Harrogate and District
NHS Foundation Trust

CONFIDENTIALITY AND SECURITY OF PERSONAL INFORMATION POLICY

Version	Date	Purpose of Issue/Description of Change	Review Date
1	July 2014	Amalgamation of the Policy in Respect of Confidentiality of Patient Information and Safe Haven's & Communication of Personal Information Policy	July 2019
1.1	Dec 2014	Minor amendment	
2	Sept 2015	Review and update	
3		Review and update	

Status	Open	
Publication Scheme	Our Policies and Procedures	
FOI Classification	Release without reference to author	
Function/Activity	Information Governance	
Record Type	Policy	
Project Name	N/A	
Key Words	Information Governance, Confidentiality, Patient Information, Personal Information, Sensitive Information, Data Protection, Information Security	
Standard	Information Governance Toolkit	
Author	Information Governance Manager	**Date/s**
Approval and/or ratification body	Data and Information Governance Steering Group	28th July 2017

CONTENTS

1. INTRODUCTION

1.1 Purpose

The purpose of this policy is to outline the principles that must be adhered to by all who work within and have access to personal information and sensitive personal information.

1.2 Scope

This policy applies to all staff employed or contracted and voluntary staff.

1.3 Definitions

Personal information incorporates the following factors:

- surname, forename, initials
- address, postcode
- telephone number
- date of birth (any other dates e.g. medical dates, dates of diagnosis)
- occupation
- sex
- national insurance number

Sensitive personal information is data that contains details of a person's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life, convictions
- legal proceedings against the individual or allegations of offences committed by the individual

2 USE AND DISCLOSURE OF PERSONAL INFORMATION

2.1 Why Personal Information is Collected

Information is collected about patients to:

- support patient care
- improve health and social care services
  - commissioning - the people who plan health and care services need information about the types of illnesses people have and the treatments they receive, as well as the result of that care or treatment. They can then check to make sure that people are getting the services that are right for them.
  - public health - some information is used for public health. The information lets the NHS look ahead and plan what to do if there are outbreaks of diseases. It also helps the NHS to take action now to stop problems from happening in the future.
  - research - information helps to improve medicines and treatments for patients. Researchers study the information to find better ways to prevent illness and treat conditions.
  - risk stratification - information can be used to identify who is most at risk of particular diseases and conditions, so those who plan care can provide preventative services and patients can be targeted with particular treatments.
  - invoice validation - information is used to make sure that NHS organisations receive the correct payments for the services they provide to individuals.

2.2 Disclosure of Personal Information for Care Purposes

Personal information can be shared between healthcare professionals when it is in the best interests of an individual and they are providing direct care.

2.3 Disclosure of Personal Information for Non-Care Purposes

2.3.1 Objections made by service users to the use or sharing of confidential information

Patients have the right to request that their identifiable information is not used for purposes beyond their care and treatment and have their objections considered. The process for considering objection should:

- include the most senior healthcare professional caring for the individual
- Include whether not supporting the objection will damage the effectiveness of care
- Include whether there is a demonstrable risk that the safety of the patient will be reduced by not upholding the objection
- Include whether there are compelling legitimate grounds relating to the individual's situation

Where their wishes cannot be followed, to be told he reasons including the legal basis. The request and the outcome must be recorded in the patient's health records.

2.3.2 Consent

When disclosing personal information for non-care purposes consent cannot be implied and so must be specifically sought or there must be some other lawful basis for disclosing the information.

Steps that should be followed:

1. Make sure you are authorised to share patient information for non-care purposes.
2. Discuss the purpose of the disclosure with the patient.
3. Ensure the patient understands what their information is going to be used for, e.g. get them to relay back to you their understanding of the purpose of the disclosure.
4. Obtain their consent to the disclosure either verbally or in writing.
5. Record the disclosure decision - whether consent is given or declined - as this will ensure the patient is not repeatedly asked for the same permission

2.3.3 Where consent may not be required

Sometimes researchers require specific information about individuals that cannot be anonymised or pseudonymised in a safe haven, and gaining explicit consent may be highly impractical. Legislation is in place that allows personal confidential data to be processed for medical purposes such as research. Regulations under section 251 of the NHS Act, allows the common law duty of confidence to be set aside under specific circumstances. Applicants must demonstrate that the aim of the processing is in the public interest, that anonymised information could not be used to achieve the required results, and that it would be impractical, both in terms of feasibility and appropriateness, to seek specific consent from each individual affected. For research the approval of a Research Ethics Committee is also needed. The key test is one of necessity, not convenience.

There are also other circumstances where consent may not be appropriate for example in cases relating to safeguarding and police. For further guidance please see Safeguarding Documents or the Police Policy.

2.4 Routinely Sharing Personal Information

It is necessary for a sharing agreement and protocol to be completed and signed by the Caldicott Guardian when routinely sharing information with other organisations especially for non-care purposes.

The Trust requires an Information Sharing Protocol with each organisation and requires an Information Sharing Agreement for each separate request for sharing of information.

- Information Sharing Protocol Template
- Information Sharing Agreement Template

3 PERSONAL INFORMATION SECURITY

3.1 Physical Security

Personal information must always be held securely. In any area which is not secure, and which can be accessed by a wide range of people (including possibly the public), such information must be locked away immediately after it has been finished with. Where it is impractical for this to be achieved, access to the work area must be restricted.

Where it is necessary to take confidential information away from Trust premises in order to carry out your duties (e.g. home visit to a patient), you must keep the information secure and make every effort to ensure that it does not get misplaced, lost or stolen.

3.2 Electronic Security

You must lock your computer and mobile devices when unattended. Always log off systems and do not leave your Smartcard unattended.

Mobile devices, memory sticks and laptops must be encrypted. Please refer to IT for further guidance.
Information should be held on the organisation's network servers, and not stored on local hard drives.

Personal information stored on network shared drives should be restricted as appropriate. IT can assist in establishing folder access rights.

Information should not be saved or copied into any PC or media that has not been approved by IT.
Safe Haven folders should have access restrictions imposed by the IT Helpdesk. The IT helpdesk should be advised of new access requests for that location. The request form at Appendix 3 should be completed and signed by the Line Manager and Head of the Department before being sent to the IT Helpdesk and a copy sent to the Information Governance Manager.

3.3 Safe Transfer of Personal Information

When transferring any personal information you must:

- ensure the person is entitled to receive the information
- use the most appropriate method to ensure that the information is transferred securely
- limit the information to only what is required, irrelevant information must be removed or redacted (blocked out) before the transferring
- ensure that you are sending information to the correct location
- ensure that no additional information is sent in error
- only send information to those who are entitled to receive it
- mark it 'Private and Confidential'

3.3.1 Post

- Incoming mail must be opened away from public areas.
- All mail must be checked before posting to ensure it is going to the correct address and that nothing additional has been put in the envelope in error.
- All mail that contains personal information must be enclosed in a sealed envelope and marked 'Private and Confidential', addressed correctly.
- All mail containing sensitive personal information must be sent via Special Delivery or by a courier (TNT)
- Bulk amounts of personal information must be sent via Special Delivery or by a courier (TNT)

3.3.2 Email

- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password
- You should not set up your emails to be automatically forwarded to another account, you should set up an out of office to identify who emails should be forwarded to
-

For HDFT to HDFT or NHS.net to NHS.net

- You must check you are sending the email to the correct email address
- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password
- You must not send the password in the body of the email or a following email. You must contact the person you are sending the email to and confirm the password.

For HDFT to any email address

- You must check you are sending the email to the correct email address
- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password
- You must not send the password in the body of the email or a following email. You must phone the person you are sending the email to and confirm the password.
- Send the recipient the Encrypted Email Instructions before emailing them the confidential or sensitive email
- Then type the word 'Encrypt' in the subject field on the email to encrypt the whole email

For NHS.net to any email address

- You must check you are sending the email to the correct email address
- You should put any confidential or sensitive information in an attachment and encrypt the attachment with a password
- You must not send the password in the body of the email or a following email. You must contact the person you are sending the email to and confirm the password.
- Send the recipient the and Receiver Guidance before emailing them the confidential or sensitive email

- Then follow these instructions to encrypt the whole email Sender Guidance

3.3.3 Verbal

- The identity of the enquirer must always be verified by checking the any relevant details, for example if it is a patient ask them to confirm their date of birth, address, attendance dates etc. If the enquiry is via the phone, call them back so that the identity can be fully verified. In the case of an organisation, the switchboard number must be used to call back, not a direct dial number.
- If answering machines are used by departments they should be setup so that messages left are recorded silently. This will ensure that no unauthorised personnel overhear confidential messages whilst they are being recorded.

3.3.4 Fax

The fax machine should be sited in a secure location where access to the machine is controlled.

Sending

- By each fax machine there should be a laminated copy of the Fax Flow Chart (Appendix 4) which acts a prompt to follow the correct procedures when sending a fax.
- All external faxes must use the Trust's Fax Cover Template
- All faxes, internal or external, containing patient information or other confidential information must use the Trust's Fax Cover Template
- Check the recipients fax number, memory alone must not be relied on when dialling. It is acceptable to pre-programme commonly used fax numbers into the machine's memory. However, a list of speed dial numbers must be prominently displayed next to the machine.
- Check if the fax machine is a Safe Haven. If it isn't telephone the recipient of the fax let them know that you are about to send a fax containing confidential information and ask if they will wait by the fax machine whilst you send the document and acknowledge the receipt of the fax.
- Dial the number carefully.
- Monitor the transmission.
- Stop the transmission if there appear to be any anomalies with the transmission.
- Obtain a printed record of the transmission where possible.
- No paperwork must be left unattended at the fax machine.
- If a published fax number turns out to be incorrect, inform all interested parties of the error and amend the list as necessary.

Receiving

- The recipient should remove the fax from the machine on receipt.
- Where necessary, the recipient should contact the sender to confirm receipt and that the fax will be appropriately dealt with and safely stored.

3.3.5 Secondary use

Patient identifiable data for secondary use (for example research purposes, audit, service management, commissioning, contract monitoring and reporting facilities etc.) should not be sent outside the Safe Haven folder location. There are two options for transferring data for secondary use. The first is to suitably anonymise the data so it is not identifiable. The second, for where patient level data (but not identifiable data) is required, is to pseudonymise the data so individual records can be viewed which do not identify the patient. Please refer to the Pseudonymisation & Anonymisation of Data Policy for further guidance.

4 ACCESS TO HEALTH RECORDS

Data Protection Act 1998 governs access to the health records of living people. The Access to Health Records Act 1990 governs access to the health records of deceased people.

4.1 Applying for Access

If someone wishes to have copies of health records they need to complete an application form. Forms are available via the following methods:

- Trust Intranet: Corporate Services Directorate > Information Governance > Quick Guides and Useful Websites > Access to Health Records
- Trust Website: Patient and Visitors > Your Personal Details > Access to Your Health Records
- In Writing: Information Governance Officer, Medical Records Department, Harrogate District Hospital, Lancaster Park Road, Harrogate HG2 7SX
- By Phone: Information Governance Officer - 01423 553284

4.2 Solicitor Access to Health Records

A solicitor can act on behalf of a patient to access health records. These requests for copies of health records must be forwarded to the Information Governance Officer.

4.3 Fees

Under the Data Protection Act 1998 (Fees and Miscellaneous Provisions) Regulations 2001 the maximum fee that can be charged for providing copies of health records is £10 for computer records and £50 for copies of paper records or a mixture of computer and paper records. The Trust charges £15 for copies of paper records and £10 for radiology CDs.

4.4 Time Limit

Once the Information Governance Officer has received the completed application form and the access fee the Trust will comply with the request within 40 days and where possible 21 days.

4.5 Whole or Partial Exemptions

The Data Protection (Subject Access Modification) (Health) Order 2000 enables the data controller to limit or deny access to an individual's health record where:

- The information may cause serious harm to the physical or mental health or condition of the patient, or any other person, or
- Access would disclose information relating to or provided by a third person who has not consented to that disclosure unless:
  - The third party is a healthcare professional who has compiled or contributed to the health records or who has been involved in the care of the patient
  - The third party, who is not a health professional, gives their consent to the disclosure of that information.
  - It is reasonable to disclose without that third party's consent

Please note that fear of the Trust receiving legal action is not a reason for denying access.

4.6 Children's Health Records (Under the age of 16)

As a general rule a person with parental responsibility will have the right to apply for access to a child's health record. However, in exercising this right a healthcare professional should give careful consideration to the duty of confidentiality owed to the child before disclosure is given.

4.7 Deceased Patient's Health Records

Under the Access to Health Records Act 1990 when a patient has died, their personal representative or executor or administrator or anyone having a claim resulting from the death (this could be a relative or another person), has the right to apply for access to the deceased's health records.

4.8 Informal Access to Health Records

A patient can request to view their health record with the healthcare professional whilst still a current patient with no charge at the healthcare professional's discretion. If the patient then wishes to have copies of their records the request changes to formal access and they will need to complete an application form.

5 BREACHES OF CONFIDENTIALITY

All employees are required to:

- Maintain the confidentiality of information about the Trust, its staff and its patients in accordance with the Trust's Information Governance policies and Data Protection Act 1998 and other legislation outlined in section 7, during and after the termination of employment.
- Only access confidential information that they are required to do so as part of their role.
- Implement the appropriate technical and physical measures to ensure that confidential information is safe and secure.

- Familiarise themselves with the Trust's Information Governance policies and Data Protection Act 1998 principles.
- Undertake Information Governance training on an annual basis.

Failure to comply with or adhere to the Trust's Information Governance Policies or the Data Protection Act will be treated as misconduct under the Trust's Disciplinary Policy, which may result in dismissal or criminal proceedings. The Trust's Information Governance Policies are available on the Trust's intranet page.

As an individual, you do have the right to apply to view or have copies of your own records via the appropriate routes. You do not have the right to directly access your own records. Inappropriate access to confidential information will be treated as misconduct under the Trust's Disciplinary Policy which may result in dismissal and/or criminal proceedings.

6 NEW PROCESSES, SERVICES, INFORMATION SYSTEMS

When setting up new process, services and information systems which hold and use person identifiable information must follow certain steps to ensure that data protection and confidentiality issues have been properly considered and managed prior to procurement and implementation. These steps are outline in the Information Risk Management Policy

7 LEGAL FRAMEWORK

7.1 Caldicott Principles

The Caldicott Principles represent best practice for using and sharing identifiable personal information and should be applied whenever a disclosure of personal information is being considered.

1) Justify the purpose(s)
2) Don't use personal confidential data unless it is absolutely necessary
3) Use the minimum necessary personal confidential data
4) Access to personal confidential data should be on a strict need-to-know basis
5) Everyone with access to personal confidential data should be aware of their responsibilities
6) Comply with the law
7) The duty to share information can be as important as the duty to protect patient confidentiality

7.2 Data Protection Act 1998

The Data Protection Act 1998 provides eight principles that apply to all use and disclosure of personal information.

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
    a. at least one of the conditions in Schedule 2 is met, and

   b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4) Personal data shall be accurate and, where necessary, kept up to date.
5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6) Personal data shall be processed in accordance with the rights of data subjects under this Act.
7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

7.3 Common Law Obligations

The Common Law Duty of Confidentiality position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

7.4 NHS Care Record Guarantee for England

The Care Records Guarantee sets out high-level commitments for protecting and safeguarding patient information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

7.5 NHS Code of Practice on Confidentiality

The NHS Code of Practice on Confidentiality is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.

7.6 NHS Code of Practice on Information Security Management

The NHS Code of Practice on Information Security Management is a guide to the methods and required standards of practice in the management of information security for those who work within, under contract to, or in business partnership with NHS organisations in England. Its purpose is to identify and address security management in the processing and use of NHS information and is based on current legal requirements, relevant standards and professional best practice.

7.7 A Guide to Confidentiality in Health and Social Care

The Health and Social Care Information Centre has produced a Guide to Confidentiality in Health and Social Care which explains the various rules about the use and sharing of confidential information. It has been designed to be easily accessible and to aid good decision making. It also explains the responsibility organisations have to keep confidential information secure.

7.8 The NHS Act

Section 251 of the NHS Act enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be transferred to an applicant without the discloser being in breach of the common law duty of confidentiality. The Confidentiality Advisory Group (CAG) review applications and advise whether there is sufficient justification to access the requested confidential patient information. Using CAG advice as a basis for their consideration, the Health Research Authority or Secretary of State will take the final approval decision.

7.9 Health and Social Care (Safety and Quality) Act 2015

The Health and Social Care (Safety and Quality) Act 2015 supports the sharing of information relating to an individual for the purposes of providing that individual with health or social care services in England;

7.10 NHS Constitution for England

The NHS Constitution for England states that patients *"have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure"*

7.11 NICE Clinical Guideline 138 and Quality Standard 15

Under the NHS Standard Contract a provider must at least once in each contract year audit its practices against quality statements regarding data sharing set out in NICE Clinical Guideline 138. Quality Standard 15 contains the quality statements:

- Quality Statement 12: Coordinated care through the exchange of patient information
- Quality Statement 13: Sharing information with partners, family members and carers

7.12 Care Professionals' Code of Practice

Care professionals must also comply with the codes of practice of their respective professionals.

7.13 Human Rights Act

Article 8.1 of the European Convention on Human Rights enshrined in Schedule 1 of the Human Rights Act 1998, provides that "*everyone has the right to respect for his private and family life, his home and his correspondence.*" This is however, qualified

by reasons where it may be legitimate to infringe this right. As stated in Article 8.2, these are "*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The right to privacy will be respected unless it can be shown that there is a legitimate reason to infringe those rights.

7.14 Statistics and Registration Service Act 2007

The Statistics and Registration Service Act 2007 permits NHS organisations to submit 'patient registration information' to the Statistics Board for the production of population statistics. This means information about individuals who are or have been registered in England or Wales to receive primary medical services. The information includes:

- address and any previous address
- date of birth and sex
- patient identification number
- history of registration.

Information about the health or condition of, or the care or treatment provided, is specifically excluded from disclosure and must not be shared with the Statistics Board.

8 ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has ultimate responsibility for compliance with the Data Protection Act 1998 and should ensure that

- responsibility for brining data protection issues for consideration by the senior level of management is delegated appropriately *(Senior Information Risk Officer)*
- a data protection lead or manager is in place to organise and enforce the approach to data protection and report directly to the above individual *(Data Protection Officer)*
- the role of the Caldicott Guardian is appropriately assigned and supported

Caldicott Guardian

The Caldicott Guardian:

- oversees the arrangements for the use and sharing of patient information
- plays a key role in ensuring the highest standards for handling patient identifiable information
- actively supports work to enable information sharing where appropriate to share
- advises on options for lawful an ethical processing the information
- represents and champions confidentiality and information sharing requirements and issues at senior management level

The Caldicott Guardian is required to be registered on the National Register of Caldicott Guardians.

Data and Information Governance Steering Group
The Data and Information Governance Steering Group has overall responsibility for overseeing the development and the implementation of information governance policies, procedures, audits and action plans. The DIGSG also reviews untoward occurrences and incidents relating to information governance and ensures that effective remedial and preventative action is taken. The Group also acts as the Caldicott Function. It is made up of Senior Information Risk Owner, Data Protection Officer, Information Governance Manager and Head of Patient Systems & Health Records.

The Caldicott Function:
- supports the Caldicott Guardian
- ensures the confidentiality and data protection work programme is successfully coordinated and implemented
- ensures compliance with the principles contained within the Confidentiality: NHS Code of Practice and that staff are made aware of individual responsibilities
- completes the Confidentiality and Data Protection Assurance component of the Information Governance Toolkit, contributing to the annual assessment
- provides routine reports to the senior management on confidentiality and data protection issues
- identifies and address any barriers for sharing information

Senior Information Risk Owner
The Trust's Senior Information Risk Officer (SIRO) is the Chief Operating Officer. The SIRO:
- takes overall ownership of the Organisation's Information Risk Policy
- acts as champion for information risk on the Board of Directors
- implements and leads the NHS information governance risk assessment and management processes within the Organisation
- advises the Board of Directors on the effectiveness of information risk management across the Organisation

Data Protection Officer
The Data Protection Officer ensures that the Trust complies with the Data Protection Act 1998, and ensures that employees are fully informed of their own responsibilities for acting within the law and that the public, including employees, are informed of their rights under the Act.

Information Governance Manager
The Information Governance Manager is responsible for managing the organisations Information Governance function, including setting and implementing appropriate policies and procedures as well as ensuring appropriate audits and monitoring mechanisms are undertaken.

Information Governance Officer
The Information Governance Officer provides support to the Information Governance Manager. The Information Governance Officer ensures appropriate responses to all subject access requests within the allocated timescale, liaising with the appropriate healthcare professionals.

Information Security Officer
The Information Security Officer Is responsible for providing advice on all aspects of information security and risk management. The quality of their assessment of information security risks, threats and advice on controls will contribute significantly to the effectiveness of the organisation's information security.

Unit/Department Managers
Unit/department managers are responsible for data protection practice within their work area ensuring:

- the working practices carried out within the unit/department are in line with the Trust's policies
- all staff within the work area are adequately trained and aware of their personal responsibilities for data protection issues

All staff
All staff must ensure that they are following all Trust Policies and Procedures and legislation outlined in section 7. Failure to comply with or adhere to the Trust's Policies and Procedures or legislation will be treated as misconduct or gross misconduct under the Trust's Disciplinary Policy, which may result in dismissal and/or criminal charges.

9 POLICY DEVELOPMENT

The stakeholders of this policy are all staff employed or contracted and voluntary staff

10 CONSULTATION, APPROVAL AND RATIFICATION PROCESS

The consultation process undertaken at current document review is documented in Appendix 1. This document will be approved and ratified by the Data and Information Governance Steering Group.

11 DOCUMENT CONTROL

This document will be available on the Trust Intranet for read only access. As the document replaces a previous version, the old document will be archived within the intranet. The front page of the document will indicate the version number, the approving body and the date of approval, along with the next review date.

Copies of this document should not be printed unless it is absolutely necessary, as there is a risk that out of date copies may be in circulation.

Requests for this document in an alternative language or format (such as Braille, audiotape, large print etc.) will be considered and obtained whenever possible.

12 DISSEMINATION AND IMPLEMENTATION

A “publish and point” method of communication will be used, where relevant staff are informed about the publication of a new or revised document on the intranet.

13 MONITORING COMPLIANCE AND EFFECTIVENESS

The Trust will monitor this Policy through the Information Governance Toolkit. An assessment of compliance with requirements, within the Information Governance Toolkit will be undertaken each year. Annual reports and proposed action/development plans will be presented to the Trust Board for approval prior to submission to the toolkit. It is assumed that both Internal and External Audit will review this and associated procedures.

14 REFERENCE DOCUMENTS

- Caldicott Principles
- Data Protection Act 1998
- Care Records Guarantee
- NHS Code of Practice on Confidentiality
- NHS Code of Practice on Information Security Management
- Guide to Confidentiality in Health and Social Care
- The Health and Social Care (Safety and Quality) Act 2015
- NHS Constitution for England
- NHS Standard Contract
- NICE Clinical Guideline 138
- Quality Standard 15
- Quality Standard 15, Quality Statement 12
- Quality Standard 15, Quality Statement 13
- Human Rights Act 1998
- Statistics and Registration Service Act 2007

15 ASSOCIATED DOCUMENTATION

- Safeguarding Documents
- Police Policy.
- Information Sharing Protocol Template
- Information Sharing Agreement Template
- Fax Cover Template
- Pseudonymisation & Anonymisation of Data Policy
- Information Risk Management Policy

16 APPENDICES

Appendix 1: Consultation Summary
Appendix 2: Procedure for Requesting New Access to a Network Drive Location That Contains Person Identifiable Information (Safe Haven)
Appendix 3: Safe Haven Access Request Form
Appendix 4: Procedure for Sending Faxes

Appendix 1: Consultation Summary

Those listed opposite have been consulted and any comments/actions incorporated as appropriate. The author must ensure that relevant individuals/groups have been involved in consultation as required prior to this document being submitted for approval.	**List Groups and/or Individuals Consulted**
	Data Protection Officer
	Caldicott Guardian
	Data and Information Governance Steering Group
	Information Governance Leads

Appendix 2: Procedure for Requesting New Access to a Network Drive Location That Contains Person Identifiable Information (Safe Haven)

Background

In order to ensure that the organisation and its employees comply with the Data Protection Act 1998 and relevant policies, the following procedure must be followed for any new access requests to locations on the network drive where personal (staff or patient identifiable) information is being held. This includes the completion of a Safe Haven Access Form

Any electronic form of identifiable data should be password protected where possible and stored in an access restricted folder on the network drive. The access restriction must be specific enough so only those employees who require access to the data to perform their roles can.

The access request form will be used for any new access requests to agreed Safe Haven locations. For example this may be a new member of staff, or a member of staff changing roles or taking on further responsibilities, though other valid circumstances may exist. Also should a member of staff already have access to a Safe Haven and move job roles, this access should be reviewed and in some cases revoked.

Process

When a need for new access to an identified Safe Haven location arises, the direct line manager of the employee should complete the attached form (Appendix 4) and obtain approval by the Head of Department.

The form should then be sent to the IT Helpdesk, copying in the Information Governance Manager who will keep as a record. The IT Helpdesk should then implement the request.

If you believe a new Safe Haven location needs to be set up please contact the Information Governance Manager for advice in the first instance.

Appendix 3: Safe Haven Access Request Form

Safe Haven Access Request Form

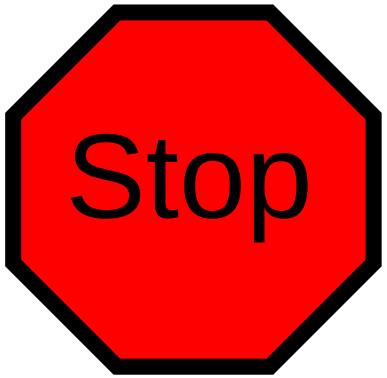
Name of Employee	
Job Role	
Base Location	
Full Network location(s) for which access is required (e.g. F:isserver\infoserv\data\Information Governance)	
Why is this access needed? (e.g. is there a specific task the employee is required to do that requires this data?)	

Line Manager:		
I confirm that I have read and understood the procedure for requesting new access to a network drive location that contains Person Identifiable Information (Safe Haven)		
Signature		Date:
Name:		
Job Title:		
Tel:		
Base:		
Head of Department:		
Further action required: Approved: Yes ☐ No ☐		
Signature		Date:
Name:		
Job Title:		
Tel:		
Base:		

Appendix 4: Procedure for Sending Faxes

Harrogate and District NHS
NHS Foundation Trust

Guidelines for Sending Secure Faxes

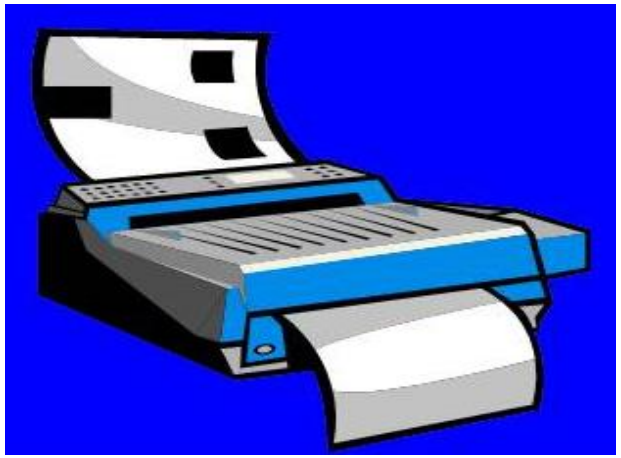


Is your fax going **outside** of the organisation?

Yes → Use the Trust's Fax Cover

Does your fax contain **patient information** or **other confidential information**?

Yes → Use the Trust's Fax Cover



- Check the recipient's number.
- If sending confidential information, check if the fax machine is a Safe Haven. If it isn't, telephone the recipient of the fax, let them know that you are about to send a fax containing confidential information and ask if they will wait by the fax machine whilst you send the document and acknowledge receipt of the fax.
- Dial the number carefully.
- Monitor the transmission.
- Stop the transmission if there appear to be any errors with the transmission.
- Obtain a printed record of the transmission where possible.
- No paperwork should be left unattended at the fax machine.