University Hospital Southampton NHS
NHS Foundation Trust

Data Protection and Confidentiality Policy

Version: 5

Date Issued:	12 March 2018
Review Date:	24 January 2021
Document Type:	Policy Level 1

Contents		**Page**
Paragraphs	Executive Summary	3
1	Introduction, Scope and Purpose, Definitions	4-5
2	Related Trust Policies	6
3	Roles and Responsibilities	6-7
4	Principals and Procedures	7-13
5	Implementation	13
6	Monitoring Compliance and Effectiveness	13-14
7	Arrangements for Review of Policy	14
8	References	14
9	Appendices	14

Appendices		**Page**
Appendix A	Staff Guidance on the Secure Transfer and Communication of Personal Data	15-18
Appendix B	Sample fax cover sheet	19
Appendix C	Staff Guidance on the Disclosure and Sharing of Personal Data	20
Appendix D	Charging scheme for requested information	22

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled.
As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

Executive Summary

Data is central to all UHS does, it enables effective treatment, supports world leading research and allow us to better plan our resources. Personal data belonging to current, past and prospective patients, current, past and prospective employees, suppliers, contractors, business partners is our most valuable asset in providing care, second only to our staff.

The Data Protection Act (2018) and the General Data Protection Regulation sets the legal framework, by which we can process personal information. It applies to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A).

This policy provides a guide to the key elements of the legal framework governing information handling outlines the responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling

Data Protection and Confidentiality Policy - Data Protection Principles

The Data Protection Act (2018) defines six Data Protection Principles; which all processors of personal information must abide by. The 6 principles are:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

1 Introduction, Scope and Purpose of this Policy

1.1 Introduction

1.1.1 The NHS cannot operate effectively if the patients we need to treat to not trust us to provide confidential and effective care. Part of this trust is being able to provide confidential information to clinicians and other staff and be confident that if will remain confidential and only be shared when necessary.

1.1.2 This document provides guidance for everyone on processing information in accordance with the principles and legal obligations outlined in the Data Protection Act (2018), General Data Protection Regulation and common law duty of confidentiality. It explains how we can comply with best practice for information handling within the NHS as described in the NHS Code of Confidentiality, Data Security and Protection Toolkit and the Caldicott Reports.
.

1.2 Scope

1.2.1 This policy provides guidance to ensure that information processed by Trust staff is handled in a safe and secure manner which complies with current legislation and best practice relating to data protection and confidentiality.

1.2.2 It will apply to all areas of the Trust and all staff who handle information. It will be of particular relevance to staff members who handle personal and sensitive information relating to both patients and staff.

1.2.3 Data Protection and Confidentiality is a component of Information Governance and as such this policy and associated procedures form part of the Trust's overall Information Governance Framework.

1.3 Purpose

1.3.1 The objectives of this policy are

- To demonstrate the ways in which we ensure that patient and staff data is handled effectively and securely
- To promote best practice and innovative use of personal information, especially to inform care and research
- To ensure that we understand our responsibilities and obligations.

1.4 Definitions

Term	Definition
Personal data	Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
Data controller:	The person (or company) who determines the purposes for which and the manner in which any personal data are, or are to be, recorded. In our case, the Data Controller is the Trust
Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person who processes data on behalf of the data controller.
Direct care	The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider. Examples include assessment, performing procedures and implementation of a care plan.
Duty of confidence	A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.
Explicit consent	A form of consent normally given orally or in writing and is where a patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.
Information governance	Information governance is a combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.
Legitimate relationship	A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.
Processing	This term covers the collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to alteration, retrieval, disclosure and destruction or disposal of the data.
Non care or secondary purpose	Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

2 Related Trust Policies

- Information Governance Policy
- Disciplinary Policy
- Policy For Use And Handling Of Patient Identifiable Data
- Informatics Security Policy
- Records Management Policy
- Freedom of Information Policy
- Data Quality Policy
- Access to Personal Records Policy and Procedure
- Still Photography and Moving Image Recording Policy
- Risk Management Policy and Procedure
- Incident Management Policy
- Incident Reporting Policy
- Management of Medical Devices Policy

3 Roles and Responsibilities

3.1 Management Responsibilities

3.1.1 As Accountable Officer the **Chief Executive** is responsible for overall leadership and management of the Trust and has the ultimate responsibility for ensuring compliance with the Data Protection Act (2018), the General Data Protection Regulation, Human Rights Act (1998) and the Common Law Duty of Confidentiality. The Chief Executive delegates aspects of her responsibility to relevant executive directors according to their organisation portfolios.

3.1.2 The **Director of Transformation** has been appointed as the Trust **Senior Information Risk Officer (SIRO)** and is also the executive lead for Informatics including information governance.

3.1.3 **The Associate Director, Corporate Affairs** is the Data Protection Officer and responsible for managing data protection issues throughout the Trust.

3.1.4 **The Director of Informatics** chairs the **Information Strategy Steering Group,** where data protection issues should be discussed and escalate to the Quality Governance Steering Group

3.1.5 Day to day responsibility for data protection and confidentiality management is the responsibility of the **Trust Information Governance Manager** who is also the Trust lead for information governance.

3.1.6 The Trust has appointed the **Director of Nursing and Organisational Development** as the Trust Caldicott Guardian with specific responsibility for the confidentiality agenda and the collection, use and sharing of patient information.

3.1.7 Divisional and care group managers are responsible for the local implementation of this policy in their areas of responsibility.

3.2 Individual Responsibilities

3.2.1 Everyone working for the NHS has a legal duty to keep information about patients and clients and other individuals such as staff or volunteers confidential. They are required to adhere to confidentiality agreements i.e. common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

3.2.2 The terms and conditions within Trust employment contracts include specific conditions relating to confidentiality as follows:

- In the course of your employment you will have access to confidential information relating to the Trust, its clients, patients, employees, other parties, as well as information relating to the Trust's policies or finances. You must not use such information for your own benefit nor disclose it to other persons without the consent of the Trust and the party concerned unless required to so by law. This applies both during and after the termination of your employment. If any member of staff is found to have revealed confidential information without consent, disciplinary action may be taken. If you are in any doubt regarding the use of information in the pursuit of your duties, you should seek advice from your manager before communicating such information to any third party. Nothing in this clause inhibits the provisions of the Public Interest Disclosure Act 1998Individual health professionals will also be subject to professional regulatory regimes which may include standards related to confidentiality and information handling.

3.2.3 All staff are responsible for ensuring they keep up to date with Information Governance training in accordance with the Trust Statutory and Mandatory training policy as this training covers relevant data protection and confidentiality requirements.

3.2.4 This requirement also applies to agency staff and contractors working at the Trust who may have access to personal information. Most agencies working with the NHS provide their staff with this training. Where this not the case local arrangements should be made to ensure the employee is adequately trained before working at the Trust.

4 Principles and Procedures

4.1 Data Protection Act 2018 and GDPR

4.1.1 The Data Protection Act (2018) (DPA) and the General Data Protection Regulation (GDPR)sets out the legal requirements and duties placed on data controllers (i.e. the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about).

4.1.2 The Trust is required to register annually with the Information Commissioner as a Data Controller. The Trust's unique registration number is **Z4989884.**

4.1.3 The DPA sets out 6 data protection principles which describe legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the 6 data protection principles is unlawful.

4.1.4 Although the Data Protection Act (2018) does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought from the data protection office dataprotection@uhs.nhs.uk

4.1.5 Under GDPR each controller of personal information must decide under what basis it is processing personal information. If there is no relevant basis, then the processing is likely to be illegal.

- Under Article 6 the Trusts basis for processing personal information is:

"the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law".

- As the Trust processes special category information – which includes health data then it must have a second basis (under Article 9), which are:
    - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

    - processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

    - processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4.2 NHS Caldicott Report

4.2.1 The Caldicott Report was published in 1997 (updated in 2013 and 2016) and focused on the protection and processing of patient identifiable information within the NHS. The reports provided the NHS with a series of principals to adhere to:

- Justify the purpose for collecting or holding patient-identifiable information
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

4.2.2 The Trust appointed Caldicott Guardian (Director of Nursing and Organisational Development) advises the Trust Board on matters of patient confidentiality and promotes the safe and secure handling of patient data. The Trust Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures.

4.3 Data Processing

4.3.1 Data processing covers the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintaining confidence between the Trust and its patients, staff and others with whom we deal.

4.3.2 The DPA requires that processing of any personal information held by the Trust must be both fair and lawful. This requires that the processing meets fair processing criteria and satisfies one or more 'conditions for processing' set out in the DPA.

4.3.3 To ensure 'fair processing' we must be lawful, fair and transparent about the way we will use the personal data we hold. We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- help people to understand their rights

4.3.4 To meet this requirement the Trust publishes a fair processing notice to inform patients about the way we handle and use their personal data. This is made available in hard copy format and published on the Trust public website.

4.3.5 Routine data processing for the purposes of patient care will normally be conducted for a purpose that satisfies one of the processing conditions in the DPA. When sharing takes place for non care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

4.3.6 A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information. A copy of the pro-forma for DPIA's is available on StaffNet

4.4 **Access to IT Systems**

4.4.1 It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

4.4.2 The Informatics Security Policy provides detailed guidance on the security of Trust IT systems including minimum standards of access controls.

4.4.3 Staff should not attempt to access or use electronic record systems they have not been trained to use or authorised to access. Existing system users should not allow others to access systems using their login credentials. Sharing system passwords is a disciplinary offence and viewed as a serious breach of Trust procedure.

4.5 Access to Records

4.5.1 The Trust holds over a million individual patient records in a variety of formats. In addition it holds personal records for present and former members of staff and others it does business with. While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

4.5.2 Many of our digital clinical systems will allow a user to access any individual record held in that system. Users should only access individual personal records for those data subjects (patients, staff etc) that they have authorisation to access for specific purposes or in the case of patient records where they have a 'legitimate relationship' with the patient.

4.5.3 **Staff have no right to access personal information held in records about their relatives or friends unless the circumstances in paragraph 4.6.2 apply**.

4.5.4 While some Trust staff are in a position to potentially access personal data held about them in Trust records (e.g. their personal medical records) this is not a facility available to members of the public. NHS policy is that NHS staff should follow the same procedure as members of the public to access their data. Therefore **Trust staff should not access their own data held in any Trust records without specific authorisation**.

4.5.5 Procedures for obtaining access to or copies of personal information held by the Trust about individuals are explained in the Access to Personal Records Policy.

4.5.6 The Trust carries out audits of access to personal data and any member of staff who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' record data may face disciplinary action.

4.6 Communicating Personal Information

4.6.1 In order to provide effective care services there is a need to transfer information between organisations and individuals. In order to comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

.

4.6.2 Any data containing identifiable information transferred by the Trust outside the Trust for processing must be securely encrypted during transit. Any transfer outside the European Economic Area must only be carried out if appropriate security controls are in place.

4.6.3 A guide to staff on the transfer or communication of personal data by post, fax, by hand and e-mail and the use of portable media is in **Appendix A.**

4.7 Disclosure and Sharing of Personal Information

Sharing Personal Information for Care Purposes

4.7.1 In order to provide safe and effective care, personal information about patients will need to be shared with all those caring for an individual. In addition to the clinical team providing care, the direct care team may include laboratory staff, social care staff, specialist care teams and administrative staff supporting the care process.

4.7.2 In accordance with both DPA2018, GDPR and Caldicott principles information shared for care purposes should be relevant, necessary and proportionate. In applying this principle care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

4.7.3 Caldicott principle 7 (Duty to share) emphasises the need to share information in certain circumstances where the duty to share information clearly outweighs the normal duty of confidentiality owed. This would be the case when there is a threat to the safety of others and the sharing of personal information about individuals (e.g. vulnerable adults or children) with the police or other agencies may prevent that threat materialising.

Sharing Personal Information for Non Care Purposes

4.7.4 Non care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using

anonymised or de identified data. This removes the need to consider consent issues. Further guidance on this topic can be found in the Trust Policy for Use and Handling of Patient Identifiable Data.

4.7.5 In certain circumstances the law requires that confidential information should be disclosed when consent may not be provided. Examples of this include a direction within a court order to disclose confidential information or the requirement to notify Public Health officials when a patient is suspected of suffering from a notifiable disease.

4.7.6 Where a legal obligation to disclose does not exist there are some limited circumstances where the sharing of personal information without consent may be justified in the 'Public Interest'. Disclosures made without consent to support the detection investigation and punishment of serious crime and to prevent abuse or serious harm to others are examples of such circumstances. Such disclosures are considered on a case by case basis and can be complex. The public good that would be met by sharing the information has to be weighed against the obligation of confidentiality owed to an individual and the public good in maintaining trust in a confidential service.

4.7.7 Further guidance on specific aspects of information sharing and disclosure is given in **Appendix C**. This guidance covers disclosures to the police, disclosure to relatives and carers, and access to information about patients for the purposes of clinical audit, service improvement and research purposes.

4.8 Disposal of Personal Information

4.8.1 It is a principle of the DPA that data should 'not be kept for longer than necessary'. To assist staff in meeting this requirement the Trust Records Management Policy provides detailed guidance to staff about the minimum retention periods applicable to Trust records and record disposal procedures.

4.8.2 The Trust reports a significant number of incidents relating to the inappropriate disposal of manual records. All printouts, reports and printed copies of records containing personal data should be kept secure at all times. This particularly applies to handover reports and documents used by staff working in ward areas.

4.8.3 Any documents containing personal data should be disposed of securely and not discarded in domestic waste and recycling bins. The Trust waste management team operate a confidential waste disposal service and provide regular collections of confidential waste from all Trust areas.

4.8.4 The disposal of items of electronic equipment which may hold personal data (PCs, laptops and any other devices with information storage capabilities) should be carried out through the Informatics department to ensure all data is effectively removed before disposal.

4.8.5 The disposal of medical devices and equipment should follow the guidance on Decommissioning and Disposal provided in the Trust Management of Medical Devices Policy.

4.9 Breach of Policy and Procedure

4.9.1 Any breach of data protection and confidentiality can have severe implications for the Trust, our patients and staff and, where significant numbers of patients are involved, can impact on the reputation of the NHS as a whole.

4.9.2 Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 constitutes a serious disciplinary offence or gross misconduct under the Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

4.9.3 The office of the Information Commissioner's Office (ICO) regulates data protection and is charged with upholding individual's information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of a financial penalty of up to £20,000,000.

4.9.4 Staff who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Trust Incident Reporting Policy.

4.9.5 .

5 Implementation

5.1 This policy will be published on Staffnet and the publication of this version will be highlighted in the IG pages of Staffnet. Annual IG training must be completed by all staff in accordance with the Trust training needs analysis for all staff groups and reference to the existence of this policy is made during face to face IG training sessions.

5.2

5.3 The Trust information leaflet for patients (Patient Confidentiality and Use of Patient Information) and the Trust Staff Code of Conduct leaflet both contain key information published in this policy.

6 Monitoring Compliance and Effectiveness

6.1 The purpose of monitoring is to provide assurance that the agreed approach is being followed – this ensures we get things right for patients, use resources well and protect our reputation. Our monitoring will therefore be proportionate, achievable and deal with specifics that can be assessed or measured.

:

What aspects of compliance with the document will be monitored	What will be reviewed to evidence this	How and how often will this be done	Detail sample size	Who will co-ordinate and report findings	Which group or report will receive findings
Breaches of procedure	Reported incidents	Quarterly review and summary report on all IG incidents	N/A	Trust Information Governance Manager	Information Governance Steering Group
Legitimate access to personal Information	Requests from users to access patient records	Quarterly as part of audit of record tracking	50 records per quarter	Health Records Operational Manager	Information Governance Steering Group
Legitimate access to personal Information	Review of privacy Notification s on NHS Portal	Monthly	N/A	Trust Information Governance Manager	Identified Breaches escalated as appropriate

Overall compliance with NHS best practice and legal requirements	Compliance with standards set in Information Governance Toolkit	Annual assessment made by IGSG	N/A	Director of Informatics (Chair of IGSG)	Quality Governance Steering Group approve assessment before submission to DofH

6.2 Where monitoring identifies deficiencies actions plans will be developed to address them.

7 Arrangements for Review of the Policy

7.1 This policy will be reviewed in three years unless a substantial change in policy or legislation takes place when an earlier review will be undertaken.

8 References

Information Commissioner Website

https://ico.org.uk/for-organisations/guide-to-data-protection/

Health and Social Care Information Centre Confidentiality Policy Section:

http://systems.hscic.gov.uk/infogov/confidentiality

9 Appendices

A. Guide to the Secure Transfer and Communication of Personal Data
B. Sample Fax Cover Sheet
C. Guide to the Disclosure and Sharing of Personal Information

Appendix A to Data Protection and Confidentiality Policy

Staff Guidance on the Secure Transfer and Communication of Personal Data

Introduction

Public sector organisations continue to report a high level of data beaches, many of which relate to the insecure transfer and inappropriate disclosure of sensitive personal information. It is therefore important that all staff are aware of best practice and guidance for the secure transfer and communication of personal data.

Guidance for staff on the use of postal services, fax and e-mail to communicate and transfer personal data is outlined in this appendix. Guidance covering manual transfers and taking personal information off site is also provided. (Further help and guidance can be obtained by contacting the Data Protection office (ext 5079).

Circumstances may arise where a transfer of personal data needs to take place but for some reason it is not possible to follow best practice and the proposed method of transfer poses a degree of risk. In these circumstances the sender must conduct a simple risk assessment and consider if the perceived need to communicate the data by the method selected outweighs the risk associated with the method of transfer. For example where there is an urgent need to communicate with another professional about a patient and no secure method of communication is available an insecure communication channel (including the minimum of personal identifiers) may be selected for use.

Post

It is acceptable to use first and second class post for routine clinical correspondence such as appointment letters and non-urgent test results. Post office 'signed for' or 'special delivery' tracking services provide an increased level of security and the selection of the appropriate service to use should be made after completing a local risk assessment.

Patient records, personal files, letters including sensitive confidential information and transfers of 'bulk data' should be sent using one of the signed for services or a recognised courier service.

While envelopes with transparent windows provide a convenient and simple way of showing the addressee details printed on letter headings, there is a recognised risk to confidentiality when these are used to send multiple letters containing personal information to a single addressee (e.g. multiple patient clinic letters sent to a single GP surgery).

To reduce the risk of an incorrect address being displayed i. these types of envelopes should only be used for transferring single letters where they include person data.

When using postal services to transfer personal information the following guidance should be followed:

- Ensure the envelope is robust enough to protect the contents and sealed correctly (do not use unsealed internal envelopes for transfers of personal information).
- Ensure the full and correct name and address of the recipient is clearly shown.
- Mark the envelope 'Private and Confidential'
- Add the senders details on the back of the envelope
- Ask external recipients to confirm safe delivery
- Do not use window envelopes for any bulk mailings

Fax

The use of Fax machines to transfer identifiable data poses some significant risks to confidentiality. The Increasing availability of secure e-mail services has reduced our reliance on Fax machines but it is recognised in some situations it is still appropriate to continue to send personal information by Fax machine.

Where the continued use of Fax is necessary the inherent risks can be minimised by following the guidance below:

- Fax machines should be located in secure areas at both ends of the transmission
- always double check the FAX number that you are sending information to
- if you are unsure about the number you are sending a FAX to, do not send the information without verifying the number with the recipient
- Use pre-programmed numbers where possible to avoid misdialling
- contact the recipient before sending to let them know you will be sending a FAX
- ask the recipient to acknowledge receiving the FAX immediately
- confidential Faxes must not be left lying around for unauthorised staff to see
- where possible send personal identifiers separately from clinical details.
- If possible just use the patient NHS number and date of birth as an identifier
- make sure the fax cover sheet is marked Private and Confidential and states who the information is for. .

A fax cover sheet that can be adopted for local use is shown at **Appendix B** to this policy.

E – Mail

NHS policy is that e-mails that that include personal data should be sent 'securely' to avoid the risk of accidental disclosure through misdirection or interception. This is best achieved by ensuring that the e-mail is encrypted during transit so that the contents cannot be read other than by the intended recipient.

E-mails sent between UHS user outlook accounts are protected from interception during transit by Trust Firewall security. The Trust therefore permits personal information to be included in e-mails sent between UHS outlook e-mail accounts.

The simplest way to comply with NHS policy and securely send personal data outside the Trust network is by using NHSmail, the NHS provided secure e-mail service available free to all NHS staff. An e-mail sent between NHSmail accounts is encrypted and remains secure during transit. As well as individual personal accounts it is possible to set up NHSmail generic accounts that can be accessed by more than one person.

If you need to send an email, containing patient information, outside of NHSmail, write [secure] at the start of the email subject (this must include the square brackets). Doing this ensures that the information is encrypted during transit. If the email account you are sending the information too is not secure, then the recipient will be asked to log into the encryption software prior to the information being released to them..

Details on how to set up an NHS e-mail account and use the new secure services are available at this link or staff may seek advice via the IT help desk.

http://systems.hscic.gov.uk/nhsmail .

When the use of NHS mail is not possible alternative methods of securing personal data in transit via e-mail should be adopted. These range from the use of a third party encryption service to provide full protection during transit to the simple use of password protection for

attached files containing the personal data being communicated. As a minimum users should consider separating the personal identifiers in a communication from the remainder of the text and sending this in a separate e-mail. The method chosen should be appropriate for the degree of risk assessed.

Use of Removable Media

Many of the most highly publicised losses of data in the public sector have involved data held on CDs and memory sticks. The risk of theft or loss of these devices is high and therefore it is essential that any identifiable data being transferred on portable devices is always encrypted.

Memory sticks should only be used for short-term storage of personal data.

Transferring Personal Information by Hand and/or Taking Information Off Site

Transferring personal information manually is often seen a quick and effective way to deliver information to another person or organisation. When transferring personal information by hand, or taking personal information off site for meetings etc, the risks from loss or theft can increase. The following points should be considered and if necessary action taken to mitigate any identified risks proportional to the amount and sensitivity of the information being transferred:

- The Medium:
    - Consider if the information can be saved on an encrypted memory stick or laptop for transit rather than transferring in a printed medium.
    - If using this method consider how you will print/download/access the information on arrival.
    - Consider if it is possible to use the Trust Remote Access application 'APPGATE' at the new location to download the information from the UHS file system securely.
- Security in Transit:
    - During the transfer maintain the security of the information by using a lockable briefcase or similar.
    - If using public transport retain the information with you at all times.
    - If travelling by car lock the information in the boot of the car during transit.
- Labelling
    - Consider how you can identify and label the material in some way so if lost/stolen and then subsequently found by a member of the public it can be identified as UHS property and safely returned.
    - Printed material can be placed in a sealed envelope and labelled as '*Property of UHSFT if found please return to….*'

- Overnight Storage
    - The need to store Personal Data overnight at home should be avoided if possible.
    - If unavoidable personal information should be stored in a lockable container which is not accessible to other persons living at the home.

Appendix B to Data Protection and Confidentiality Policy - Sample Fax cover Sheet

University Hospital Southampton NHS
NHS Foundation Trust

FAX COVER SHEET

Southampton General Hospital
Tremona Road
Southampton
SO16 6YD

Tel: 023 8081 xxxx

DATE: **TIME:**

TO:

FROM: **TEL NO:**

Number of pages including cover sheet: ☐

Message:

This fax contains personal information and is PRIVATE and CONFIDENTIAL

IF YOU DO NOT RECEIVE ALL OF THIS FAX PLEASE TELEPHONE 023 8081 xxxx

PRIVACY AND CONFIDENTIALITY NOTICE

The information contained in this facsimile is intended for the named recipients only. It may contain privileged and confidential information and if you are not an intended recipient, you must not copy or distribute it. If you have received this facsimile in error, please notify us immediately by telephone on 023 8081 xxxx. Thank you in advance for your assistance.

Appendix C to UHS Data Protection and Confidentiality Policy

Staff Guidance on the Disclosure and Sharing of Personal Data

Introduction

General guidance and advice on information sharing and disclosure is included at paragraph 4.8 of this policy. The appendix considers some common disclosure situations encountered by UHS staff and is provided to support staff to make decisions about disclosure in those situations.

Information governance policy and procedure is designed to support best practice in information handling and should not be a barrier to the sharing of personal information when necessary and appropriate. However, it is recognised that some circumstances produce complex situations which require careful consideration, and if unsure about a specific issue staff should seek guidance from line management, the Data Protection office or during non working hours the site management office.

A flowchart to follow when considering how to respond to a request to share /disclose information about a ward patient is attached at annex 1. It will cover many but not all situations staff will encounter and the principles can be applied to other areas receiving information requests.

Disclosing Information to Relatives and Carers

Ward staff will deal with numerous inquiries from relatives and friends of patients seeking information about progress and treatment. Many inquiries will be made over the telephone by people who are not registered as the patient's next of kin or carer and in these circumstances it is sometimes difficult to decide if any information should be passed on.

While in most circumstances a patient will not object to updates about their condition being given in response to an inquiry, circumstances do arise when this will not be appropriate. It is therefore good practice to establish and record on admission if the patient wishes to place any restrictions on the information provided about them to others. This will make it easier to respond appropriately to any telephone inquiries received. Where restrictions are placed on information to be provided about patients it is important all staff likely to handle inquiries are made aware of the details to avoid a breach of confidentiality.

On receipt of an inquiry from a person not known to ward staff, where practical, the consent of the patient to disclose information should be sought. Where this is not possible a disclosure decision has to be made based on the information provided by the caller justifying their 'need to know'. Sensitive and detailed information should normally only be disclosed or discussed with nominated or recognised next of kin, close relatives or carers. It may be appropriate to agree a password with the patient and the family so that it is easy to identify a family member or close relative over the phone

If suspicious about the motives of a person making an inquiry about a patient do not pass on any details but take a contact number and discuss with a senior colleague and seek advice before making contact again.

Disclosing Information to the Police

Section 29 of the Data Protection Act (1998) provides a lawful basis for the Trust to disclose personal data about a person in the absence of their consent where this will support certain aspects of law enforcement and in particular:

- the detection punishment and prevention of crime
- the identification apprehension and prosecution of offenders

Most inquiries made by the police for information using this provision will be handled by the Data Protection office or Emergency Department. Occasionally inquiries will be made direct to wards and departments and where time permits these should be discussed with the Data Protection office or in non working hours with site management before providing a response.

Occasionally urgent requests will be made asking for specific information to be provided in a short period of time. Often this is due to strict timelines imposed on the police to make decisions to charge suspects or to support urgent lines of investigation. In these circumstances decisions may have to be made quickly but staff should not be pressured into disclosing information when they feel it is not in the patient's best interest.

While the law permits disclosure in the circumstances outlined above it does not compel the trust to comply with such information requests. Each case should be considered on the individual merits of the request. Where consent to disclose information to the police is not provided or refused the Trust has to consider the duty of confidentiality owed to the data subject and the public interest in maintaining a confidential service and balance this with the wider public interest in making the requested disclosure to support law and order purposes. Striking the appropriate balance in some situations can be challenging and in these scenarios, where possible UHS staff should seek specialist advice. Any requests from the police should be forwarded to the Trust Information Governance Manager at dataprotection@uhs.nhs.uk

In addition to the police it should be noted that other agencies such as the Home office, HMRC and NHS Counter Fraud Services may request information about patients using this exemption.

Access to Information for Audit, Service Improvement and Research Purposes

Clinical Audit

Clinical audit is recognised as a necessary tool to check the care provided by the Trust meets acceptable standards and is safe and effective. Access to patient personal information (e.g. detailed medical records) without consent for the purpose of clinical audit is normally permissible. The audit should be internal to the Trust and not part of a multi site/organisation audit and the audit would normally be registered with the Trust clinical audit service. Where these criteria are not met and access to patient information is requested advice should be sought before sharing information or allowing access to patient records.

Service Improvement

Dependent on the circumstances access to patient personal information without consent for the purpose of conducting a Service Improvement project may also be permissible. The term 'service improvement' is widely used to cover a range of improvement activities and caution should be exercised to ensure the boundaries between service improvement and research activities are not blurred.

Research

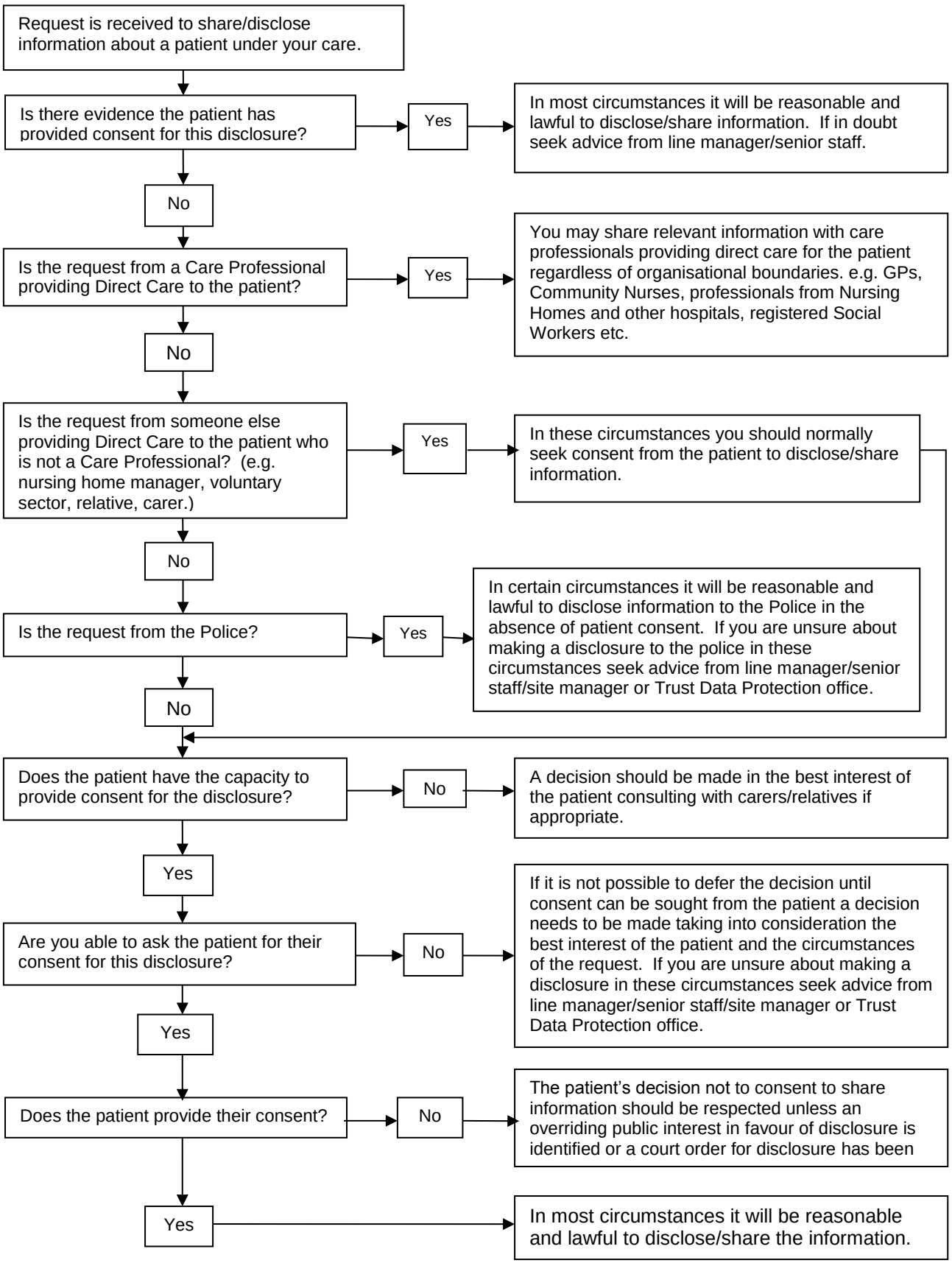
The Trust undertakes a significant amount of medical research and clinical trials. Advice on specific aspects of research governance can be provided by the Trust Research and Development (R&D) department. Most research activity requires formal ethical approval and patient consent is normally required before access to any patient personal information is provided or made. The need to obtain patient consent can be waived in some circumstances following formal application to the NHS Research Authority (NHSRA).

Sharing Information for Safeguarding Purposes

Caldicott principle 7 makes clear that in certain situations the duty to share information is as important as considerations of confidentiality. This is particularly the case in matters of safeguarding where in the past public authorities have failed individuals by not sharing information they have held which if passed on may have prevented someone harming them.

Where an individual is thought to be at risk relevant information should be shared between agencies involved with the individual if the provision of that information might reduce or eliminate the identified risk. If it is possible to obtain consent from the subject to share their data this should be done, but the absence of or a refusal to provide consent should not deter staff from sharing information where it is felt to be appropriate and justified to support a safeguarding purpose.

Annex 1 to Appendix C to UHS Data Protection and Confidentiality Policy



Data Protection and Confidentiality Policy	Version: 5
Document Monitoring Information	
Approval Committee:	Information Governance Steering Group (IGSG)
Date of Approval:	24 October 2017
Ratification Committee:	Policy Ratification Group (PRG)
Date of Ratification:	24 January 2018
Signature of ratifying Committee Group/Chair:	Amanda Lowe, Associate Director Corporate Affairs
Lead Name and Job Title of originator/author or responsible committee/individual:	Johnathan Pillinger-Cork, Trust IG Manager
Policy Monitoring (Section 6) Completion and Presentation to Approval Committee:	24 January 2018
Target audience:	All Trust staff
Key words:	Data protection, confidentiality, information governance, Caldicott, records, disclosure, information, data, processing,
Main areas affected:	Trust wide
Summary of most recent changes if applicable:	Reviewed guidance for sending patient identifiable information in windowed envelopes
Consultation:	With DGM, DDOs and IGSG
Equality Impact Assessment completion date:	13 January 2018
Number of pages:	21
Type of document:	Policy Level 1
Does this document replace or revise an existing document	Yes – Data Protection and Confidentiality Policy V4
Should this document be made available on the public website?	No
Is this document to be published in any other format?	No

The Trust strives to ensure equality of opportunity for all, both as a major employer and as a provider of health care. This document has therefore been equality impact assessed to ensure fairness and consistency for all those covered by it, regardless of their individual differences, and the results are available on request.