancellor for that purpose. The remainder should either be destroyed or be retained by the Trust for its research or litigation purposes in line with the processes outlined below.

3.9 Minimum retention periods for NHS health records which are not for permanent preservation

The following recommendations are intended to give guidance on the destruction, at the earliest possible date, of all records which have not been identified as suitable for permanent preservation or which are no longer required for their original purpose: The Department of Health's advice is that the retention periods proposed are acceptable by the Courts. See also NHSX_Records_Management_Code_of_Practice_2020

All departments in the Trust should have an active destruction plan/programme.

Type of Record	Retention Guidelines
Records relating to children and young people (including paediatric, vaccination and community child health service records).	Until the patient's 25th birthday or 26th if entry was made when young person was 17, or 8 years after death if sooner.
Records relating to mentally disordered persons within the meaning of the Mental Health Act 1983	20 years from the date at which, in the opinion of the doctor concerned, the disorder has ceased or diminished to the point where no further care or treatment is considered necessary, or 8 years after death if sooner.
Records used for research purposes	Retain in accordance with applicable legislation and in accordance with the maximum period of time permitted by the hospital, institution or private practice NB Documents can be retained for a longer period, however, if required by the applicable regulatory requirements or by agreement with the sponsor. It is the responsibility of the sponsor to inform the hospital, institution or practice as to when these documents no longer need to be retained.
All other personal health records	8 years after the conclusion of treatment.

3.10 Process for disposal and destruction of records

Please see appendix 11 for a flowchart demonstrating the process for the destruction and disposal of Paper Health Records. When services, or records libraries, find that they are running out of space to store records, they should review the records held and pull out the records for patients which have not been seen for the longest period of time. The boxes containing the records should be marked with the destruction date, in accordance with the department of health retention periods e.g. 20 years post discharge for mental health records or 8 years post discharge for general records, 25 years for children and 8 years from death for all records. These older records should then be sent to the off site storage company. The off site storage company will then destroy the records when they reach the department of health guidelines for destruction. Certificates of destruction are obtained for all records which are destroyed. Copies of certificates are kept by localities which records are sent from e.g. records libraries or Trust services. Services which hold records which reach the destruction date must log any records destroyed. For details of full process see Standard Operating Procedure for Archiving Records with Dataspace (IM8).

Note: The Independent Inquiry into Child Sexual Abuse has resulted in a suspension of destruction of all records. The exception is where the full paper record has been scanned and attached to the patient's electronic health record.

3.11 Video / audio recordings

Some departments make use of audio and visual recording as part of the treatment of the patient. The audio/visual recording forms part of the record and may be subject to access by the patient etc. As the recordings are viewed as supplemental to the main clinical records, they may be erased after they are no longer required, however, patients should be informed of the use and retention period of the recordings. The model consent form in appendix 12 is developed from guidelines produced by the General Medical Council and Royal College of Psychiatrists.

3.12 Securing a health record in the case of a serious case / management review

In the event of a serious case review, e.g. children or vulnerable adults who have died or been subject to abuse or neglect is suspected, the health records should be secured to ensure that the record can be monitored so that no changes can be made, using the following method:

1. A clinical note to be written in the paper record "These records have been secured for a potential serious case/management review (Time and Today's Date)"
2. A clinical note to be written in the electronic record "These records have been secured for a potential serious case/management review (Time and Today's Date).
3. Notification of the request to be made to the Clinical Systems Manager for electronic records so that the electronic record can be "locked down" to prevent the addition or alteration of records.
4. An electronic copy of the electronic record to be taken as at the date of the clinical note and the record to be placed in the secure system by the Clinical Systems Manager.
5. The electronic copy to be used for comparison if any suspected change has been made.

Any suspected changes can then be identified by using the paper copy or the saved electronic copy.

3.13 Breaches of confidentiality

If there is any breach of confidentiality regarding health records an incident form should be completed immediately in line with the incident reporting and management policy. Any incidents relating to Data Protection / confidentiality issues should be notified to the Information Governance Lead (Data Protection Officer). The aforementioned manager will liaise with the Caldicott Guardian and the relevant service will inform the data subject verbally and then by letter.

Appendix 1 - Examples of the types of incident that may warrant a marker

It is not possible to list every category of incident which may warrant marking a service users electronic care records. Not only will the nature of the incident have to be considered but also the effect the incident has on all of those involved (staff, patients, relatives and visitors) and the likelihood of a further incident taking place.

CWP uses two definitions to establish a nationally consistent reporting standard within the NHS. Staff should be familiar with these definitions so that they know what types of incidents should be reported to CWP Security Services Manager. The following definitions and categories are applicable when considering placing a marker on records and each category should include appropriate handling information. Note: These lists are not exhaustive.

Physical assault is defined as: *'The intentional application of force against the person without lawful justification resulting in physical injury or personal discomfort'.*

Type of categorised physical assault
• Physical assault (no physical injury suffered) *Spitting & verbal threats
• Physical assault (physical injury sustained)

Non-physical assault is defined as: 'The use of inappropriate words or behaviour causing distress and/or constituting harassment'.

Type of categorised non-physical assault
• Offensive or obscene language, verbal abuse and swearing2
• Brandishing weapons, or objects which could be used as weapons
• Attempted assaults
• Offensive gestures
• Threats
• Intimidation
• Harassment or stalking
• Damage to buildings, equipment or vehicles which causes fear for personal safety
• Offensive language or behaviour related to a person's race, gender, nationality, religion, disability, age or sexual orientation
• Inappropriate sexual language or behaviour

N.B. some of the above examples of non-physical assault can be carried out by phone, letter or electronic means (e.g. e-mail, fax and text).

* Spitting is included in the definition of a physical assault, in circumstances where the spittle hits the individual.

* The use of swear words may warrant a marker depending on the circumstances in which they are used. For some individuals, swear words may be used in everyday speech, however a marker should be considered where swear words are used aggressively.

Appendix 2: Risk factors checklist

The following checklist provides the main risk factors which should be considered when determining whether a record should be marked. This could be incorporated as part of the risk assessment process and should be completed by the senior clinicians and/or other managers and staff as appropriate, following an incident of physical or non-physical violence or aggression against a member of staff.

(Please note that this list is not exhaustive, and it is likely that other factors will come into play when assessing the level of risk of violence that an individual poses.)

No.	Question	Yes /No
	Was the incident of a physical nature?	
	Did the victim sustain any injuries?	
	Did the victim (or witnesses) require medical and/or psychological attention following the incident?	
	Is an urgent response required to alert staff?	
	Did the incident involve a patient's associate (relative or friend)?	
	Did the incident involve a dangerous animal?	
	Does the individual or associate have a history of previous incidents of violence or aggression?	
	Is it likely that the incident will be repeated?	
	Is the incident, if not serious itself, part of an escalating pattern of behaviour?	
	Did the incident (or will future similar incidents) impact negatively on the ability of staff to provide services?	
	Does the individual have an appointment scheduled in the near future?	
	Are staff due to visit a location where the individual (and associate, where applicable) may be present in the near future?	
	Does the individual attend (e.g. a clinic or out-patients) frequently or daily?	
	Is the individual an in-patient?	
	Are staff likely to come into contact with the patient or associate while working alone?	
	Does the individual have a medical condition or was the individual taking medication at the time of the incident which may have influenced his/her actions? (requires advice from a senior clinician)	
	Are other patients at risk?	

Appendix 3 - Proforma for risk of violence markers

Patient Name				
NHS number				
Name of individual accused of incident				
Relationship to the patient				
Dangerous animal involved?	Yes	No	**Date of incident**	
Datix incident number		**Police incident number**		
Description of Incident				
Please indicate:	Physical		Non-physical	
Injury sustained	Yes		No	
Incident details;				
Electronic records also marked	Yes	No		
Effective date				
Agreed management plan and advice for staff;				
In the event of a further incident:				
Complete Incident Form:	**Contact CWP LSMS:**	**Contact the police:**	**Other contact;**	
Detail all relevant medical conditions or medications?				
Patient or Nearest Relative, advocate been notified?	Yes	No		
Other Comments:				
Completed by: (print name)			**Dated**	

An electronic copy of this form must be sent to CWP Security Services Manager – ken.edwards1@nhs.net tel: 07827307334

Appendix 4 - Template for marker notification letter

Dear (individual's name)

Notification of risk of violence marker being placed on an NHS electronic care record

I am writing to you from Cheshire and Wirral (CWP) Trust where I am the (include role/job title). Part of my role is to ensure that our staff are protected from abusive and violent behaviour when carrying out their duties. It is in connection with this that I am writing to you.

(Insert summary of behaviour complained of, include dates, effect on staff/services and any police/court action if known)

Behaviour such as this is unacceptable and will not be tolerated. CWP is firmly of the view that all those who work in or provide services to the NHS have the right to do so without fear of violence, threats or abuse. The NHS Constitution makes it clear that just as the NHS has a responsibility to service users, so service users have a responsibility to treat staff with respect and in an appropriate way.

All employers have a legal obligation to inform staff of any potential risks to their health and safety. One of the ways this is done is by marking the electronic care record of individuals who have in the past behaved in a violent, threatening or abusive manner and therefore may pose a risk of similar behaviour in the future. Such a marker may also be placed to warn of risks from those associated with service users (e.g. relatives, friends, animals, etc). A copy of the trust policy on risk of violence markers is enclosed/can be obtained from [insert details]

I (or the panel – insert panel name) have carefully considered the reports of the behaviour referred to above and have decided that a risk of violence marker will be placed on your records. This information may be shared with other NHS bodies and other providers we jointly provide services with (e.g. ambulance trusts, social services and NHS pharmacies) for the purpose of their health and safety.

This decision will be reviewed in (6/12) months' time (insert date if known) and if your behaviour gives no further cause for concern this risk marker will be removed from your electronic care record. Any other provider we have shared this information with will be advised of our decision.

If you do not agree with the decision to place a marker on your record, and wish to submit a complaint in relation to this matter, this should be submitted in writing to:

(Insert complaints service/panel details. N.B. Even if a panel is being used details of complaints process should still be included.)

Yours (sincerely/faithfully),

Insert name, job title and contact details

Appendix 5 - Template for notification of the removal of a marker

Date:

Dear (individual's name)

Notification of risk of violence marker being removed from an NHS electronic care record

I am writing to you from (insert name of trust), where I am the (job title). I wrote to you previously on (date/reference) concerning the placement of a risk of violence marker on your electronic care record after careful consideration of an incident...

(Insert summary of behaviour complained of, include dates, effect on staff/services and any police/court action if known)

This risk of violence marker was recently reviewed after a period of 6/12 months. After careful consideration, I (or the panel – insert panel name) have decided that there is no further cause for immediate concern.

(State specific reasons for the decision, if any.)

Therefore, the risk of violence marker has been removed from your electronic care record. Any other provider with whom we have shared this information will also be notified of our decision to remove the marker.

However, you should be advised that any future incidents in which you are involved, and which indicate a risk to staff of physical or non-physical violence or abuse, may result in a risk of violence marker once again being placed onto your records. Behaviour such as this is unacceptable and will not be tolerated.

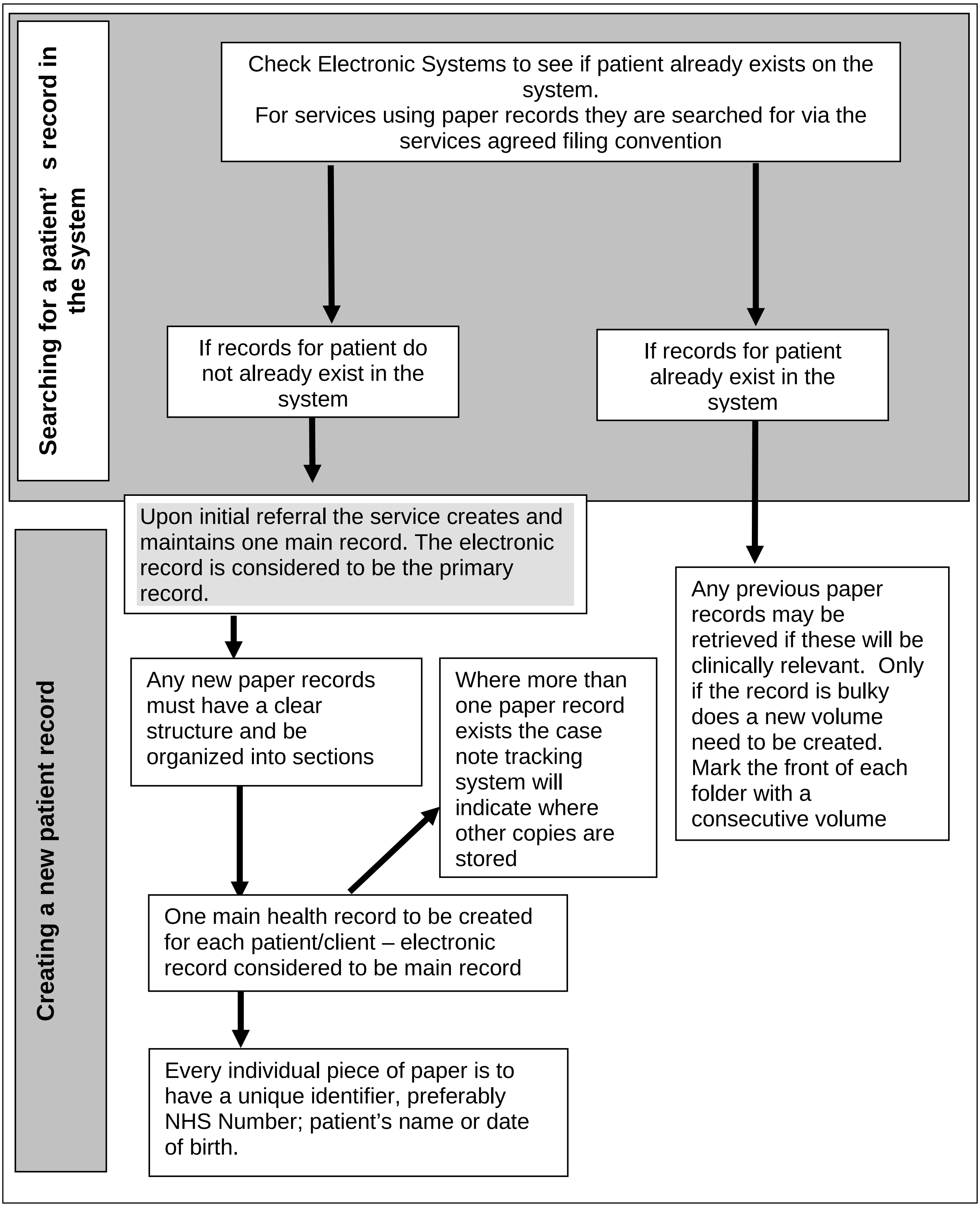
(Insert name of trust) is firmly of the view that all those who work in or provide services to the NHS have the right to do so without fear of violence, threats or abuse. The NHS Constitution makes it clear that just as the NHS has a responsibility to NHS service users, so service users have a responsibility to treat staff with respect and in an appropriate way.

A copy of the trust policy on risk of violence markers is enclosed/can be obtained from [insert details].

Yours (sincerely/faithfully),

Insert name, job title and contact details

Appendix 6 - How a new record is created



Searching for a patient’ s record in the system

Check Electronic Systems to see if patient already exists on the system.
For services using paper records they are searched for via the services agreed filing convention

If records for patient do not already exist in the system

If records for patient already exist in the system

Creating a new patient record

Upon initial referral the service creates and maintains one main record. The electronic record is considered to be the primary record.

Any new paper records must have a clear structure and be organized into sections

Where more than one paper record exists the case note tracking system will indicate where other copies are stored

Any previous paper records may be retrieved if these will be clinically relevant. Only if the record is bulky does a new volume need to be created. Mark the front of each folder with a consecutive volume

One main health record to be created for each patient/client – electronic record considered to be main record

Every individual piece of paper is to have a unique identifier, preferably NHS Number; patient’s name or date of birth.

Appendix 7 - How health records are tracked when in current use

Principles:

- All localities must keep an accurate track of where paper records are located;
- Only one set of paper records should exist for each patient within each service. However, because of exemptions to the general principle of keeping one set of paper records per client, patients may have more than one set of paper records if they are seen by different services;
- Each record, in each service, should be clearly marked to indicate if records in other services exist - whoever does the initial assessment, or whoever subsequently becomes aware of the existence of other records should use the alert box on the inside front cover of the record;
- If a patient progresses from one service to another e.g. CAMHS to an adult service, it may not be appropriate to send the whole record if it contains a lot of third party information (possibly information on whole family) which would make the record meaningless if it were removed. In those circumstances, a very comprehensive synopsis should be provided to the receiving service and if possible accompanied by a verbal 'hand-over';
- Upon discharge, the records should be kept in the most appropriate locality (usually near to where the patient resides and is likely to receive treatment).

Process for electronic tracking of paper health records

The case note tracking system is available on the intranet under `favourites'. All electronic health record systems feed into the case note tracking system, so this system can be used by all services.

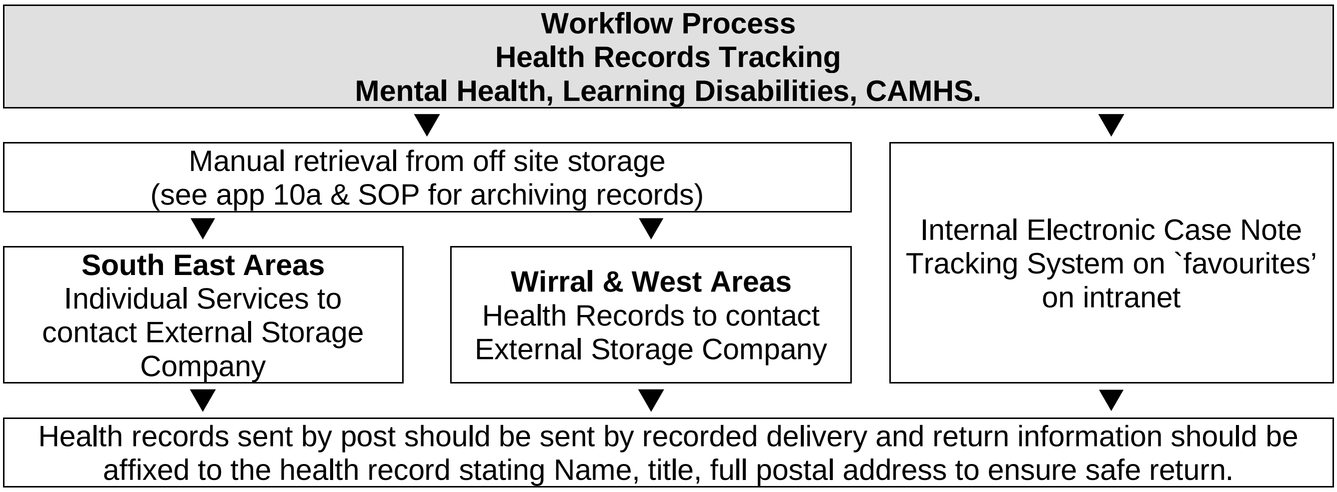
A record must be made in the electronic case note tracking system when new paper records are created, when records are sent from one location to another, and when records are received by any location. Paper records being taken out of any location for the purpose of home visits, must be logged out of that location and then logged back in on their safe return. A full user guide to this system is available on the home screen of the case note tracking system.

The system has an audit trail which shows who booked out a record, when and whether it has been receipted by the receiver.

Process for tracking health records within Physical Health West Services

Physical Health West (PHW) Services joined the Trust in April 2011. PHW services still used paper tracing systems for health records. Services migrated to the use of the EMIS web electronic health record system. All PHW services now only have electronic health records for current patients, therefore the use of the case note tracking system is not required. Any historic paper records are scanned and attached to the electronic record or are available on the CSCAN system.

Process for tracking health records flow chart- Mental Health services



Workflow Process
Health Records Tracking
Mental Health, Learning Disabilities, CAMHS.

Manual retrieval from off site storage
(see app 10a & SOP for archiving records)

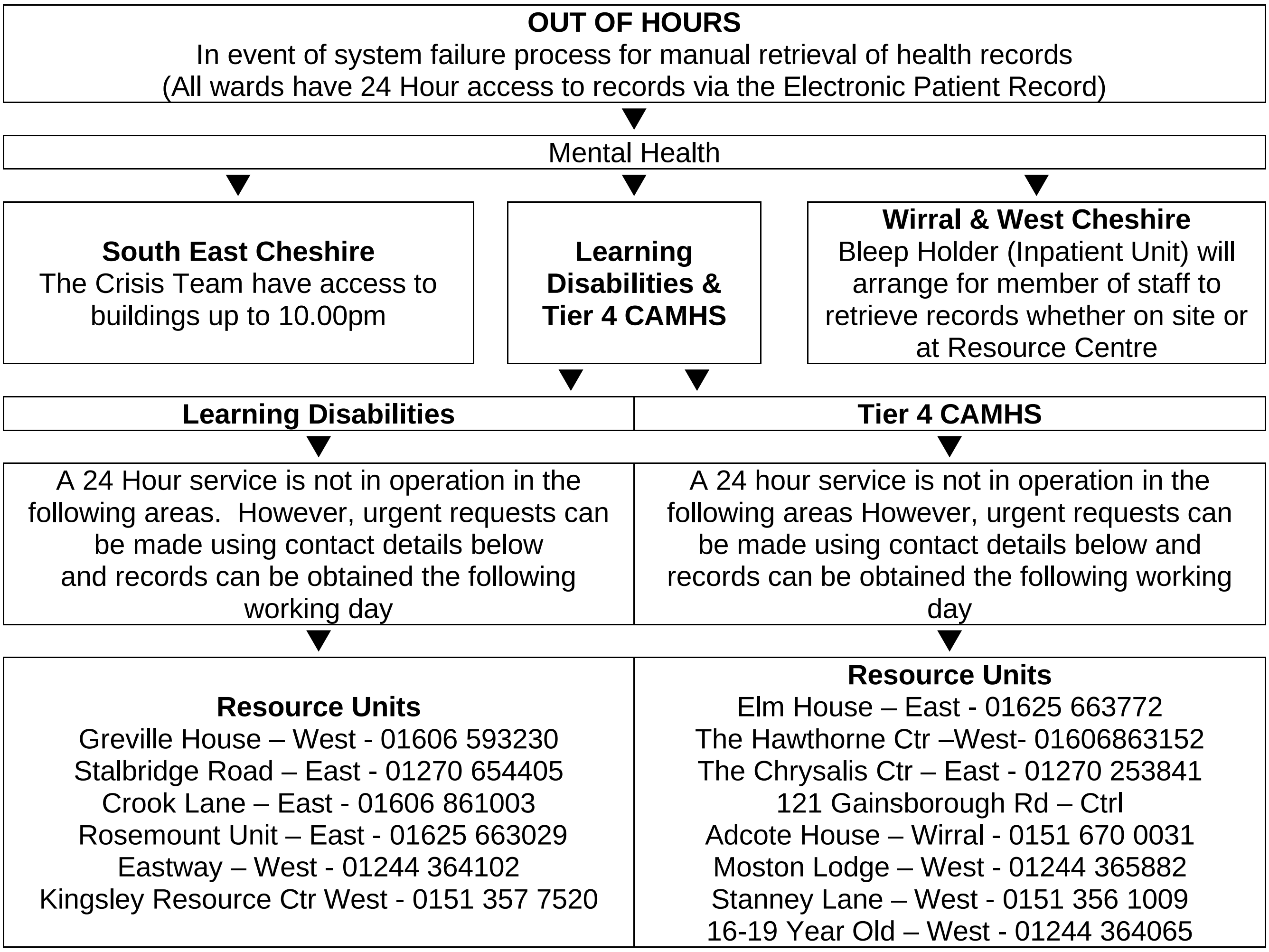
South East Areas
Individual Services to contact External Storage Company

Wirral & West Areas
Health Records to contact External Storage Company

Internal Electronic Case Note Tracking System on `favourites' on intranet

Health records sent by post should be sent by recorded delivery and return information should be affixed to the health record stating Name, title, full postal address to ensure safe return.

How health records are retrieved from storage – out of hours mental health



OUT OF HOURS
In event of system failure process for manual retrieval of health records
(All wards have 24 Hour access to records via the Electronic Patient Record)

Mental Health

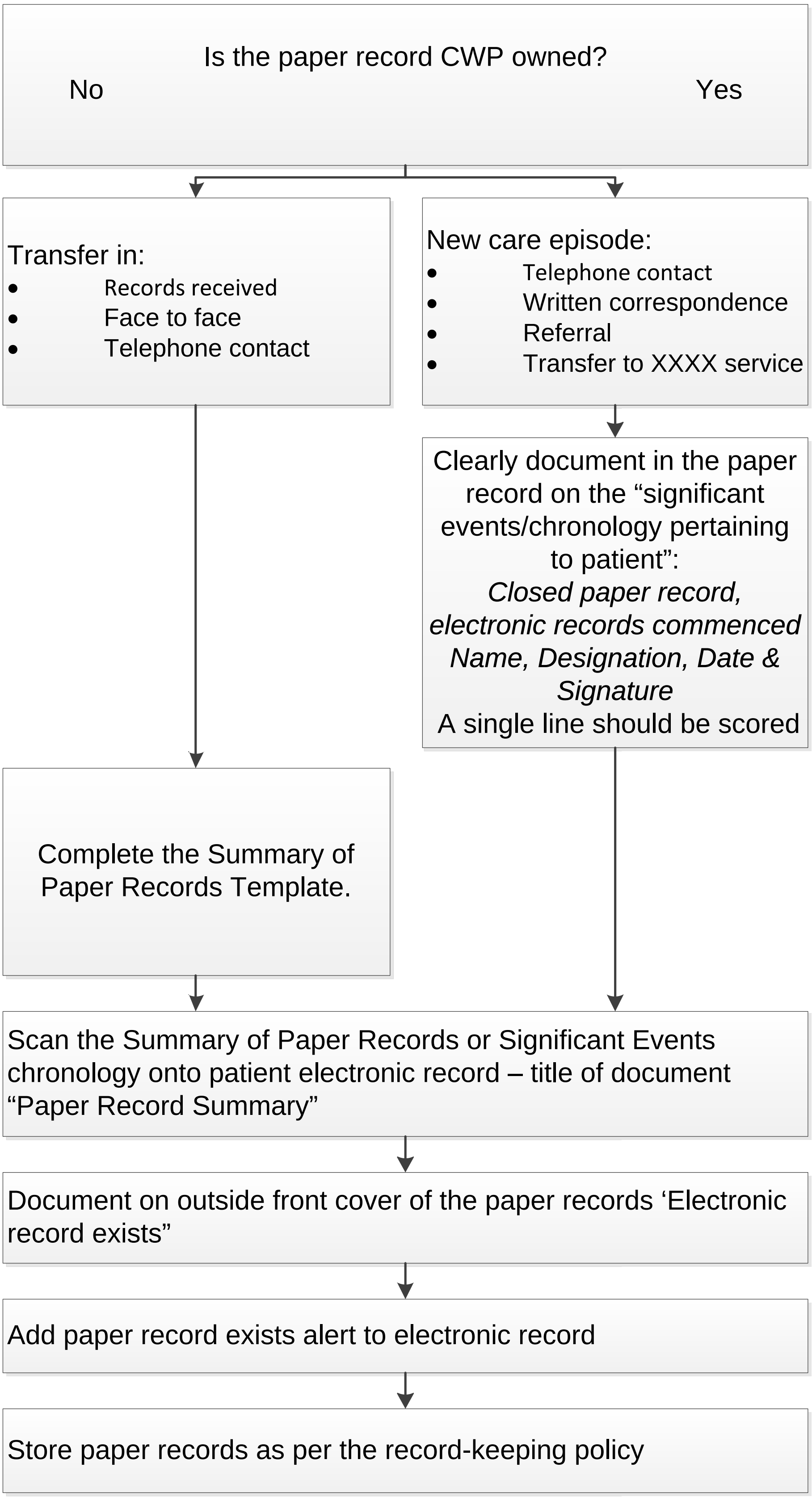
South East Cheshire
The Crisis Team have access to buildings up to 10.00pm

Learning Disabilities & Tier 4 CAMHS

Wirral & West Cheshire
Bleep Holder (Inpatient Unit) will arrange for member of staff to retrieve records whether on site or at Resource Centre

Learning Disabilities	**Tier 4 CAMHS**
A 24 Hour service is not in operation in the following areas. However, urgent requests can be made using contact details below and records can be obtained the following working day	A 24 hour service is not in operation in the following areas However, urgent requests can be made using contact details below and records can be obtained the following working day
Resource Units Greville House – West - 01606 593230 Stalbridge Road – East - 01270 654405 Crook Lane – East - 01606 861003 Rosemount Unit – East - 01625 663029 Eastway – West - 01244 364102 Kingsley Resource Ctr West - 0151 357 7520	**Resource Units** Elm House – East - 01625 663772 The Hawthorne Ctr –West- 01606863152 The Chrysalis Ctr – East - 01270 253841 121 Gainsborough Rd – Ctrl Adcote House – Wirral - 0151 670 0031 Moston Lodge – West - 01244 365882 Stanney Lane – West - 0151 356 1009 16-19 Year Old – West - 01244 364065

Appendix 8 - Closure of paper records flow chart



Is the paper record CWP owned?

No

Yes

Transfer in:

- Records received
- Face to face
- Telephone contact

New care episode:

- Telephone contact
- Written correspondence
- Referral
- Transfer to XXXX service

Clearly document in the paper record on the "significant events/chronology pertaining to patient":
Closed paper record, electronic records commenced Name, Designation, Date & Signature
A single line should be scored

Complete the Summary of Paper Records Template.

Scan the Summary of Paper Records or Significant Events chronology onto patient electronic record – title of document "Paper Record Summary"

Document on outside front cover of the paper records 'Electronic record exists"

Add paper record exists alert to electronic record

Store paper records as per the record-keeping policy

Appendix 9 - Sample of summary of paper records used by Starting Well Services

Summary of paper records for starting well services.

Below is the guidance for inclusion in the Summary of Paper records form. This is not an exhausted list and provides examples for inclusion. The summary needs to provide a true representation of care received to date by the child and family.

Child s Name	
Summary of records :	From ……….. to ……………
DoB:	
NHS No:	
Mothers Name:	
Partners Name :	
Father of Childs Name:	

Safeguarding concerns /involvement /risks (include past / present):
***Completed RIC's, MARAC referrals/outcomes**
***Subject to CP Plan, ChIC plan,**
***Risks identified domestic abuse, parental substance misuse.**
***Any specific for visiting arrangements**

Child Health and Development (include past /present):
***ASQ's completed and when**
***Immunisation history**
***No of A&E attendances**
***Any chronic or acute health conditions**

Other services or agencies involved (include past /present).
***Child Development Team**
***Integrated Early Support**
***IDVA**
***Social Care/ ChIC Team**

Named Social Worker	
Named TAF Lead	
Named ChIC Nurse	

Named Health Visitor:	
Signature:	
Date:	

Summary of Paper Records for Starting Well Services.

Child s Name	
Summary of records :	From ……….. to ……………
DoB:	
NHS No:	
Mothers Name:	
Partners Name :	
Father of Childs Name:	

Safeguarding concerns /involvement /risks (include past / present):

Child Health and Development (include past /present) :

Other services or agencies involved (include past /present).

Named Social Worker	
Named TAF Lead	
Named LAC Nurse	

Named Health Visitor:	
Signature:	
Date:	

Appendix 10 - Processes for archiving paper health records

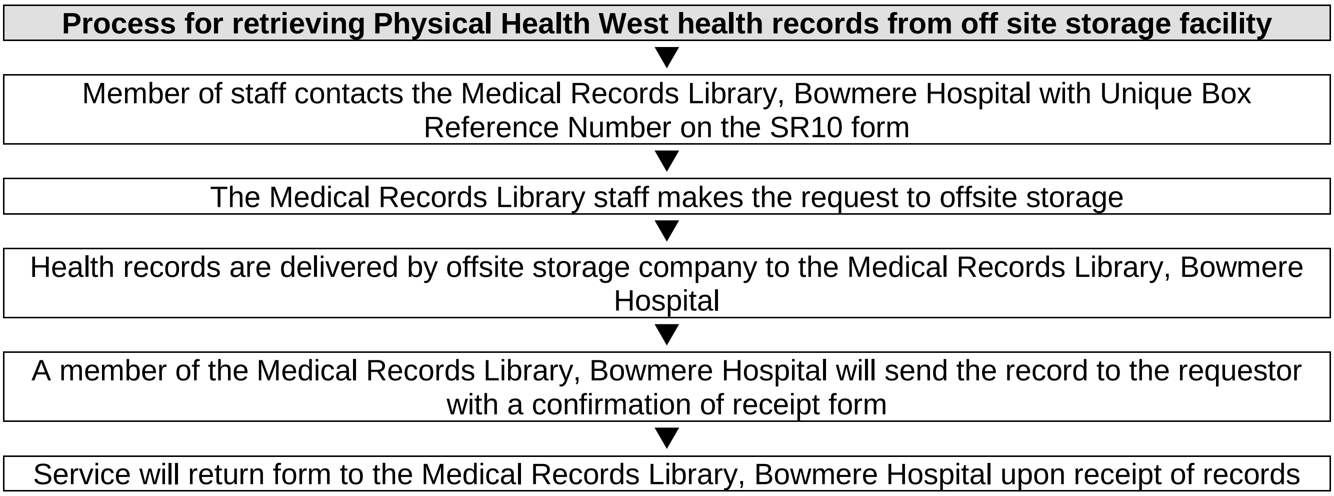
Aim:
To ensure there is a process in place that ensures all records are correctly processed, identified and archived in a safe secure manner.

Principles:

1. Only storage boxes approved for the archiving records and supplied by the relevant archive services must be used;
2. When filled, the boxes and their contents should weigh no more than 15kg;
3. Box lids must fit securely and be free from damage;
4. The contents of each box should be filed in a logical order (alphabetically or numerically);
5. Each paper record should be held securely together, either in a trust approved paper folder, or with treasury tags, so that there are no loose sheets of paper;
6. Paper clips and bulldog clips must not be used to hold paper records together;
7. A record must be made of all contents of each archival box, listing the notes archived, either on the electronic Case Note Tracking system or on the appropriate form (SR10 for Physical Health West);
8. Each archival box must be clearly labeled, with the originating service and location recorded on each box;
9. Records for adults and children must be kept apart due to differing retention periods for these records;
10. Boxes ready for archiving must be kept securely until collected by the appropriate agency;
11. Each archive box will be allocated a reference number by the operational services department;
12. A record of the collection of the archive boxes must be made at the time of their collection;
13. The Trust will receive confirmation of arrival of the archive boxes at any external storage service and update the Case Note tracking system to record that the records have been received.

Please also see Standard Operating Procedure for Archiving Records with Dataspace (IM8)

Appendix 10a - How health records are retrieved from storage (Physical Health West)



Process for retrieving Physical Health West health records from off site storage facility

▼

Member of staff contacts the Medical Records Library, Bowmere Hospital with Unique Box Reference Number on the SR10 form

▼

The Medical Records Library staff makes the request to offsite storage

▼

Health records are delivered by offsite storage company to the Medical Records Library, Bowmere Hospital

▼

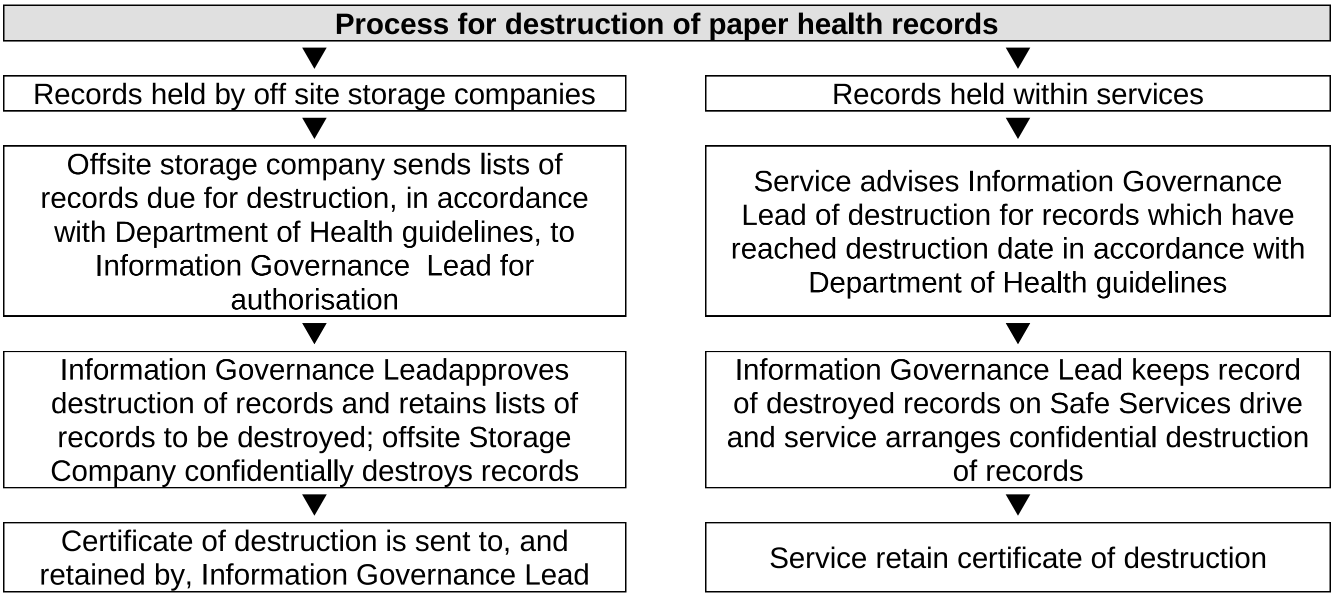
A member of the Medical Records Library, Bowmere Hospital will send the record to the requestor with a confirmation of receipt form

▼

Service will return form to the Medical Records Library, Bowmere Hospital upon receipt of records

Appendix 11 - Processes for disposal and destruction of records

For tracking electronic records which have been electronically archived or destroyed following the appropriate retention period the electronic system will record the date that the record was archived or destroyed. The archived record can be tracked through the electronic system used by the service.



Process for destruction of paper health records

Records held by off site storage companies

Offsite storage company sends lists of records due for destruction, in accordance with Department of Health guidelines, to Information Governance Lead for authorisation

Information Governance Leadapproves destruction of records and retains lists of records to be destroyed; offsite Storage Company confidentially destroys records

Certificate of destruction is sent to, and retained by, Information Governance Lead

Records held within services

Service advises Information Governance Lead of destruction for records which have reached destruction date in accordance with Department of Health guidelines

Information Governance Lead keeps record of destroyed records on Safe Services drive and service arranges confidential destruction of records

Service retain certificate of destruction

Appendix 12 - Audio and visual recordings

Model consent form for audio / visual recordings			
Name of client		Name of Therapist	
NHS Number			

As part of supervision it is useful for therapists to videotape/digitally record a session with you and submit the videotape for review. It would be very helpful therefore, if you would give your consent, after you have discussed this with your therapist.

Consent to videotaping / digitally recording of sessions for supervision and assessment:
I consent to a session(s) being videotaped/digitally recorded. I understand the tape/recording will only be used for the purposes of supervision and so will only be seen by the therapist and the therapist's Clinical Supervisor. My personal details will remain confidential at all times. I give my consent on the understanding that the recording will be erased once the above purposes have been fulfilled or within 12 months, whichever occurs sooner.

The tape/recording will be stored securely in line with the Trust's storage of information protocol.

This agreement has been discussed with me and I have had the opportunity to ask questions regarding this agreement. I also understand that I may withdraw my consent at any time and give instructions for the tape/recording to be immediately erased.

Name		Date	
Signed			
Therapist name			
Therapist clinical supervisor's name			
Signature			
Location		Date	

Appendix 13 - Health Records Audit Tool

1. Name of person completing audit tool *

2. Care Group *

- □ Children, Young People and Families
- □ Learning Disabilities and NDD (Inc. ASD)
- □ Neighbourhood
- □ Specialist Mental Health - Place Based
- □ Specialist Mental Health - Bed Based

3. Clinical Service *

- □ Learning Disabilities and NDD (Inc. ASD)
- □ SMH Bed Based East and West
- □ SMH Bed Based Wirral and PICU
- □ SMH Forensic, Rehab, CRAC
- □ SMH Place Based - East Cheshire
- □ SMH Place Based - South Cheshire and Vale Royal
- □ SMH Place Based - Wirral
- □ SMH Place Based - West Cheshire
- □ CYP - Cheshire CAMHS
- □ CYP - West Cheshire Starting Well Service
- □ CYP - Wirral CAMHS
- □ CYP - Tier 4 CAMHS and Outreach
- □ Neighbourhood - Integrated Teams
- □ Neighbourhood - Front Door

4. Patient NHS number of record audited *

5. Team /Ward service user currently open to: *

2. Please answer the following questions based on the record

Note: for completing questions 6, 7 & 8 of this audit staff must have access to the Summary Care Record (SCR) which is on the National Portal which is under favourites on the intranet and is accessed using a smart card

6. Does the NHS Number match the NHS number recorded for the patient on the Summary Care Record (SCR)? (SCR is on the National Portal which is under favourites on the intranet and is accessed using a smart card)

□ Yes

□ No

□ N/A (patient does not have NHS number)

7. Does the post code recorded for the patient match the NHS number recorded for the patient on the Summary Care Record (SCR)? (SCR is on the National Portal which is under favourites on the intranet and is accessed using a smart card)

□ Yes

□ No

□ N/A (e.g. patient no fixed abode)

8. Does the registered GP recorded for the patient match the NHS number recorded for the patient on the Summary Care Record (SCR)? (SCR is on the National Portal which is under favourites on the intranet and is accessed using a smart card)

□ Yes

□ No

□ N/A (patient is not registered with a GP)

9. Is the care plan current? *

□ Yes

□ No

10. Is there evidence that the patient has been involved in the planning of their care? *

□ Yes

□ No

11. Is there evidence that the service has involved family and/or carers? *

□ Yes

□ No

□ Not Applicable

12. Is there evidence of any written requests and preferences (advanced directive) made by a person with capacity conveying their wishes, beliefs and values for their future care should they lose capacity, or evidence of the location of the document if not held within the record e.g. with GP? *

□ Yes

□ No

Comments:

13. Is there evidence of a risk assessment within the record? *

□ Yes

□ No

□ N/A

Comments:

14. Is there evidence of liaison with other agencies e.g. General Practitioner, Social Care etc.? *

□ Yes

□ No

Comments:

15. Are the emails attached to the record written in an appropriate manner e.g. is language on content suitable? (last 3 months) *

□ Yes

□ No

□ Not applicable

Comments:

16. Have any non Trust approved abbreviations (approved list on information governance page of intranet) been used in the record? (last 3 months)

□ Yes

□ No

17. Are entries contemporaneous (i.e. at the same period of time) whenever possible, or made immediately after the patient/clinician contact? *

□ Yes

□ No

18. Is the NHS number quoted on all correspondence? *

□ Yes

□ No

Comments:

19. Have entries made by students, and trainees who do not hold an NHS contract of employment, been read and approved/ countersigned by their Trust clinical supervisor? (last 3 months) *

□ Yes, fully

□ No

□ N/A no such entries made

20. Have staff names been written/typed out in full? (i.e. initials have NOT been used to identify staff involved in discussions) (last 3 months) *

□ Yes

□ No

□ Electronic record, not applicable

21. Where more than one staff member is involved in a decision, the most senior/appropriate clinician has been clearly identified? (last 3 months) *

□ Yes

□ No

□ N/A (i.e. only one member of staff involved in a decision)

22. Does the patient record contain *

□ Paper records only (exclude paper lite records)

□ Electronic records only

□ Paper and Electronic records

3. Paper records only (last 3 months)

23. Are the records bound in a folder?

□ Yes

□ No

24. Are the papers inserted behind correct dividers?

□ Yes

□ No

25. Is every individual piece of paper secured within the folder?

□ Yes

□ No

26. Does every individual piece of paper include two patient identifiers e.g. patient's name, DOB or NHS number? (last 3 months)

	Name	DOB	NHS Number
Yes	□	□	□
No	□	□	□

27. Are there any plastic/poly pockets in the folder? (last 3 months)

□ Yes

□ No

28. Does the paper record contain copies of records which have been printed off from the electronic system, creating a dual record? (last 3 months)

□ Yes

□ No

29. Are the records written legibly? (last 3 months)

□ Yes

□ No

30. Does each entry note the date (day, month and year) (last 3 months)

□ Yes

□ No

31. Is each entry signed? (last 3 months)

□ Yes

□ No

32. Is the professional's name also printed legibly underneath the signature? (last 3 months)

□ Yes

□ No

33. Is the professional's position/grade also printed legibly underneath the name? (last 3 months)

□ Yes

□ No

34. Are large records kept in separate volumes which are consecutively numbered in chronological order?

□ Yes

□ No

4. Alterations PAPER RECORDS ONLY (last 3 months)

35. Have there been any alterations to the record?

□ Yes

□ No

5. Alterations PAPER RECORDS ONLY (last 3 months)

36. Are any alterations made by scoring out with a single line?(last 3 months)

□ Yes

□ No

37. Are any alterations made followed by the date?(last 3 months)

□ Yes

□ No

38. Have any alterations made been individually signed? (last 3 months)

□ Yes

□ No

39. Has correction fluid been used?

□ Yes

□ No

6. Additions PAPER RECORDS ONLY (last 3 months)

40. Have there been any additions made to existing entries? (last 3 months)

□ Yes

□ No

7. Additions PAPER RECORDS ONLY (last 3 months)

41. Have any additions made to existing entries been individually dated? (last 3 months)

□ Yes
□ No

42. Have any additions made to existing entries been individually signed? (last 3 months)

□ Yes
□ No

8. Results and Prescriptions PAPER RECORDS ONLY (last 3 months)

43. Have any reports and results been signed by the clinician or practitioner before being filed? (last 3 months)

□ Yes
□ No
□ No (no reports or results evident)

44. Is there a prescription sheet/ chart? (last 3 months)

□ Yes
□ No
□ N/A

45. Does the prescription sheet/ chart contain adequate details i.e. patient identifier, dosage and signature? (last 3 months)

□ Yes
□ No
□ Not applicable

46. Is the prescription chart written legibly? (last 3 months)

□ Yes

□ No

□ Not applicable

47. Is there evidence of recorded entries for each inpatient shift? (last 3 months)

□ Yes

□ No

□ N/A

48. Has the service user been discharged from CWP inpatient care? (last 3 months)

□ Yes

□ No

□ n/a

49. Were the discharge arrangements recorded on the care plan? (last 3 months)

□ Yes

□ No

□ N/A

50. Is there evidence of a discharge letter? (last 3 months)

□ Yes

□ No

□ Not applicable

Appendix 14 - Development of Clinical Forms

A formal control process for the development of clinical forms ensures:

a. Minimise risk to patients and staff
b. Ensure standardisation of data to be recorded
c. Ensure compliance with governance standards
d. Ensure only the relevant information is collected for the specific
e. purpose
f. Ensure all documents are approved and accessible by all staff
g. Avoid development of additional forms when a form may already be in
    a. existence
    b. or information is available electronically via the Trust's systems
h. Enable improved collation of data for performance/quality reporting
i. All forms will be subject to periodic review to ensure they are still required and appropriate to their specific use.

- All forms should include the following fields in order to comply with Health Records standards.

a. Patient's name
b. Patient's NHS number
c. Signature of health professional
d. Printed name of health professional
e. Printed rank of health professional
f. Point of contact of health professional
g. Date and time

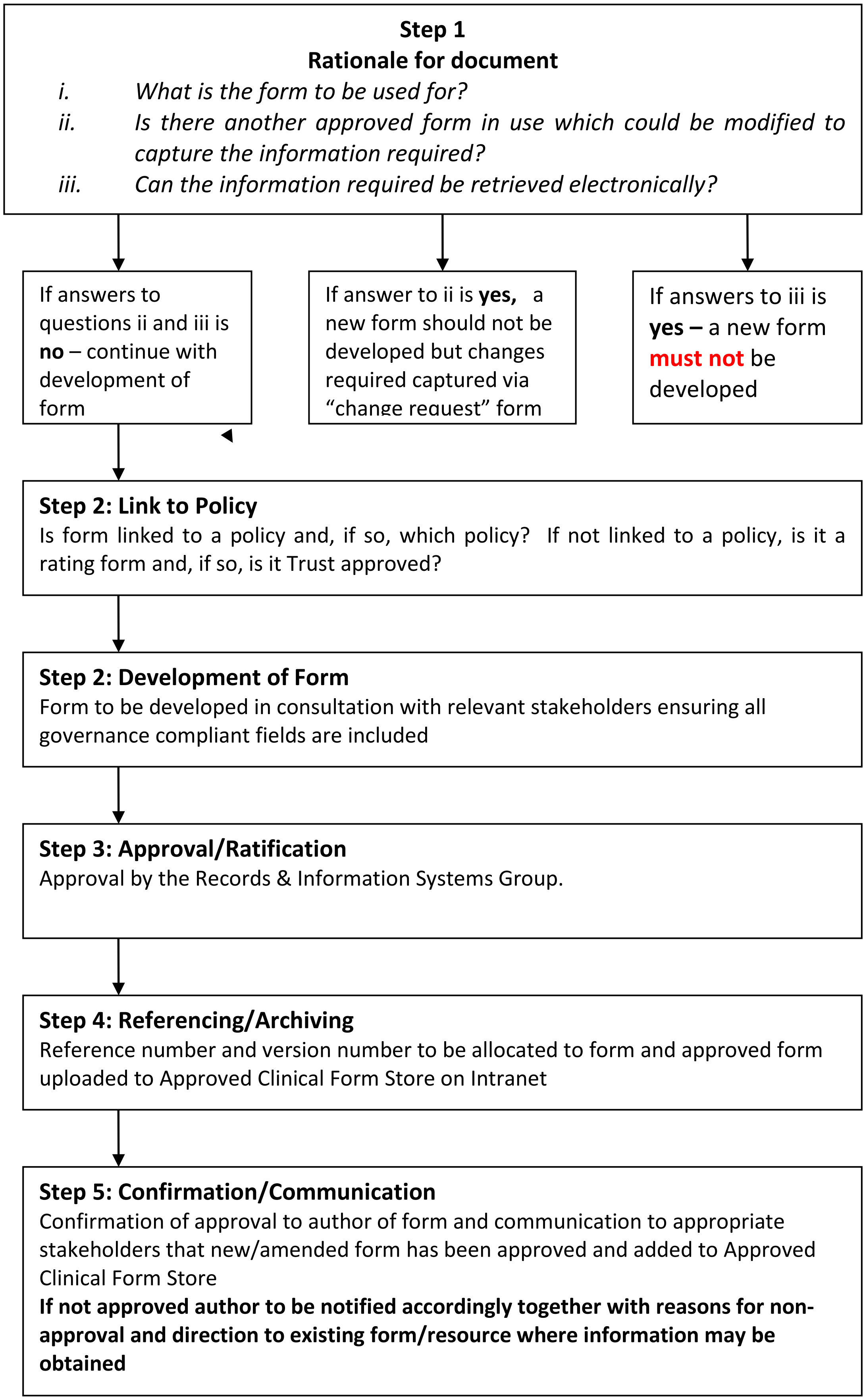
- When approved forms will be allocated a Reference Number
  eg: CL/CAMHS/CP14/21

  CL - to indicate the form is a clinical document
  Service name or TW (Trustwide) – to indicate relevant service
  Number of appropriate policy - eg CP14 Prevention and management of slips, trips and falls
  No - number allocated
  V1 - Version number

- All approved forms will be stored in an Approved Clinical Form Store located on the intranet. Random checks of patient records will be undertaken to ensure only approved documentation is in use.

- Please see following flow chart for process for approval of new/amended clinical forms:

PROCESS FOR APPROVAL OF NEW/AMENDED CLINICAL FORMS



Step 1
Rationale for document

i. *What is the form to be used for?*
ii. *Is there another approved form in use which could be modified to capture the information required?*
iii. *Can the information required be retrieved electronically?*

If answers to questions ii and iii is **no** – continue with development of form

If answer to ii is **yes,** a new form should not be developed but changes required captured via “change request” form

If answers to iii is **yes –** a new form **must not** be developed

Step 2: Link to Policy
Is form linked to a policy and, if so, which policy? If not linked to a policy, is it a rating form and, if so, is it Trust approved?

Step 2: Development of Form
Form to be developed in consultation with relevant stakeholders ensuring all governance compliant fields are included

Step 3: Approval/Ratification
Approval by the Records & Information Systems Group.

Step 4: Referencing/Archiving
Reference number and version number to be allocated to form and approved form uploaded to Approved Clinical Form Store on Intranet

Step 5: Confirmation/Communication
Confirmation of approval to author of form and communication to appropriate stakeholders that new/amended form has been approved and added to Approved Clinical Form Store
If not approved author to be notified accordingly together with reasons for non-approval and direction to existing form/resource where information may be obtained

Appendix 15 - Scanning of paper documents guidance

The scanning of physical documents raises questions relating to the disposal of original papers and the legal admissibility of an electronic image. At present there is no definitive law regarding the legal admissibility of scanned documents over paper originals. Certain guidelines have been developed to aid the ever-growing number of public authorities that are working towards a more digital future. This policy adheres to the guidelines set out in BIP 0008:2008 to the British Standard on legal admissibility and evidential weight on scanned records. This provides guidance on the use of electronic images as evidence in legal situations.

The aim of this policy is to create clear guidelines to all staff when scanning any paper documentation. The trust aims to implement a process which will improve staff time in terms of accessibility to records, and to also reduce the amount of physical filing which is produced and duplicated.

What to scan

Any physical documentation that would be deemed necessary and/or noteworthy to a patient's health and well-being or treatment, may be scanned. If the physical item is essential information that would be stored on a physical file, this must be scanned into the relevant system. Any documents that can be created electronically in the first instance must be completed online and not duplicated in a physical document and scanned. Any physical documentation that does not belong to the Trust must be kept in its original format and not scanned. This can include deeds, guarantees or certificates which are not the property of the Trust. These can only be scanned and destroyed with written consent from the owner. Any document that requires a signature of consent can be scanned but must also be kept in its original format until such time that electronic signatures become available. Do not scan any duplicate documents that are already on a system used by staff. Once a document is scanned it should not be re-printed with the exception of outside agencies (if no electronic transfer method is available) or a subject access request. A quality check of the scanned image must be undertaken, noting of activity carried out and the confidential destruction of the original physical document.

How to scan

Before scanning of a document can take place, the following actions should be carried out:
□ Assess the condition of the document to ensure that it is not too fragile for scanning, pages are not stuck together or inserts such as post-it notes are not attached to any sheets.
□ Any notes attached to the document must be placed on a blank sheet of paper for scanning.
□ Remove any staples or paperclips.
□ Ensure all pages are in chronological order.
□ For patient or staff files, ensure the front page has the following details:
Full Name
Date Of Birth
NHS Number/Employee Reference Number
Date of Document
□ Any blank pages within a file must not be removed and must be scanned in the order they scanned in the order they appear within the original document.
□ Remove any poly pockets / plastic wallets
□ Check that all the information in the document pertains to the same patient (NHS number, name and date of birth). If misfiled information is found it must be removed and relocated in the appropriate record.

Scanning equipment

All scanning should be carried out to the following resolution settings:
□ Black and White images – 200 DPI (Dots Per Inch)
□ Coloured Images – 300 DPI
□ Photographs – 300 DPI

Note: 200 DPI is the lowest setting on the Trust's Multi Function Devices but they can be adjusted to 300 dpi.

Quality Control

The quality check of a scanned image must be carried out as soon as the scanning has taken place. To ensure all documents are scanned to a satisfactory quality, staff must ensure:

- Every piece of a document is scanned, including blank pages and double-sided documents.
- Any scanned document is unchanged from its original format. Any amendments or additions made to a document must be made prior to scanning.
- All aspects of the scanned document are legible.
- Pages should be positioned correctly and not at an angle.

Security and Protection

Records that contain Personal Identifiable Data should only be scanned by staff who are authorised to handle the information. The scanned images should be immediately quality checked and stored within the correct system. No scanned document should be stored on a shared or personal drive, and/or desktop. The original document should be confidentially destroyed as soon as possible after storing the scanned document. No persons should keep the paper version for their own needs.
If you are unsure about destroying a document, do not scan it. Contact the Trusts Records & Information Governance Manager for advice. There should never be two versions of a document.
Scanning of records should take place in a secure environment where only authorised personnel have access.

Document Retention –

All physical documentation should be kept until sufficient quality checks have been carried out on a scanned image. A scanned document must be securely stored before destroying a physical record. A scanned document must be destroyed from the area in to which it was originally scanned once it has been appropriately stored.
Original Physical Documents can be destroyed once:

- The scanned image is securely stored
- The scanned Document has been thoroughly quality checked to ensure the electronic version is a true and accurate copy of the original. Once these checks have been carried out, the original document can now be destroyed.

Legal Admissibility

Any scanned document will be managed in accordance with the Trusts Health Records Policy.
The scanned copy will, for legal purposes, become the definitive record and will then be subject to correct records and retention policies set in place for digital documentation. Scanned documents are admissible in court but can differ depending on the court action. In Criminal cases a certified scanned copy can be used with proper authentication including how it was scanned and notations declaring it unaltered. In civil action cases, scanned copies can be produced with the court deciding on the evidential weight issued to the document. These principles arise from the Civil Evidence Act 1995 and the Policy and Criminal Evidence Act 1984.

REFERENCES

- Department of Health Informatics Directorate – Information Governance Policy. NHS Information Governance Records Management – Guidance on Digital Document Scanning (2011)
- Digitisation at The National Archives (2015)
- British Standard BS 10008:2008 (2008)
- The Civil Evidence Act (1995)
- Policy and Criminal Evidence Act (1984)