Pennine Care NHS
NHS Foundation Trust

Policy Document Control Page

Title

Title: ***Policy for the electronic transfer of Person Identifiable Data - harmonised***

Version: 5

Reference Number: CO51

Supersedes

Supersedes: 4

Description of Amendment(s):

- **Updated with changes to process.**
- **Clarification on the use of NHSmail.**
- **Update to authorisation request form.**
- **Addition of Appendix 4, the use of the Trust SFTP option.**

Originator

Originated By: Jiten Patel

Designation: Head of ICT Service Delivery

Equality Impact Assessment (EIA) Process

Equality Relevance Assessment Undertaken by: Barbara Hoyle

ERA undertaken on: 3.8.11

ERA approved by EIA Work group on: 14.9.11

Where policy deemed relevant to equality-

EIA undertaken by

EIA undertaken on

EIA approved by EIA work group on

Integrated Governance Group **Referred for approval by: Head of ICT Service Delivery** **Date of Referral: 24.6.13** **Approved by: Information Governance Steering Group** **Approval Date: 26.7.13** **Executive Director Lead: Director of Planning Performance & Information**
Circulation **Issue Date: 02 October 2013** **Circulated by: Performance and Information** **Issued to: An e-copy of this policy is sent to all wards and departments**
Review **Review Date: August 2016** **Responsibility of: Head of ICT Service Delivery**
An e-copy of this policy is sent to all wards and departments (Trust Policy Pack Holders) who are responsible for updating their policy packs as required. **This policy is to be disseminated to all relevant staff.** **Date Posted: 02 October 2013**

1. Introduction

This Policy sets out the Trust's approach to the electronic transfer of Person Identifiable Data (PID) and/or Trust sensitive information. Appropriate care must be taken to protect Person Identifiable Data when it is transferred in an electronic format. The Data Protection Act requires that

> *'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or personal data and against accidental loss or destruction of, or damage to, personal data'.*

The British Standard for Information Security (BS7799) also requires that appropriate controls are put in place to maintain the security of information exchanged with external organisations, requiring procedures and standards to be established to protect information in transit.

The Policy sets out in detail the requirements for all data transfers of PID and/or sensitive data is to be authorised by the appropriate body, and encrypted before transmission.

Scope

These procedures must be applied at all times *whenever* Person Identifiable Data and/or sensitive data is transferred electronically either within the Trust, or externally.

NHSmail is excluded from this policy as encryption is automatic between the users' PC and the NHSmail service, however only messages sent to other NHSmail users or secure GSi domains are guaranteed as secure. Domains that are secure for the exchange of patient data are:

.x.gsi.gov.uk

.gsi.gov.uk

.gse.gov.uk

.gsx.gov.uk

.police.uk

.pnn.police.uk

.cjsm.net

.scn.gov.uk

.gcsx.gov.uk

.mod.uk.

The Trust does not permit the transfer of clinical information via email other than between NHSmail users and secure GSi domains detailed above. In order to meet the requirements of this Policy, any Person Identifiable Data sent via other email systems must therefore be encrypted. NHSmail does not allow encrypted files to be sent therefore another medium of transfer is required.

Methods of transfer refer to the transfer of information using the following mediums as examples:

- CD or DVD;
- Flash Memory (USB Pen drives etc)
- Secure File Transfer Protocol (SFTP) via NHS mail
- Secure File Transfer Protocol (SFTP) via Trust Server

The use of any cloud storage, such as sky drive, drop box, etc is **NOT** permitted.

Encryption software

The encryption software utilised by the Trust is WinZip version 11 with version 3.1 of the WinZip self extracting add-on software. This software will enable the creation of a Self Decrypting Archive (SDA) which will create a file that can be extracted by the recipient without the need for pre-installed software.

Securing the Information

Information will be secured using the Advanced Encryption Standard (AES) at a level referred to as 256 bit. The password used will be a minimum of 8 characters and use a combination of letters, numbers and at least one character using the Shift key and a number for example:

Example: 1aMin8tor

Under no circumstances are passwords to be transferred with the encrypted file, irrespective of the method of transfer. Passwords will be recorded against a logged call on the ICT Service Desk.

Details will be provided within the file to direct the authorised recipient to the ICT Service Desk who will provide the password upon proof of identity.

Arranging for files to be encrypted

Encryption of Person Identifiable Data will be carried out by the ICT Department following a logged request via the Service Desk on 0161 716 1234

2. Procedures

These procedures apply to all electronic transfers of Person Identifiable Data.

2.1 Authorising Transfers

2.1.1 Transfers authorisation requests

Anyone wishing to send Person Identifiable Data and/or sensitive data is required to complete an authorisation request form (Appendix 1). For one off transfers of data this form can be authorised by an appropriate Head of Department. Where regular transfers are required, approval must be sought from the Medical Director, using the attached authorisation request form (Appendix 1)

Signed authorisation forms will be held in the ICT Department for reference.

An example list of person identifiable or sensitive information is set out in Appendix 1.

2.1.2 Identifying PID to Transfer

To support any request for authorisation to transfer PID, evidence will be required indicating that consideration has been given to the amount of information to be transferred. This must be kept to a minimum, thereby ensuring compliance with the Caldicott principal of good practice, ensuring that only the minimum amount of PID is transferred per individual, balanced against the need of the commissioned or provided service objectives.

For advice on this contact the Trust’s Information Governance Manager

2.1.3 Preparing the Information for transfer

Information needs to be secured before it is transferred which will involve encrypting and making the file into a Self Decrypting Archive (SDA). This will be carried out by the ICT Department. You will need to provide the ICT Service Desk with the name, post code, and agreed security code, for example mother’s maiden name of the recipient.

The file will contain instruction to the recipient to contact the ICT Service Desk upon receipt of the file, giving them a reference number to quote. Once they telephone and quote that reference number, the recipient will be asked to provide the name, post code and an agreed security code, (for example mother’s maiden name) recorded against the job. The password to decrypt the file will only be released once this information has been verified as correct.

2.2 Transferring the Information

Once files have been encrypted by the ICT Service Desk the following details will be recorded by the ICT Service Desk against the logged call:

- Date and time file created
- Short description of the file content
- Location of file to be encrypted
- Password used
- Address of the recipient
- Name, post code and agreed security code, for example mother’s maiden name of authorised recipient (it must be clear who is going to be receiving this information, and only this person will have the password disclosed)

Guidance is provided below on four commonly used mediums of data transfer.

2.2.1 Writeable CD/DVD

Once the ICT Department have encrypted the file it will be “burnt” onto a CD or DVD. The INC reference number will be written on the CD/DVD and will be passed onto the staff member to send to the recipient.

CDs and DVDs ***must*** be sent as outlined in the Appendix 2 ensuring a full audit trail exists for the transfer. It is the sender's responsibility to ensure that the recipient destroys the CD/DVD once the data has been extracted.

2.2.2 USB Flash Memory

The Trust mandates the use of a particular type of Pen Drive which is secured with a password. Details can be obtained from the ICT Department. Following the transfer of community services, encrypted pen drives previously issued by the PCT, such as "ironkey" and "safesticks" will be allowed to connect to the Trust network. These devices will need to be activated prior to use by contacting the ICT Service Desk on 0161 716 1234. Only these authorised devices will work on a PC connected to the Trust's network. The device should be inserted into the PC and the relevant file copied from the network drive to the device. Due to the portable nature of these devices, extra care should be taken to avoid loss, and any PID should be deleted from the device as soon as possible after use.

Where required by the recipient non approved USB Memory drives can be used, and the encrypted file will be saved onto the drive, following the same procedure as CD/DVD transfer.

2.2.3 NHSmail Secure File Transfer Protocol (SFTP)

This is a program used to transfer files up to 1Gb of size to other NHS organisations. The system utilises NHSmail security so that the transmission of data is secure at all times. This system is provided by Health & Social Care Information Centre (formally Connecting for Health) and requires both the sender and recipient to have an NHSmail email account. Appendix 3 provides a flow diagram to support decision making in whether to make use of this facility.

2.2.3 Trust Secure File Transfer Protocol (SFTP)

This is a Trust system that allows files to be transferred securely to external recipients. The system utilises secure file transfer protocol so that the transmission of data is secure at all times, it does require the recipient to have FTP software to access the files. A temporary username and password is provided to allow the recipient to access and download the file. Where regular transfers are required this is the Trust's preferred method of transmission. This system is provided and managed by the Trust ICT Department. Appendix 4 provides a flow diagram to support decision making in whether to make use of this facility.

3. Audit Procedures

A minimum of two audits will be carried out within any year to ensure adherence to this Policy. Details of these checks will be held against the ICT Service Desk log associated with the encrypted files. The audits will be undertaken by the Information Governance Manager, or nominated representative. The results of the audit will be reported to the Information Governance Steering Group.

4. Breaches

Any Person Identifiable Data that is transferred without encryption as detailed in this Policy **must** be reported to the Trust's Information Governance Manager and an incident form completed. Any such incidents will be fully investigated and may result in disciplinary action being taken.

5. Training

All Trust staff will be made aware of their responsibilities when transferring Person Identifiable Data through generic and specific training program and guidance.

6. Review

This policy will be reviewed every two years or sooner if new legislation or national guidance is introduced.

APPENDIX 1

Pennine Care NHS
NHS Foundation Trust

SERVICE REQUEST: AUTHORISATION FORM FOR THE ELECTRONIC TRANSFER OF PERSON IDENTIFIABLE DATA

I request authorisation to transfer person identifiable data items via the following mechanism:

USB Pen drive □

CD/DVD □

Secure FTP via NHSmail □

Secure FTP via Trust Server □

Other □ Please specify …………………………………………..

I have read and agree to abide by the Policy for the electronic transfer of Person Identifiable Data.

Name: …………………………………… Job Title: ……………………………………

Signed…………………………………… Date: ………………………………………..

The following data items will be transferred:

Sender	Recipient, department/person	Purpose	Data items (see below)

Name of Recipient: ………………………………………………………………………………

Contact Number of Recipient ………………………………………………………………..….

Address Inc. Postcode of Recipient………………………………………………………………

Agreed Security Question and Answer……………………………………………………..……..

Location of File to be encrypted …………………………………………………………….…..…

Definition of Data Items

No.	Data Item	Definition	
1	Personal	Name Date of birth Next of kin Personal circumstances	Financial information Physical description Gender
2	Personal/ Sensitive	Racial/ethnic origin Religion/Belief Sexual Orientation Disability Trade Union membership	Court Proceedings Criminal convictions Political opinions
3	Clinical (Sensitive)	Information relating to physical or mental health or condition	
4	Demographic	Address Postcode Telephone number	Location description Directions
5	Other	Environmental Social	Health Professional

Line Manager Authorisation

I authorise the above named to make the electronic transfer of Person Identifiable Data as described above.

☐ This is a one-off authorisation

☐ This is to authorise this request to be forwarded to the Medical Director for consideration

Name: …………………………………… Job Title: ……………………………………

Signed…………………………………… Date: ………………………………………..

**********************INTERNAL USE ONLY*************************

Medical Director Authorisation

☐ Authorised ☐ Rejected - Reason for rejection ………………………………………

…………………………………………………………………………………………….

Name: ……………………………Signature………………………………Date:…………………..

APPENDIX 2

Pennine Care NHS
NHS Foundation Trust

SENDING PERSON IDENTIFIABLE DATA VIA MAIL

Transfer of any form of Person Identifiable Data via mail is only permissible by the following methods:

1. Recorded Delivery
2. Royal Mail Special Delivery
3. Courier Service

Each item for posting must be delivered to Trust HQ reception accompanied by either form RDB1 or RDB2 below..

Please note that if the item arrives at Trust HQ without the appropriately completed form, the item will be seriously delayed until the sender’s information is to hand. It is not sufficient to write ‘Recorded Delivery’ etc., on the envelope/parcel as the postal staff do not have any way of tracing the origin of such mail.

Pennine Care NHS
NHS Foundation Trust

FOR INTERNAL USE ONLY

CONFIDENTIAL/SENSITIVE DATA MAIL FOR HAND DELIVERY VIA THE INTERNAL POSTAL ROUTE i.e. Borough to Borough
Please complete this form for any highly confidential/sensitive mail to be hand delivered within the internal postal route by the Trust HQ Postman *(the form should be stapled to the envelope/parcel)*

REQUESTED BY: ……………………………………………………………(Please print name)

Borough ……………………………. Tel No …………………… … Date ……..………………...

Date:		
Code no(s).		
Contents: **e.g. CD/DVD, case number and volume (DO NOT USE PATIENT INDENTIFIABLE INFORMATION)**		
Delivery location:		
Signature on collection:		
Print name:		**Date**
Signature on delivery:		
Print name:		**Date**

FORM RDM1

Pennine Care NHS
NHS Foundation Trust

FOR EXTERNAL USE ONLY

REQUEST FOR MAIL TO BE SENT BY RECORDED DELIVERY/ROYAL MAIL SPECIAL DELIVERY/COURIER SERVICE

Please complete the following details:-

REQUESTED BY: ………………………………………………………….(Please print name)

Borough: ………………………… Tel No. …………………….. Date ……….………

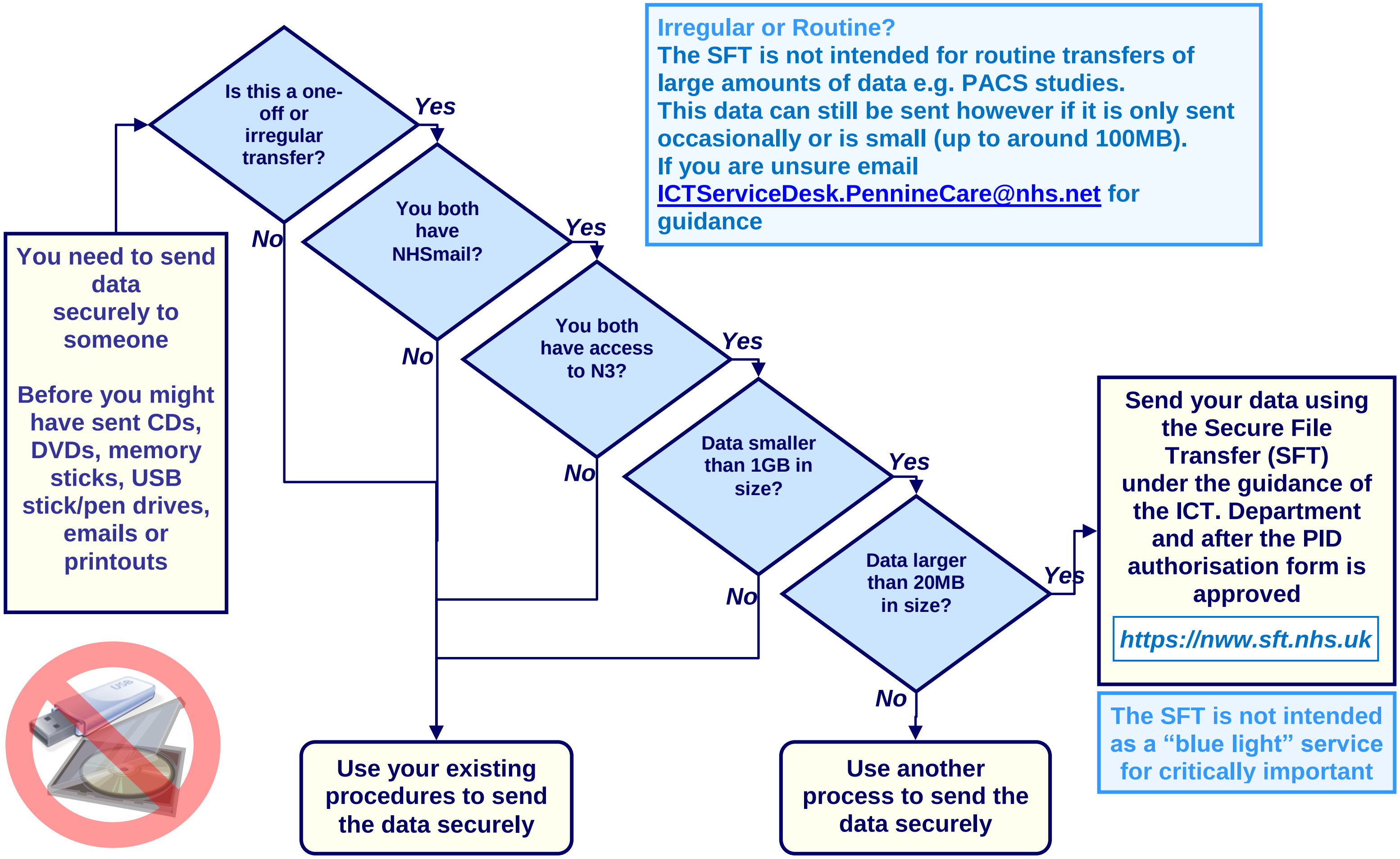
Date:	
Code no(s).	
Contents: **e.g. CD/DVD, case number and volume (DO NOT USE PATIENT INDENTIFIABLE INFORMATION)**	
Delivery location:	

Signature on collection:		
Print Name		**Date:**
Dispatched by: **Signature**		
Print name:		**Date:**

FORM RDM2

APPENDIX 3

When to use the SFT



You need to send data securely to someone

Before you might have sent CDs, DVDs, memory sticks, USB stick/pen drives, emails or printouts

Is this a one-off or irregular transfer?

You both have NHSmail?

You both have access to N3?

Data smaller than 1GB in size?

Data larger than 20MB in size?

Send your data using the Secure File Transfer (SFT) under the guidance of the ICT. Department and after the PID authorisation form is approved

https://nww.sft.nhs.uk

Use your existing procedures to send the data securely

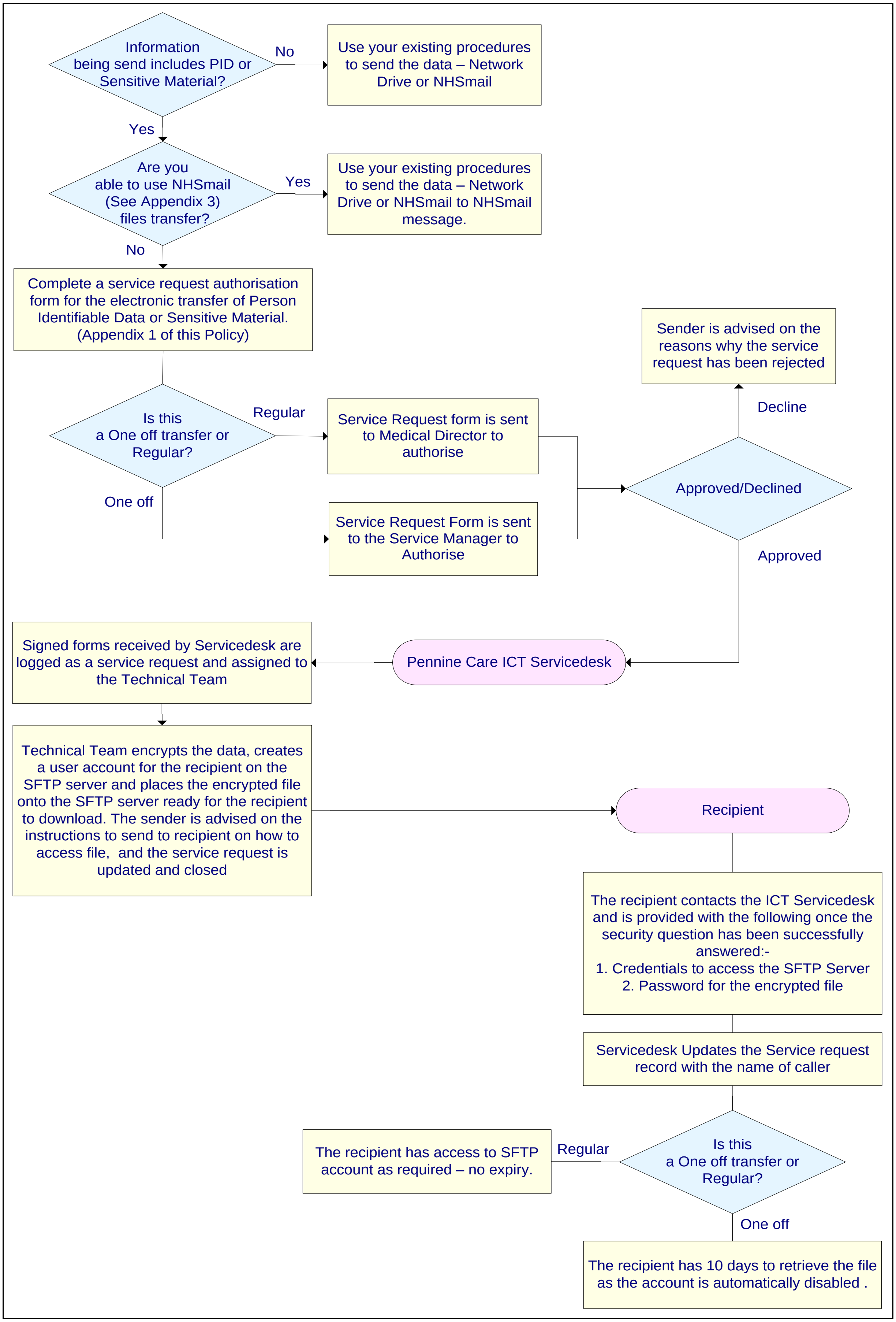
Use another process to send the data securely

Irregular or Routine?
The SFT is not intended for routine transfers of large amounts of data e.g. PACS studies.
This data can still be sent however if it is only sent occasionally or is small (up to around 100MB).
If you are unsure email ICTServiceDesk.PennineCare@nhs.net for guidance

The SFT is not intended as a "blue light" service for critically important

Pennine Care Secure File Transfer (SFTP)

Appendix 4



Information being send includes PID or Sensitive Material?

No: Use your existing procedures to send the data – Network Drive or NHSmail

Yes: Are you able to use NHSmail (See Appendix 3) files transfer?

Yes: Use your existing procedures to send the data – Network Drive or NHSmail to NHSmail message.

No: Complete a service request authorisation form for the electronic transfer of Person Identifiable Data or Sensitive Material. (Appendix 1 of this Policy)

Is this a One off transfer or Regular?

Regular: Service Request form is sent to Medical Director to authorise

One off: Service Request Form is sent to the Service Manager to Authorise

Approved/Declined

Decline: Sender is advised on the reasons why the service request has been rejected

Approved: Pennine Care ICT Servicedesk

Signed forms received by Servicedesk are logged as a service request and assigned to the Technical Team

Technical Team encrypts the data, creates a user account for the recipient on the SFTP server and places the encrypted file onto the SFTP server ready for the recipient to download. The sender is advised on the instructions to send to recipient on how to access file, and the service request is updated and closed

Recipient

The recipient contacts the ICT Servicedesk and is provided with the following once the security question has been successfully answered:-
1. Credentials to access the SFTP Server
2. Password for the encrypted file

Servicedesk Updates the Service request record with the name of caller

Is this a One off transfer or Regular?

Regular: The recipient has access to SFTP account as required – no expiry.

One off: The recipient has 10 days to retrieve the file as the account is automatically disabled .