Trust Standard Operating Procedure

Disclosure of Person Identifiable Data by Post

Issue Date	Review Date	Version
November 2020	November 2025	2

Purpose

To provide staff who are posting person identifiable data relating to patients or staff with more information.

Who should read this document?

All staff that disclose person identifiable data by post should read this document.

Key Messages

When posting person identifiable data, staff must:

- Double check the contents of envelopes to ensure it contains the correct documents.
- Be very careful when using window envelopes to ensure that only the name and address is visible.

Core accountabilities

Owner	Information Governance Support Manager
Review	Caldicott and Information Governance Assurance Committee
Ratification	Director of Corporate Business
Dissemination (Raising Awareness)	Information Governance Support Manager
Compliance	Information Governance Support Manager

Links to other policies and procedures

Information Governance Policy
Disclosure of Personal Information by Email SOP
Data Protection Impact Assessment SOP
Disclosure of Personal Information by Telephone SOP
Disclosure of Personal Information by Fax SOP
Audio and Visual Recording Policy
Auditing Clinical Systems SOP
Disposal of Confidential Waste SOP
Moving & Tracking of Patient Case Notes

Version History

1	March 2019	Initial Document - transferred from an APN to an SOP with minor amendments to legislation
2	November 2020	Updated following expiry date

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

Standard Operating Procedures are designed to promote consistency in delivery, to the required quality standards, across the Trust. They should be regarded as a key element of the training provision for staff to help them to deliver their roles and responsibilities.

Standard Operating Procedure (SOP)

Disclosure of Person Identifiable Data by Post

1 Introduction

This SOP has been produced to provide staff with information on transmitting person identifiable data by post securely.

A large volume of data is passed into, out of and around the NHS by post. There is an internal post system, as well as using the Royal Mail for external post. This post often contains large amounts of very sensitive and confidential information.

Staff must ensure that they choose the most appropriate way of sending items via the post.

2 Definitions

Personal Data is information or expressions of opinion, which relate to a living individual who can be identified from that information. For example, name, address, date of birth, employee number etc.

Special Category Data relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition or sex life.

3 Regulatory Background

Data Protection Legislation

The following sets out the way organisations should process personal data of living individuals:

- EU General Data Protection Regulation (GDPR)
- UK Data Protection Act 2018

Common Law Duty of Confidentiality

Information is only disclosed to individuals who are authorised to receive it by individuals who are authorised to release it. Disclosure is determined on a need to know basis.

Caldicott Report

The seven Caldicott Principles when using patient information are:

- Justify the purpose
- Only use if absolutely necessary

- Use the minimum required
- Access on a need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect confidentiality.

4 Key Duties

All staff have a duty to protect patient/staff confidentiality in line with the relevant legislation. This procedure is designed to help staff maintain their obligations.

5 Procedure to Follow

The internal post service and Royal Mail are secure for the transmission of person identifiable data.

Staff should ask themselves the following questions if they need to send person identifiable data by post.

1. Can you be sure of whom you are sending the information to?
2. If so, are they entitled to the information?
3. Are you authorised to disclose the information?
4. What is the minimum information required?

All staff must:

- Check that the correct name and address (including postcode) is on the envelope.
- Double check the contents of envelopes to ensure it contains the correct documents.
- Be very careful when using window envelopes to ensure that only the name and address is visible.
- Always mark letters that contain confidential information “Private and Confidential” and if necessary, “Addressee Only”.
- Always properly address confidential letters to specific individuals or job titles, and do not use blanket departments.
- Not use internal transit envelopes for person identifiable data as these can be easily opened and resealed.
- Ensure that when sending casenotes in the internal post, they should be in sealed bags/envelopes which are labelled and traced appropriately.
- Consider sending highly sensitive documents or large volumes of person identifiable data by Royal Mail Special Delivery or Royal Mail Recorded

Delivery Services. This provides a good level of assurance as well as confirmation of postage, receipt and tracking/audit trails.

- Ensure that original sets of casenotes are only sent in the external post in extenuating circumstances and either Royal Mail Special Delivery or Royal Mail Recorded Delivery Services must be used.
- Respect patient confidentiality when hand delivering letters to home addresses of patients. This practice is permissible but staff undertaking these tasks must take full ownership of ensuring the envelope is delivered to the correct address in a timely manner and understand that the principles of confidentiality in this situation extend beyond the workplace.

When sending confidential information to other organisations via the courier service this procedure should still be followed and all confidential information should be concealed securely in an envelope.

6 Postal Incidents

If you are notified by a patient that they have either; received a letter not for them or received someone else's letter with their own, you should:

- Apologise to the patient and advise that the matter will be investigated.
- Ask the patient to provide the name/hospital number of the other patient(s) in order to send out a replacement letter so as to not impact patient care.
- Explain that you will send a stamped addressed envelope for the return of the incorrect letters to the Trust.
- Report on Datix and inform the Information Governance team.

If a patient informs you that they have received a letter for someone who no longer lives at the address, inform them they should cross through the name and address on the envelope, write "not known at this address" and put it in the post box. There is no need to put this on Datix.

7 Document Ratification Process

The design and process of review and revision of this procedural document will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and ratified by the Director of Corporate Business.

Non-significant amendments to this document may be made, under delegated authority from the Director of Corporate Business, by the nominated author. These must be ratified by the Director of Corporate Business and should be reported, retrospectively, to the Caldicott and Information Governance Assurance Committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments,

informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

8 Dissemination and Implementation

Following approval and ratification, this procedural document will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the Director of Corporate Business and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

9 Monitoring and Assurance

This procedure is underpinned by the Information Governance Policy and the Data Protection and Confidentiality SOP.

All breaches of confidentiality must be reported on the Trust Incident Reporting System, Datix. Staff should also notify their Line Manager and the Information Governance Team.

Incidents will be managed in line with the Guide to the Notification of Data Security and Protection Incidents produced by NHS Digital and the Trust's Information Governance Incident Handling SOP.

Staff that breach confidentiality may be subject to disciplinary action in line with the Trust Performance and Conduct Policy.

10 Reference Material

- Data Protection Act 2018
- EU General Data Protection Regulation (GDPR)
- Information Commissioners Office (ICO) Website

This SOP forms part of the Information Governance suite of formal documents which can be found on Trust Documents.