NHS
Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL	
Title:	**Missing Records Policy**
Version:	**7**
Reference Number:	**RM004**
Scope:	
This policy applies to all staff who handle health or staff records whether they are in paper or electronic format	
Purpose:	
The purpose of this document is to describe what to do if records are unavailable when required.	
Requirement for Policy	
To comply with the General Data Protection Regulation, Data Protection Act 2018, Data Protection and Security Tool, CQC and the Records Management Code of Practice for Health and Social Care 2016.	
Keywords:	
Health records; personnel files; missing; lost; contaminated; destroyed; erasure	
Supersedes:	
Version 6	
Description of Amendment(s):	
Updated in line with the GDPR and the Data Security & Protection Toolkit; Incorporates both paper and electronic records Was previously known as CO028	
Owner:	
Records Manager – Carole Trodden	
Accountability:	
• Trust Solicitor • Director of Service Development and Delivery	
Individual(s) & group(s) involved in the Development:	
This document has been developed in collaboration with the following interested parties: • Carole Trodden	

Individual(s) & group(s) involved in the Consultation:	
The document has been circulated for consultation and comments have been taken into consideration and the document amended accordingly: • Members of IGMM • Members of IGAG	
Equality Impact Analysis:	
Date approved: **Reference:**	18th December 2018 RM007-EIA007
Freedom of Information Exemption Assessment:	
Date approved: **Reference:**	8th February 2019 POL2018-97
Information Governance Assessment:	
Date approved: **Reference:**	8th February 2019 POL2018-97
Policy Panel:	
Date Presented to Panel: **Presented by:** **Date Approved by Panel:**	11th February 2019 Carole Trodden 11th February 2019
Policy Management Team tasks:	
Date uploaded to Trust's intranet: **Date uploaded to Trust's internet site:**	12th February 2019 12th February 2019
Review:	
Next review date: **Responsibility of:**	February 2022 Carole Trodden
Other Trust documentation to which this policy relates (and when appropriate should be read in conjunction with):	
CL122	Safeguarding Families Policy
CO010	Incident Reporting, Management and Investigation Policy
RM001	Records Management Policy
RM002	Moving/Transferring of Bulk Paper Records Procedure
RM003	Management of Mental Health & Specialist Services Health Records Guidance
RM005	Management of Business and Corporate Records Management Guidance

RM006	Records Retention Schedule Guidance
RM007	Management of Community Services Health Records Guidance
Policy Associated Documents:	
TAD_RM007_01	Missing Records Log
TAD_RM007_02	Flowchart for staff when a record is unavailable
TAD_RM007_03	Cause Codes
Other external documentation/resources to which this policy relates:	
	General Data Protection Regulation 2018 https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation
	Data Protection Act 2018 https://www.gov.uk/government/collections/data-protection-act-2018
	Data Security & Protection Toolkit: https://www.dsptoolkit.nhs.uk/Help/29
	Information Governance Alliance: www.hscic.gov.uk/iga
	Information Commissioner’s Office: https://ico.org.uk/
	www.cqc.org.uk/sites/default/files/documents/guidance_about_compliance_summary.pdf
CQC Regulations **This Policy supports the following CQC regulations:**	
Regulation 17	Good Governance

Contents Page

1. INTRODUCTION

Unauthorised or accidental loss of access to, or destruction of personal data are a risk to individuals' rights and freedoms as they could be required for the purposes of continuity of care; investigations; complaints; disciplinaries; subject access requests. Under Article 29 Working Party on Personal data in the General Protection Data Regulation (GPDR) this is known as an 'Availability Breach'.

It is therefore vital that tracing procedures are undertaken at all times.

2. PURPOSE

The purpose of this procedure is to provide supporting information and further details regarding the processes for dealing with unavailable records at the time of requirement so that there is:

- A consistent approach to searching and reporting missing paper records;
- Communication of a personal data breach to the data subject
- A standard approach adhered to;
- Trust benefits from shared learning

3. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

The **Chief Executive** has overall responsibility for ensuring that records are managed responsibly within the Trust. As accountable officer the Chief Executive is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this, as it will ensure appropriate, accurate information is available as required.

The **Trust** has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

The **Director of Service Development and Sustainability is the Senior Information Risk Officer (SIRO)** for the Trust. The SIRO has overall responsibility for the organisation's information risk policy and will also lead and implement the information governance risk assessment and advise the Board on the effectiveness of risk management across the organisation.

The Trust's **Caldicott Guardian** acts as the 'conscience' of the Trust in relation to person identifiable information and actively supports work to facilitate and enable information sharing. The Medical Director is the Caldicott Guardian and is responsible for ensuring person identifiable information is shared in an appropriate and secure manner. The Caldicott Guardian is the nominated Executive lead for all health, business and corporate records. The Caldicott Guardian also has a fundamental role around ensuring that the Trust is compliant with the GPDR and that personal data is available when required.

The Divisional Business Units (DBU's) are responsible for implementing any action plans arising from non-compliance to the Records Management Policy and procedures.

The **Records Manager** is responsible for the overall development and maintenance of records management practices throughout the Trust. In particular, the Records Manager is responsible for drawing up guidance for good records management practice and promoting compliance with this guidance in such a way as to ensure the easy, appropriate and timely access to personal information.

The responsibility of local records management is devolved to the service directors and department managers. **Information Asset Owners** (IAO's) such as, Service Directors, Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policy and procedures. The IAO's are supported by the **Information Asset Managers** (IAM's) who will coordinate the identification of information assets within their remit and will assign an **Information Asset Administrator** (IAA) for each asset.

All Trust Staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep records safely so that they are available when required and that if unavailable they have a duty to inform the individual affected under the GDPR.

4. TRACKING PAPER RECORDS

All health / staff record movements must be tracked. If paper health records are tracked electronically, such as hospital records in mental health services or child health records in community services, then this must be used to record the location of the health paper record. Individual departments/services will use an auditable tracking log to indicate the location of the paper health record if it is moved for any reason. All records should be tracked as per the Records Management Policy (RM001) either electronically or manually. A booking in/out system or tracer cards can be used.

5 MISSING RECORDS PROCEDURE

The Missing Records Procedure has been developed to support effective records tracking systems to comply with the Records Management Policy and support processes to ensure that records are made available to staff when required.

The procedures and processes should facilitate the availability of the complete record at all times when required.

The guidance for staff flowchart to use when a record is unavailable can be found in TAD_RM007_02.

Missing Record Procedure

When a paper record is unavailable the following steps should be undertaken:

Step 1: The last tracking location on the electronic record, tracer card or booking in/out book should be identified and checked.

Step 2: The member of staff should conduct all reasonable searches including checking:

- Other filing areas
- Current libraries
- Discharge libraries
- Off-site storage
- With colleagues

Step 3: The member of staff should report this to his/her supervisor/ line manager as soon as possible after the completion of Steps 1 and 2, and before the data subject is due to attend or record is required.

Step 4: The supervisor / line manager should ensure that a thorough search is undertaken, using tracking and contact history, (for example, check PLUS or PARIS if applicable) including initiating a search at the base where the record should be kept.

Step 5: An electronic incident form must also be completed at this stage as per the Incident Reporting, Management and Investigation Policy. Please see TAD_RM007_03 for guidance to the correct cause code. If a volume of health or staff records are missing this is graded a 4.

Step 6: On receipt of an incident form relating to missing/lost/stolen/records, the Records Manager will issue a Missing Record Log (TAD_RM007_01) to the author of the incident or service to which the incident belongs.

Step 7: At this stage the IG Incident lead will review the incident in line with the guidance from the Data Protection & Security Toolkit and if it meets certain criteria may report it. If the data breach is severe enough it may at this point be escalated to the Information Commissioner's Office (ICO) and the Department of Health & Social Care. A more detailed investigation (IR) may be instigated by the IG incident lead depending on the circumstances of the data loss and how this would affect the rights and freedoms of the individual(s) concerned.

Step 8: The lead clinician or manager must inform the data subject of their potential loss of information in a timely manner unless it is deemed not in the data subject's best interest

Step 9: If the missing record is a health record then a temporary record may need to be made up at this stage including all the relevant information available (from electronic systems, GP, previous volumes etc).

Step 10: The missing paper record or volume should be highlighted as missing (adding a comment to this effect on electronic tracking systems or tracer cards noting the date it was unavailable). Volume 2 will be created on the electronic system with a comment to say this is a temporary record. Alternatively if the service has gone ‘live’ with an electronic patient system the new record will be created electronically and reference will be made to Trust’s the paper record being missing. The missing records log and the electronic tracking system should be updated to reflect this change.

Step 11: Staff should continue to search for the record over the next 6 months. If not found after 6 months the record is deemed ‘lost’ and recorded on the missing records summary as lost by the records manager.

Step 12: The records management service will be keep a log of all missing records and monitor services compliance with this procedure and ; identify any actions to be undertaken. The Records Manager will report any issues or trends to the Information Governance Assurance Group (IGAG).

Step 13: The Divisional Business Units (DBU’s) are responsible for implementing any action plans arising from non-compliance to the Records Management Policy in respect of missing or lost paper records.

6 COMMUNICATION OF A PERSONAL DATA BREACH TO THE DATA SUBJECT

Article 34 of GDPR requires any personal data breach, which is likely to result in a high risk to the rights and freedoms of individuals, to be communicated with those affected.

Any communication must contain the following four elements:

- a description of the nature of the breach
- the name and contact details of the data protection officer or other contact point from whom more information can be obtained
- a description of the likely consequences of the personal data breach
- a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Template letters can be provided by the IG Manager.

Patients with mental health issues

- Follow service procedures unless patient also has cognitive impairment or you are advised to withhold incident information by the lead clinician. Discuss with the lead clinician the reasons why the information is withheld and document this.

- Do not discuss incident information with a carer/relative without the express permission of patient (unless in exceptional circumstances).

Patients with cognitive impairment:

Involve patients with cognitive impairment directly in communications about the incident, making an advocate available to assist in the communication process.

- Where patients have an authorised person to act on their behalf by lasting power of attorney, ensure this extends to decision making and the medical care and treatment of the patient. Hold discussions with the holder of power of attorney.
- If there is no such person, clinicians should act in the patients best interests. They should decide who the appropriate person is with whom to discuss the missing records incident. Discussion should take regard of patient's welfare as a whole.

Patients with learning disabilities:

- If a patient has difficulty expressing their opinion verbally, assess whether they are also cognitively impaired.

- If they are not cognitively impaired, provide alternative communication methods (e.g. written questions) and agree with them appointment of an advocate.

- Ensure the patients views are considered and discussed.

- Involve patients with cognitive impairment directly in communications about the incident, making an advocate available to assist in the communication process.

A communication is not necessary in the following three circumstances

- the controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach for example the data were encrypted.
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.
- it would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.

7 FOUND PAPER RECORDS

When the original paper record is located the following procedure should be followed:

Step 1: Complete the missing paper record log to indicate that the original paper records have been located and forward to the records manager.

Step 2: For health paper records inform the lead clinician. If the data subject had been previously informed that the paper records were missing the lead clinician will need to inform the data subject that the paper records had been found. Inform the staff member if they were staff records.

Step 3: Merge the paper temporary folder with the original set of paper records.

Step 4: If the original paper records are found, please update the electronic tracking system or tracer card.

Step 5: The Records Manager will inform the Risk Department to update the incident and also update the missing records log summary.

8. EQUALITY IMPACT ANALYSIS

As part of its development, this document was analysed to consider / challenge and address any detrimental impact the policy may have on individuals and or groups protected by the Equality Act 2010. This analysis has been undertaken and recorded using the Trust's analysis tool, and appropriate measures will be taken to remove barriers and advance equality of opportunity in the delivery of this policy / procedure

9. FREEDOM OF INFORMATION EXEMPTION ASSESSMENT

Under the Freedom of Information Act (2000) we are obliged to publish our policies on the Trust's website, unless an exemption from disclosure applies. As part of its development, this policy was assessed to establish if it was suitable for publication under this legislation. The assessment aims to establish if disclosure of the policy could cause prejudice or harm to the Trust, or its staff, patients, or partners. This assessment has been undertaken using the Trust's Freedom of Information Exemption Guide, and will be reviewed upon each policy review.

10. INFORMATION GOVERNANCE ASSESSMENT

This Policy has been analysed to ensure it is compliant with relevant information law and standards as in place at the time of approval, and are consistent with the Trust's interpretation and implementation of information governance components such as data protection, confidentiality, consent, information risk, and records management.

Compliance will be reviewed against any changes to legislation / standards or at the next review of this document.

11. SAFEGUARDING

All staff have a responsibility to promote the welfare of any child, young person or vulnerable adult they come into contact with and in cases where there are safeguarding concerns, to act upon them and protect the individual from harm.

All staff should refer any safeguarding issues to their manager and escalate accordingly in line with the Trust Safeguarding Families Policy and Local Safeguarding Children/Adult Board processes.

12. MONITORING

The effective application of this policy, including adherence to any standards identified within will be subject to monitoring using an appropriate methodology and design, such as clinical audit.

Monitoring will take place on a biannual basis and will be reportable to the Quality Group via the Clinical Effectiveness and Quality Improvement Team.

13. REVIEW

This policy will be reviewed three-yearly unless there is a need to do so prior to this; e.g. change in national guidance.

14. REFERENCES

Data Protection Act 2018

Equality Act 2010

Freedom of Information Act 2000

General Data Protection Regulation 2018