HPFT

Protection and Use of Service User Information (PUPI)

HPFT Policy

Version	7
Executive Lead	Executive Director – Innovation and Transformation
Lead Author	Head of Information Rights and Compliance
Approved Date	23/05/2018
Approved By	Information Management and Technology/Information Governance Programme Group
Ratified Date	23/05/2018
Ratified By	Information Management and Technology/Information Governance Programme Group
Issue Date	23/05/2018
Expiry Date	23/05/2021'IGC on 20.01.2021 agreed expiry date extension to 30.11.2021 following rapid review'
Target Audience	- Any related service which may make referrals to the Unit - All staff dealing with this Care Group

Document on a Page

Title of document	Protection and Use of Service User Information (PUPI)		
Document Type	Policy		
Ratifying Committee	Information Management and Technology/Information Governance Programme Group		
Version	**Issue Date**	**Review Date**	**Lead Author**
7	23/05/2018	23/05/2021	Head of Information Rights and Compliance
Staff need to know about this policy because	The purpose of these guidelines is to minimise the risk of an individual's confidentiality being breached. The security of service user information is the responsibility of all staff within the Trust.		
Summary of significant changes from previous version are:	GDPR update		

Contents Page

PART 1 – Preliminary Issues:

1. Summary

The purposes of these guidelines are to minimise the risk of an individual's confidentiality being breached. The security of service user information is the responsibility of all staff within the Trust. These guidelines are based on the following:

- **NHS Confidentiality Code of Practice**
  Staff should also refer to supplementary guidance to the Code – Public Interest Disclosures.

- **A Guide to Confidentiality in health and social care** – treating confidential information with respect, Health and Social Care Information Centre (HSCIC, Version 1.1 September 2013

2. Purpose

The Protection and Use of Service User Information is governed by the Data Protection Legislation and Caldicott Principles. The DPA safeguards all information which can identify a living individual, held in any format including but not limited to visual, verbal, written, electronic and microfilm. The Caldicott Principles set out seven principles to underpin the handling, transfer and protection of service user identifiable information[1]. In addition to legislation, Health/Social Care Professionals are expected to meet the requirements of their professional regulatory bodies.

NHS Digital (previously HSCIC) has statutory responsibility under the Health and Social Care Act 2012 to produce a Code of Practice for processing confidential information covering *'the practice to be followed in relation to the collection, analysis, publication and other dissemination of confidential information concerning, or connected with the provision of health services or of adult social care in England*'. Therefore health and social care bodies (or anyone working with them to provide services of care) processing confidential information in relation to the provision of publicly funded health or adult care activities, must have regard to this guide. Unless members of staff understand when they must share information with another professional and when they should not, they will not be able to provide the optimum standard of care. The main principles have been included in this policy, for the full guide click here.

3. Definitions

These definitions are used throughout this document.

i. **Health professional** - The appropriate health professional is the person who is currently or was most recently responsible for the service user's clinical care.

The definition of a health professional under Section 69 of the Act is as follows:

- A registered or provisionally registered medical practitioner
- A registered dentist
- A registered optician
- A registered pharmaceutical chemist
- A registered nurse, midwife or health visitor
- A registered chiropodist, dietician, occupational therapist, orthoptist or physiotherapist
- A clinical psychologist, child psychotherapist or speech and language therapist
- An art or music therapist employed by a health service body
- A scientist employed by such a body as head of department

ii. **Data Subject** - This is the patient/client/service user

iii. **Data Controller** - The Trust, Trust Officer or other health body holding the records.

iv. **Data Processor** - Any person having details with client information, including keeping, using and disclosing it.

v. **Personal Data** - Includes any information relating to a living individual who can be directly or indirectly identified from that data.

vi. **"Accessible" record** - all records including health records made in the public or the private sector to which the service user or client is entitled to access, and irrespective of the date upon which the record was made.

vii. **Special Categories** - Any information relating to a living individual's physical or mental health or condition, sexual life, racial or ethnic origin, political and religious beliefs, membership of a trade union, proceedings for any offence committed or alleged to have been committed, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person. The gender of a data subject is not sensitive personal data.

viii. **Medical Purposes** - Preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

ix. **Health Record** - Records consisting of information relating to the physical or mental health of the service user, made by or on behalf of a health professional in connection with the care of the data subject. Accessible, disclosable records will include process information and aide-memoir notes made as part of a clinical procedure or interview.

x. **Caldicott Guardian** - An officer of the Trust who has specific responsibility for controlling issues relating to record keeping and access. The Caldicott Guardian for Hertfordshire Partnership University NHS Foundation Trust (HPFT) is Dr Jane Padmore, Executive **Director of Quality and Safety** based at Trust Head Office, The Colonnades, Hatfield.

xi. **Third party** - Any person other than the Data Subject, the Data Controller or any authorised data processor.

4. Duties and Responsibilities

4.1 The IM&T/IG Programme Group

The IM&T/IG Programme Group is responsible for the development, implementation and review of the Trust's policy on the Protection and Use of Service User Information.

The Group works to ensure that the Trust, through its service areas, implements this policy and provides guidance on the development and review of local policies and systems.

4.2 Information Management and Technology Management Meeting

This Group acts as a sub group of the Information Management and Technology/Information Governance Programme Group. It will ensure alignments are made between IM&T and IG issues and the Trust's IM&T strategy.

4.3 Change Advisory Board

The Change Advisory Board (CAB) is an authoritative and representative group of people who are responsible for assessing, from a business and a technical viewpoint, all high impact Requests for Change (RFCs). All IM&T related change requests are reviewed by the CAB who will ensure that standardised methods and procedures are used for efficient and prompt handling of all changes, in order to minimise the impact of change related incidents upon service quality. The CAB will escalate any issues that are unable to be resolved within the Change Management process to the Senior IM&T management group where appropriate.

4.4 Management Responsibility

The Chief Executive and Senior Managers of the Trust are accountable for records management within the organisation and have a duty to make arrangements for the safekeeping of service user information.

Managers of services have a responsibility to ensure compliance within their areas, making sure issues relating to the safe keeping and sharing of service user information are discussed in supervision.

Managers are responsible for maintaining the security of care records in general and for ensuring access permissions for the Electronic Patient Record (EPR) are appropriate and upheld.

4.5 Caldicott Guardian

Additionally the Caldicott Guardian is responsible for approving and monitoring national/local guidelines and protocols on the handling, sharing and management of confidential service user information.

4.6 Individual Responsibility

Each member of staff is individually accountable for the records of service users on their caseloads.

Anyone who records, handles, stores or otherwise comes across service user information has a common law duty of confidence to people accessing Trust services. Such a duty will continue even after the death of an individual. Unless members of staff understand when they must share information with another professional and when they should not, they will not be able to provide the optimum standard of care.

5. Introduction

The purpose of these guidelines is to minimise the risk of an individual's confidentiality being breached. The security of service user information is the responsibility of all staff within the Trust. These guidelines are based on the:

- **NHS Confidentiality Code of Practice**
  Staff should also refer to supplementary guidance to the Code – Public Interest Disclosures.

- **A Guide to Confidentiality in Health and Social Care** – treating confidential information with respect, Health and Social Care Information Centre (now NHS Digital) (HSCIC, Version 1.1 September 2013).

- **Data Protection Legislation – controlling how personal information can be used and rights to ask for information about you.**

This guidance document covers the five 'confidentiality rules' outlined in the NHS Digital Guide:

Rule 1
Confidential information about service users should be treated confidentially and respectfully.

Rule 2
Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

Confidential information about an individual must not leak outside the care team but it must be shared within it in order to provide a seamless integrated service.

Rule 3
Information that is shared for the benefit of the community should be anonymised.

Rule 4
An individual's right to object to the sharing of confidential information about them should be respected.

Rule 5
Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

This NHS Digital guide also reflects the seven Caldicott Principles.

6. Information for Service Users

Members of staff have a statutory duty (Data Protection Legislation) to inform the individual's using our services that information is being held by the Trust which records details of their health or social care assessment, treatment and progress,

and that these records are identifiable (i.e. that they include their personal details). They must also be informed of their right to request access to their records.

Information should be given verbally and by providing the service user with a copy of the HPFT information leaflet, *" Protection and Use of Personal Information".* This leaflet is sent out from the Single Point of Access (SPA) team with the first appointment letter.

The leaflet can be found on TrustSpace and hard copies are available from the Information Rights and Compliance Team at 99 Waverley Road, St Albans, Herts.

A follow up discussion at the first appointment will ensure the service user has understood the information. This conversation should be recorded in the Service User's Electronic Patient Record and made 'crucial' – See Paris guide for further instructions. Due regard must be given to any special communication needs, for example, language interpretation, sign language or other communication aids. The relevant professional from the initial treating team must ensure/be aware that:

a. Data Protection Legislation specifies that using data for direct care purposes (for providing health and social care) is acceptable as long as information is clearly publicised and communicated through privacy notices and / or service leaflets
b. Information that can identify individuals must not be used or disclosed for purposes other than health/social care without the individual's *explicit* consent unless there is a robust public interest or legal justification to do so. You must have a valid lawful basis in order to process data.All individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement. Check that they have no concerns or queries about how their information is disclosed and used and respond appropriately. If the service user requests a more detailed explanation about how their information is used, staff can contact one of the named people listed in section 7.5g.
c. If a service user has concerns about information to be recorded about their care and treatment, the member of staff should explain that the Trust and individual professionals are accountable for all treatment provided and are legally and professionally bound to record details in order to maintain safe practice. If they refuse, the case should be referred to a senior manager and advice sought through the Caldicott Guardian. The NHS Confidentiality Code of Practice provides additional information.
d. If the service user agrees to information being recorded on paper, but not electronically, the member of staff should explain the benefits to improved information sharing with a member of the direct care team and reassure them of the confidentiality and access restraints applied to the system. If they continue to refuse, details should be recorded on paper and the service user referred to a Senior Manager.
e. Service users have the right to have inaccurate personal data rectified, or completed if incomplete. Such requests should be made either verbally or in writing. These requests must be responded to within one calendar month.
f. Service Users have a right to have personal data erased. This right to erasure is also known as 'the right to be forgotten'. Such requests should be made verbally

or in writing. These requests must be responded to within one calendar month. This right is not absolute and only applies in certain circumstances.

g. In an emergency or where it is not possible to give the above information at the first contact, staff must act in the service user's best interests and deal with the immediate assessment/treatment needs. The individual must be informed how their personal data is used and with whom it is shared as soon as possible.
h. Where an individual will not be able to receive the information, i.e. lacks mental capacity, a clinical note must be made in the service user's EPR.
i. If a child is not of sufficient age (13yrs under Data Protection Legislation) and/or understanding, a person with parental responsibility will normally give consent except where the interests of that person and the young person are not compatible.
j. A clinical note indicating that a conversation has taken place must be entered onto the EPR and made 'crucial' so it is easily identifiable.
k. All teams involved in the service user's care will be able to check to see if this action has recently been completed.

6.1 Use of interpreters

Everything possible must be done to overcome any barriers to communication. The use of an interpreter may be required if the service user speaks a language other than English or communicates by sign language due to a hearing disability or has additional communication needs due to a physical or learning disability. Staff must ensure that this is a standard part of planning care (starting with SPA).

The Trust policy on communicating with service users from diverse communities contains up to date information on how to arrange an interpreter (or for a translated resource) should this be needed.

7. Confidentiality and Sharing of Information

7.1 Deciding whether to share confidential information for direct care

When confidential information is shared within the care team, only information that is relevant, necessary and proportionate should be shared. Close attention must be paid when applying this test to avoid compromising care:

- There is a clear purpose, for example to help with a diagnosis.
- The purpose could only be achieved by the sharing of confidential information.
- The extent of the information sharing is kept as limited as possible, consistent with achieving the clear purpose.

The term ‘direct care’ is defined as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of an individual (all activities that directly contribute to the diagnosis, care and treatment of an individual.
GDPR sets a high standard for consent and requires offering people genuine choice and control over how you use their data. Implied consent is no longer acceptable, but GDPR specifies that using data for direct care purposes (for providing health and social care) is acceptable as long as information is clearly publicised and communicated through privacy notices and / or service leaflets.
The Department of Health has produced a guide for health and care professionals about ‘Confidentiality and information sharing for direct care’.
There is also the Information Sharing Booklet for Frontline Staff; these useful guides are available on the staff intranet and can be used to aid decisions about information sharing.
Where confidential information is stored in a way that makes it practical to separate pieces of confidential information, it is not acceptable to share all information in an individual’s care record unless the confidential information is relevant and appropriate to the individual’s care. For example, only part of a patient’s medical history may be relevant to a new referral so the rest of the medical record should not be shared unless there is a clinical reason to do so.

In circumstances where it is impossible to separate the relevant information, sharing in the interests of care is the priority. Confidentiality should not become a barrier to safe and effective care.

Individuals have different needs and values; even if something does not appear to be sensitive, it may be considered to be sensitive by the individual service user. It is likely that individuals will regard matters relating to their mental and sexual health as particularly sensitive.

Where it is clearly beneficial to share information for direct care, rules about confidentiality and privacy still apply; only those who have a clear ‘need to know’ should have access to the relevant confidential information. The Trust has partnership arrangements with other agencies in order to provide the best possible care package for an individual. The service user must be informed if their personal information is being passed between HPFT and a partner organisation. You can refer to a list of sharing agreements in place below.

Sharing Protocols (under review)

Note: It is important to remember that this guidance relates only to obtaining informed service user consent for the recording of health or social care information. The need to obtain informed written consent for some healthcare treatments and procedures continues and is a separate issue.

7.2 Sharing Information with Service Users

Service users, subject to certain safeguards, have a right to access their personal records under Data Protection legislation. This should be at the forefront of the minds of those recording notes and administering care. Safe and effective care is dependent upon relevant confidential information being shared amongst all those

involved in caring for an individual. Individuals must be informed about who will see their confidential information.

It is good practice for health and social care staff to share information and records with service users during the course of the treatment/care episode. They should be encouraged during care/treatment sessions to read and contribute to the recording of their records except when the welfare of the service user or other people would be seriously harmed by the sharing of such records. Where records are shared, a clinical note should be made in the EPR to record this.

Where copies of records are provided to the service user, e.g. care plan or risk assessment, they should be clearly watermarked "service user copy".

For formal access requests by service users or their representatives, refer to the Formal Access to Records Policy and Procedure available on the staff intranet.

7.3 Service Users' Correspondence

All letters concerning NHS service users written to another health or social care professional should be copied to the service user if she/he wishes to receive the letter unless there are circumstances where it may be impracticable, unlawful or undesirable to do so. Further guidance is given in Appendix 2.

7.4 Sharing information with carers, relatives or advocates

Service users may also choose whether to share confidential information with a carer or family member.

Professionals should discuss with the service user what information they wish to be shared, with whom and in what circumstances.

Confidential information should be shared with their carer when the service user has given explicit consent and when the carer consents to being told.

In most circumstances, information should not be given to carers, relatives or advocates without the consent of the service user. Where the service user does not have capacity to give valid consent, confidential information should be shared with the carer where it is in the service user's best interests.
If they do not have the capacity to consent, there must be a case by case decision based on the service user's best interests and where available, previously expressed wishes[2].

[2] Please refer to the MCA Code of Practice and the Hertfordshire Mental Capacity Act policy for further information. Both documents are available from the HPFT staff intranet together with the Mental Capacity Act Assessment of Capacity and the Mental Capacity Act best interest decision pathway.

Staff may also find useful the Royal College of Psychiatry guide on Carers and Confidentiality in Mental Health.

7.5 Sharing information with others

a) Disclosure is on a need to know basis as set out in the Caldicott Principles. The person making the request must provide evidence of who they are and the reason for requesting the information.

b) Health and social care professionals involved in a service user's treatment who share health and social care information must do so in strict professional confidence. The person receiving the information must ensure confidentiality is maintained at all times.

Other direct care providers working through contracts or service level agreements from non-Trust services must also meet this requirement. There is an important obligation on the Trust to ensure that recipients can demonstrate they can be trusted to handle confidential information in accordance with the confidentiality rules.

Carrying out a Data Protection Impact Assessment (DPIA) and developing a sharing agreement will provide assurance. *Please refer to the DPIA Policy for further guidance.*

c) Student nurses, student Allied Health Professionals (AHPs) and trainees working with people using Trust services have the same requirements to maintain confidentiality as Trust staff.

Students who wish to use information for their studies gained from working with service users, must ensure that it does not contain information that can identify individuals. *Please refer to the Guidance on Anonymisation for further details.*

It is important to consider the appropriateness of sharing information with student nurses and student AHPs in relation to a safeguarding adult or child protection procedure. The Safeguarding Team or Named Nurse – Safeguarding Children should be consulted in these circumstances.

d) The interpreting services used by the Trust have a confidentiality clause within their contracts of employment. Additionally the interpreter is contractually bound to notify the Trust if they have prior knowledge of the service user outside of their interpreting role. In this situation both parties must agree to and be comfortable with the arrangement.

e) Access requests made by external health/social care professionals should be made directly to the HPFT Health Care Professional concerned who should seek official identification or check identity by calling them back through a

switchboard or reception or using an independent source for the phone number.

f) Telephone requests should be confirmed in writing unless there are exceptional circumstances which necessitate a speedy response.

(g) The identity of staff members requesting access to records or information must be double-checked. If in doubt seek advice from the Designated Data Protection Officer e.g. Head of Information Rights and Compliance or the Caldicott Guardian.

8. Consent

a. When an individual agrees to being treated by the wider care team it creates a direct care relationship between the individual and the professional, as well as their team. It is not necessary to seek a service user's specific consent each time that information needs to be passed on for a particular health/social care purpose, provided individuals have been fully informed of the potential uses of personal information. For further information refer to section 4 of this policy.

b. Consent must be gained before information is passed to a third party including a relative or friend. Consent must also be gained before service user information is used for a purpose outside of their direct care (ie research/training) and the option to withdraw that consent at any time must be available.

c. Advice must be sought within the clinical and management team where a person's capacity to consent is in question.

9. A service user's right to object to the sharing of confidential information about them should be respected. Right to Erasure.

a. Individuals have a right to object to confidential information about them being used or shared beyond their treatment and care and to have that right respected.

In all cases, objection should be considered consistently and individuals should receive an explanation of the likely consequences of their decisions to aid an informed decision.

The process for considering objections should explicitly include:

- the most senior registered and regulated health and social care professional caring for that individual;

- consideration must be given as to whether or not supporting the objection will damage effectiveness of care;

- whether there is a demonstrable risk that the safety of the service user will be reduced by not upholding the objection; and

- whether there are compelling legitimate grounds relating to the individual's situation.

To ensure objections are considered consistently, the Trust should review the criteria for assessing objections on an ongoing basis.

Any decision to disclose confidential information about service users for any reason should be fully documented in a case note on the EPR. The relevant facts should be recorded, along with the reasons for the decision and the identity of all those involved in the decision-making.

Where an objection to the sharing of confidential information is implemented, anonymised information can be shared.

Please refer to the Anonymisation Guidance for further information.

Where the likely consequences of an objection pose such a significant risk that the objection is lawfully overruled, individuals should receive an explanation, and e.g. when the law says there is an obligation to share the confidential information for notifiable diseases[3].

b. Individuals have the right to have personal data erased. This is known as the 'right to be forgotten' The right is not absolute and only applies in certain circumstances.
- Individuals can make a request verbally or in writing
- The request must be responded to within one month

Please refer to the Formal Access to Service User Records Policy for further information

10. Access to Care Records during Investigations, Inquiries and the Investigation of Complaints

a) The following may require access to care records[4]:

- Head of Safer Care and Standards

[3] Public Health (Control of Disease) Act 1984 and amendments. See in particular the 'Health Protection (Notification) Regulations 2010 (SI 2010/659)

[4] Please also see Child Protection and Vulnerable Adults Procedures for investigations relating specifically to these areas.

- Complaints Manager
- Legal Services Lead
- Independent Review Tribunals
- Investigating Officers
- Independent Persons under the Children Act and members of Public Inquiries
- Information Rights and Compliance Team

b) Where the Trust is investigating a complaint or holding an internal inquiry, access to service user information will be dependent upon the terms of reference of the inquiry. When a service user is making a complaint about aspects of their own clinical care they should have a reasonable expectation that their data will be processed in order to facilitate an investigation.. However, the service user will be informed that their clinical record will be reviewed and relevant issues discussed with staff involved for the purpose of the complaint and investigation.

If the complaint is from a third party, consent is always obtained from the service user or a best interest decision made by the clinical team if the service user lacks capacity.

The Complaints Team require access to high level data to find out which team an individual is seeing.

c) Where the Trust is co-operating with a public inquiry, access to service user information is dependent upon the terms of reference under which the inquiry acts. Where possible, the consent of the service user must be obtained.

11. The use of information in Clinical Audit or Research

a) The process of clinical audit or research may involve the inspection of care records.

b) Any documentation resulting from audit/research must protect the service user's identity.

c) When relying on consent for non-direct care purposes you must –

Name the Trust and any third parties who will be relying on consent

Allow Withdrawal: Tell people they have the right to withdraw their consent at any time, and how to do this. There must be simple and effective withdrawal mechanisms in place

Document: Keep records to demonstrate what the individual has consented to including what they were told and when and how they consented.

d) When access is required to care records for research purposes, a letter of request should be made by the Lead Professional to the Research and Ethics Committee.

e) The Caldicott Guardian and Clinical Audit Manager will carry out an annual review of the audits planned for the year to consider whether or not to allow access to service users' records.

f) The care records or other documents relating to care or treatment must be available at all times. Where possible, they should be scrutinised in situ and not removed. The location of the records must be known at all times by the care team. Any paper records e.g. the historical paper record prior to the use of the EPR, must be logged on the EPR.

g) Where archived paper records are used, they must be returned for archiving as soon as possible.

h) Discussion of any data will only take place in a setting which does not compromise confidentially.

i) Minutes of meetings to discuss the result of audit will not contain service user identifiable information.

j) All data collection forms which hold identifiable personal information must be shredded at the completion of the audit/research.

12. Disclosure to the Media

a) Any media enquiry received relating to an incident should be referred immediately to the Communications Marketing Department.

b) Staff should not answer any enquiry themselves but inform the Communications Team of the name and contact number of the person making the enquiry.

c) Any press statement will be issued by the Communications Team in liaison with the Managing Director or Senior Manager.

d) If staff become aware that the service user or family have or may contact the media, staff should inform Communications Team immediately.

For further information, please refer to 'Dealing with the Media' guidance on TrustSpace.

13. Legal Access

Any document which records any aspect of a service user's care can be required as evidence before a Court of Law or before any of the regulatory bodies for health or social care professionals. For specific information refer to Appendix 3. If in doubt advice should be taken from the Legal Service Lead based at 99 Waverley Road.

14. Exceptions to the Requirement for Consent to Disclosure5

a) The requirement for the individual's consent to disclosure will not apply if the duty of care to the individual or the public interest makes disclosure essential for example:

- Notifiable infectious diseases
- Poisoning and serious accidents/incidents in the work place
- The information is required by statute or court order
- The information is required by the Coroner
- There is a serious risk of harm to the individual
- There is a serious public health risk or a serious risk of harm to others
- The information is required for the prevention, detection or prosecution of serious crime within the Crime and Disorder Act 1998
- A child protection investigation is being carried out or the child is on the child protection register, and disclosure is necessary to assess the risk to the child or to promote the effective protection of the child
- The child is looked after, and the sharing of information with carers is necessary to ensure the best possible care for the child

b) Each case must be considered on its merits. Wherever possible, the issue of disclosure should be discussed with the individual concerned and consent sought. This will not be possible in certain circumstances, e.g. where the likelihood of a violent response is significant or where informing a potential suspect in a criminal investigation might allow them to evade custody, destroy evidence or disrupt an investigation.

In these situations advice should be sought from the Caldicott Guardian, Data Protection Officer, legal or other special advice may be required.

c) Where Child Protection is an issue, the overriding principle is to ensure the safety of the child.

For further information, please refer to the Hertfordshire Safeguarding Children Board Child Protection Procedures or the Trust Policy for Managing Risks Associated with Safeguarding Children and Child Protection, both of which are available on the staff intranet. Additionally, you can contact the Head of Social Work and Safeguarding at 99 Waverley Road, St Albans, Herts.

[5] Please also see Child Protection and Vulnerable Adults Procedures.

15. Maintaining the Security of Service User Records

These standards apply whether the care records are on Trust premises or being used in non-Trust establishments.

The unauthorised passing on of service user information by staff employed by the Trust is a serious matter and may result in disciplinary action within the Trust and legal action by others. Care must be taken to ensure that unintentional breaches of confidence do not occur.

Staff and service users/carers must know who to contact if anything suspicious or worrying is noted. In this first instance this should be direct Manager/Team Leader/Service Line Lead.

a) Discussions between staff regarding service users should only be for professional reasons only on a need-to-know basis..

b) Care must be taken that conversations relating to service users, including those on the telephone are carried out in appropriate and confidential environments..

c) Any confidential documentation relating to service user recordsmust not be left unattended. Computer screens should be locked when unattended.

d) Service User identifiable data should not be left on answer phones or voice mails.

e) Wall boards or charts with service user information should only be used for administrative purposes and if feasible and safe, only the initials of the service user should be used. The boards should not be in the public domain i.e. visible to service users or the public.

f) Current records should be kept within a system that excludes 'unauthorised access and breaches of confidentiality'. Records, therefore, should be kept in a place (PC, room, cupboard, filing cabinet), which can be locked at times when the area is unsupervised. Passwords/keys must be kept securely and only be available to designated staff.

g) Services should work towards the storage of paper records in a locked fire proof storage cabinet.

h) Paper records should only be accessed by designated staff following correct security procedures.

i) Where records are transported in staff cars they must be placed in a locked boot and out of sight of the public. Records containing service user information should not be left in cars overnight. If records are to be kept in the

home this must be with the approval of the line manager and completion of appropriate confidentiality agreement.

The Trust Transport Department has a specific procedure for the carriage of confidential written material

j) For further information on physical storage refer to the Care Records Management Policy and the Trust's Archiving Procedure. These documents are available on TrustSpace.

k) Where service user held records are in use, the service user must be encouraged to ensure their safety and security and the records must be returned to the NHS Trust for storage at the close of an episode of care.

l) The movement of paper records must be tracked on the EPR.

m) Computer passwords must remain secure and the standards in the Information Security Policy must be followed.

15.1 Fax machines

In order to ensure service users' information is secure at all times, the Trust has phased out the use of fax machines, as directed by NHS England.

15.2 Electronic mail

a) Pagers/text messages must not be used to convey service user information unless the service user has consented to this service. This consent must be documented on the EPR. However, any text messages that are received *from* a service user must be recorded as a clinical note if deemed clinically appropriate.

b) E-mail is a secure method of communication within the Trust and can be used for the routine exchange of service user identifiable information. It cannot be used to exchange service user identifiable information outside the Trust unless the E-mail is sent to a secure address or encrypted by the Trusts recommended method.

All staff must comply with the Policy for use of Email, Internet and Intranet.

All unauthorised transmission of bulk *(more than 5 records)* service user identifiable data via email is prohibited. Anyone that needs to send bulk patient identifiable data via email will need to seek authorisation from the Caldicott Guardian and Data Protection Officer/Head of Information Rights and Compliance for more information.

15.3 Reporting Data loss/Breaches (Datix)()

All staff are required to report any lost or stolen IT equipment (laptop, iPad, PC, memory stick, phone or any other media storage device) to their line manager immediately. Any data loss should be reported as a Data Breach on Datix. Either of

the above must be reported within 24 HOURS of the incident occurring OR the date of knowledge staff member reports incident on Datix . *Please refer to the Information Security Policy and the Incident and Serious Incidents Requiring Investigation Reporting Policyfor further details.*

In the event that confidential information about an individual is inappropriately disclosed, the individual should receive an explanation and apology from the team responsible.

16. Summary of the Data Protection Legislation

The following six principles apply.
Article 5 of the GDPR requires that personal data shall be -

The following six principles apply:-

1. Processed lawfully, fairly and in a transparent manner in relation to individuals

2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

6. . Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

17. Caldicott Principles

The Caldicott Principles underpin the handling, transfer and protection of service user identifiable information:-

1. Justify the purpose.
2. Only use the service user identity when absolutely necessary.
3. Use the minimum service user identifiable information necessary.
4. Access to patient/client identifiable information should be on a strict need to know basis for the purposes set out in section 7 and 8 of the Management of Care Records Policy.
5. Everyone who uses service user identifiable information should be aware of their responsibilities.
6. Every use of service user identifiable information must be lawful.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their service users within the framework set out by these principles.

Each Trust has appointed a Caldicott Guardian, who is an officer of the Trust with specific responsibility for controlling issues relating to record keeping and access. The Caldicott Guardian for HPFT is:

Dr Jane Padmore
Trust Head Office
The Colonnades
Beaconsfield Close
Hatfield
Hertfordshire
AL10 8YE

18. Training and Awareness

Training is provided for staff by the IM&T/IG Programme Group via e learning or at a face to face session

Care Records and Confidentiality Awareness

This programme is mandatory for all managers and clinicians. The following subjects are covered:

- Confidentiality – Why is it important in the NHS?
- DPA Access to Records Act 1990
- Caldicott Principles
- Human Rights Act 2000
- Common Law Duty of Confidence
- Types of Consent
- Capacity to Consent
- Criteria for Sharing Personal Information
- Privacy Impact Assessments

- Importance of record keeping

Information Governance / Data Security

Each year all HPFT, bank and agency staff are required to complete the mandatory IG/Data Security training. The training covers the following topics:

- Overarching information governance standards
- The NHS Operating Framework
- Confidentiality
- Disclosing Information
- Patient Welfare
- Caldicott Guardian/Information Governance Lead
- The Caldicott Principles
- The NHS Care Records Guarantee
- The NHS Constitution
- Data Protection Legislation
- The Freedom of Information Act 2000
- Records Management and Information Quality
- Information Security
- Data Security Breaches

Training Courses:

Course	For	Renewal Period	Delivery Mode
Care Records and Confidentiality	All Managers and Clinicians	Every 3 years	E learning
Data Security Awareness	All Staff	Annually	E learning or face to face

19. Embedding a culture of equality and respect

The Trust promotes fairness and respect in relation to the treatment, care and support of service users, carers and staff.

Respect means ensuring that the particular needs of 'protected groups' are upheld at all times and individually assessed on entry to the service. This includes the needs of people based on their age, disability, ethnicity, gender, gender reassignment status, relationship status, religion or belief, sexual orientation and in some instances, pregnancy and maternity.

Working in this way builds a culture where service users can flourish and be fully involved in their care and where staff and carers receive appropriate support. Where discrimination, inappropriate behaviour or some other barrier occurs, the Trust expects the full cooperation of staff in addressing and recording these issues through appropriate Trust processes.

Access to and provision of services must therefore take full account of needs relating to all protected groups listed above and care and support for service users, carers and staff should be planned that takes into account individual needs. Where staff need further information regarding these groups, they should speak to their manager or a member of the Trust Inclusion & Engagement team.

Where service users and carers experience barriers to accessing services, the Trust is required to take appropriate remedial action.

Service user, carer and/or staff access needs (including disability)	
Involvement	
Relationships & Sexual Orientation	
Culture & Ethnicity	
Spirituality	
Age	
Gender & Gender Reassignment	
Advancing equality of opportunity	

20. Process for monitoring compliance with this document

Action:	Lead	Method	Frequency	Report to:
Check policies for compliance with the general requirements of this policy	Head of Information Rights and Compliance	Review policy against legislation and national guidance	Annual	
Monitor staff understanding of confidentiality and information governance issues through compliance with IG/Data Security training	Head of Information Rights and Compliance	IG/Data Security Training. Any concerns will be raised at the IM&T/IG Programme Group	Supervision meetings	

Part 3 – Document Control & Standards Information

21. Version Control

Version	Date of Issue	Author	Status	Comment
V1, Draft 1 18 January 2007	Protection and Use of Service User Information has been separated from 'main' care records policy to form a smaller policy document.	Records and FOI Act Manager		
V1, Draft 2 17 April 2007	Sentence added to e) pg 5 – contact details should individuals require a more detailed explanation about how their information might be used.	Records and FOI Act Manager		
V1, 10 May 2007	Appendix 4 added – Procedure for Disclosing Confidential Information to the Police	Records and FOI Act Manger		
V1.1 (minor amendment) 29 July 2008	A sentence added to 5.1 to highlight: • Managers must alert the Communication Department if their safe haven fax number changes. • Guidelines separate to this policy have been sent to all teams to display above the fax machine. • A list of the safe haven fax numbers is	Head of Records and Access to Information		

	available on the intranet.			
V2.1 10 November 2008	Annual update Add the following sections: • Duties • Training • Consultation, Approval and Ratification • Dissemination	Head of Records and Access to Information		
V2.2 11 November 2008	Made changes to policy after comments from: • Pamela Crosby to ensure compliance with NHSLA • Lorraine Wiener to make sure references to Child Protection documents are correct	Head of Records and Access to Information		
V2.3 10 December 2008	Clarification required for section 4. a, b. and h	Safeguarding Adults Manager		
V2.4 7 January 2009 V3, draft 1 Feb 2010	Updated 2.4 to cover individual responsibility relating data loss. Annual update	Nicola Whiter, Head of Records and Access to Information Head of Records and Access to Information		
V3.1 3 August 2010	Updated 7.2 (Electronic email) to include unauthorised transmission of bulk data. Updated list of relevant	Records and Access to Information Officer		

	policies to include Information Security Policy and Information Risk Policy			
V4 1st May 2011	Due for annual review	Head of Records and Access to Information		
V5, 18th March 2014	Updates made due to new guidance issued by HSCIC	Head of Information Management and Compliance		
V6 9th February 2014	Annual update. Added 4.0 IM&T Management Meeting responsibilities and CAB.	Senior Information Governance Analyst		
V7 April 2018	Full Review in line with Data Protection Legislation changes	Senior Information Governance Officer		

21. Archiving Arrangements

All policy documents when no longer in use must be retained for a period of 10 years from the date the document is superseded as set out in the Trust Business and Corporate (Non-Health) Records Retention Schedule available on the Trust Intranet

All expired & superseded documents are retained & archived and are accessible through the Safer Care and Standards Facilitator Policies@hpft.nhs.uk
All current Policies can be found on the Trust Policy Website via the Orange Button.

22. Associated Documents

This policy is part of the Trust's Records Management Policy set. The following documents must also be referred to:

Information Governance Policies, Procedures and Guidance
Care Records Management Policy
Corporate Records Management Policy

DPA Policy
Data Quality Policy
Email, Internet and Intranet Policy
Formal Access of Service User Records
Freedom of Information Act Policy
Information Security Policy
Management Guidelines on the FOI Exemptions
Paris Training Manual
Policy and Procedure on the Protection and Use of Service User Information
Single Equalities Scheme
Information Risk Policy

All policies are available on the staff intranet.

23. Supporting References

A guide to Confidentiality in Health and Social Care, Health and Social Care Information Centre (hscic), version 1.1, September 2013

DH: Confidentiality NHS Code of Practice 2003DH; Records Management NHS Code of Practice 2008
Confidentiality NHS Code or Practice Supplementary Guidance

DH: Health Service Circular 1999/012

Report of the Caldicott^2 Review – Information: To Share or not to Share? The Information Governance Review

Nice Clinical Guideline 138: patients must be treated with dignity and respect

NHS Constitution Rights and Pledges

Information Sharing Booklet for Frontline Staff

Confidentiality and Information Sharing for Direct Care

24. Consultation

Information Rights and Compliance Team

Practice Governance
Head of Social Work and Safeguarding
Complaints and Service Experience Manager
Communications and Marketing Manager
IM&T Manager's Meeting
Lead, Research and Development Department
IM&T/IG Programme Group

Part 4 Appendices

Appendices

Appendix 1 – Index of Confidentiality decisions in Practice

Appendix 2 – Guidance on copying letters to service users

Appendix 3 - Requests from the Police for Confidential Information about Service Users, Adults and Children

Appendix 1 - Index of Confidentiality decisions in Practice

This section provides examples of confidentiality decisions in practice, illustrating how the approach described in the previous section can be used to guide decision-makers.

This information is from the Department of Health document "Confidentiality NHS Code of Practice, November 2003. This is available on dh.gov.uk.

Model B1 – Disclosures to support or audit healthcare

1. Disclosures to NHS staff involved in the provision of healthcare

2. Disclosures to social workers or other staff of non-NHS agencies involved in the provision of healthcare

3. Disclosures to clinical auditors

4. Disclosures to parents and guardians

5. Disclosures to carers without parental responsibility

Model B2 – Disclosures for other medical purposes

6. Disclosure to researchers

7. Disclosure to NHS Managers and/or the Department of Health, e.g. commissioning, prescribing advisers, financial audit, resource allocation etc.

8. Disclosures to Occupational Health Practitioners

9. Disclosures to bodies with statutory investigative powers – GMC, Audit Commission, the Health Service Ombudsman, CQC

10. Disclosures to NHS Complaints Committees

11. Disclosure to cancer registries

Model B3 – Disclosures for non-medical purposes

12. Disclosure to hospital chaplains

13. Disclosure to non-statutory investigations

14. Disclosure to government departments

15. Disclosure to the police

16. Disclosure required by a court, including a coroner's court, tribunals and inquiries

17. Disclosure to Sure Start Teams

18. Disclosure to the media

19. Disclosure to solicitors

Model B1: Healthcare Purposes	
1) To NHS staff involved in the provision of healthcare	Where information has to be shared widely to provide healthcare, additional efforts to ensure that service users are effectively informed should be made.
2) To social workers or other non-NHS staff involved in the provision of healthcare	The test of what would satisfy the requirement to effectively inform (B1.3) should be more demanding than where disclosure is limited to NHS staff as the breadth of the information disclosure is not as obvious to service users and their consent cannot be assumed. Disclosure may lead to confidential information being held outside the NHS in the records of partner organisations. Service users need to be made aware of this and partner organisations also need to be aware that holding health records imposes particular duties and obligations.
3) To clinical auditors	Model B1 applies to internal clinical auditors i.e. within a NHS organisation; B2 to auditors working for a different organisation (even if within the NHS). The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services, is an essential component of modern healthcare provision. Every effort should be made to ensure that patients are aware that audit takes place and that it is essential if the quality of care they receive is to be monitored and improved.
4) To parents, i.e. those with parental responsibility for patients, and guardians	Young people aged 16 or 17 are presumed to be competent for the purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults. Children under 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected. Detailed guidance can be found in Seeking Consent: Working with Children at http://www.doh.gov.uk/consent/ The key issue here is the 'competence' of the child. If the child is competent, their consent is required to disclose and use information. Staff should encourage children to involve parents, particularly where significant decisions need to be made, but should respect the choice made. However, where a child has

	refused to consent to treatment for a life threatening condition, staff should inform parents and seek their consent (consent for treatment purposes may be given by parents even where a child objects).
Model B1: Healthcare Purposes	
5) To carers without parental responsibility	Carers often provide valuable healthcare and, subject to complying with the best practice outlined, every effort should be made to support and facilitate their work. Only information essential to a service user's care should be disclosed and service users should be made aware that this is the case. However, the explicit consent of a competent service user is needed before disclosing information to a carer. The best interests of a service user who is not competent to consent may warrant disclosure.

Model B2: Medical purposes other than healthcare	
6) To researchers	The use of anonymised data is preferable for research purposes. Where systems that are capable of providing anonymised data sets for researchers do not yet exist, the use of identifiable service user information to support research may well be appropriate and necessary but normally requires explicit service user consent. Whilst service users are generally aware and supportive of research, it is not reasonable to assume that they are aware of and consent to each and every research subject or proposal. All research in the NHS or other research involving NHS patients, their tissue and/or data must meet appropriate standards of research governance, including ethical approval from an appropriate ethics committee – a mandatory requirement for all NHS supported research. If a service user cannot be contacted to obtain consent, it should not be assumed that their medical details can be used for research purposes. In some exceptional circumstances, where the research subject is of such significance or a service user cannot be located in order to seek consent, the public interest may justify disclosure. Where explicit consent has not been gained and the public interest does not justify breaching service user confidentiality, the research project needs support under section 60 of the Health and Social Care Act 2001. The Patient Information Advisory Group (PIAG) Secretariat can help clarify uncertain cases.

7) To NHS managers and the Department of Health, e.g. commissioning, prescribing advisors, financial audit, resource allocation etc.	The use of anonymised data is preferable for management purposes but this is not always practicable. Systems that are capable of providing anonymised data sets for management purposes should be developed. Where they do not yet exist, the use of confidential information to support these activities may well be appropriate and necessary, but care should be taken to determine the minimum requirements. Explicit consent is required unless there is (rarely) a robust public interest justification and, in the absence of either, support is required under section 60 of the Health and Social Care Act 2001.
8) To Occupational Health professionals	Staff may be referred to an Occupational Health department, e.g. as a result of sickness absence or a perceived failure to meet work targets. This could in turn require disclosure of service user information. Explicit consent should be obtained before disclosing. When clinicians are themselves "the service user" the powers of professional regulatory bodies to require disclosure of their health records may apply. See section 10) below.
9) To bodies with statutory investigative powers – GMC, Audit Commission, The Health Service Ombudsman, CQC	GMC assessors are entitled to access confidential patient health records under the powers given to them by virtue of the Medical Act 1983 (as amended by other legislation such as the Professional Performance Act 1995 and the Medical Act Amendment Order 2000). Similarly, the Audit Commission Act 1998 provides auditors appointed under that Act with the powers to access health records and, where necessary, service user-identifiable information to further their investigations. It is for Audit Commission auditors and GMC assessors to decide what level of information is necessary for them to fulfill their functions, e.g. access to a complete record containing service user-identifiable information, selected parts or just anonymised information. If staff have concerns about the level of information requested, good practice would be to seek and document the reasons why this is needed. Service users should be informed that disclosure has been required. The Health Service Ombudsman has the same powers as the Courts to disclose information but see their work as falling under "medical purposes." Any request for information from them should be complied with without the necessity of obtaining a court order.

10) To NHS Complaints Committees	It is unlikely to be practicable for complaints committees to undertake their work without access to relevant parts of a complainant's medical record, and anonymisation is not practicable. The use of identifiable information is therefore necessary and appropriate. However, the explicit consent of the complainant, and any other patients whose records may need to be reviewed, is required prior to disclosure. It may be necessary to explain to a complainant that their complaint cannot be progressed if they refuse to authorise disclosure. In some circumstances, where the trust of patients in NHS care or patients may be at risk, the public interest may justify disclosure to complaints committees.
11) To Cancer Registries	The United Kingdom Association of Cancer Registries (UKACR) is a "generic" organisation working on behalf of a number of different registries which all serve a common purpose: • monitoring trends in cancer incidence; • evaluating the effectiveness of cancer prevention and screening program; • evaluating the quality and outcomes of cancer care; • evaluating the impact of environmental and social factors on cancer risk; • supporting investigations into the cause of cancer; • providing information in support of cancer counseling services for individuals and families at higher risk of developing cancer. UKACR has been granted temporary support under Section 60 of the Health and Social Care Act 2001 to obtain patient identifiable information for use on cancer registry database, without the consent of patients.

Model B3: Non-medical purposes	
12) To hospital chaplains	Spiritual care cannot be practicably provided without access to some confidential service user information and this form of care is strongly desired by a proportion of service users. It therefore meets the tests of necessity and appropriateness. However, the explicit consent of service users is required before confidential information is disclosed to chaplains. Where a service user is not competent to consent to disclosure, e.g. due to unconsciousness, the decision rests with those responsible for the provision of care acting in the best interests of the service user. The views of family members about what the service user would have wanted should be given considerable weight in these circumstances.
13) To non-statutory investigations, e.g. Members of Parliament	If an investigation is appropriately authorised, disclosure will meet tests of necessity and appropriateness. The minimum necessary information should be disclosed. There is a balance to be drawn between ensuring that a service user has understood and properly consented to a disclosure of information and needlessly obstructing an investigation. Careful consideration of any written authorisation and prompt action are key, e.g. where an MP states, in writing, that s/he has a service users consent for disclosure this may be accepted without further resort to the patient.
14) To government departments (excluding the Department of Health which requires information for medical purposes – see B2)	Government departments require a range of information to carry out their functions. There needs to be a statutory gateway to permit desired information disclosure and government departments should ensure that tests of appropriateness and necessity are satisfied.

Model B3: Non-medical purposes	
15) To the police	Whilst the police have no general right of access to health records, there are a number of statutes which require disclosure to them and some that permit disclosure. These have the effect of making disclosure a legitimate function in the circumstances they cover. In the absence of a requirement to disclose, there must be either explicit service user consent or a robust public interest justification. What is or isn't in the public interest is ultimately decided by the Courts. Where disclosure is justified, it should be limited to the minimum necessary to meet the need and service users should be informed of the disclosure unless it would defeat the purpose of the investigation, allow a potential criminal to escape or put staff or others at risk. Serious crime is defined by the GMC as "a crime that puts someone at risk of death or serious harm and would usually be crimes against the person, such as the abuse of children. (GMC guidance, "Confidentiality, Protecting and Providing Information", 2002, paragraph 37).
16) To the courts, including a coroner's court, tribunals and enquiries	The courts, some tribunals and persons appointed to hold enquiries have legal powers to require disclosure of confidential service user information. Care needs to be taken to limit disclosure strictly in terms of the relevant order, the precise information requested to the specified bodies and no others. It is permitted to make ethical objections known to a judge or presiding officer, but unless the order is changed compliance is necessary.
17) To Sure Start Teams	Sure Start aims to both provide new services and to reshape and add value to existing services in order to improve the life chances of young children. It is delivered through local partnerships involving local service providers from health, education, social services and other public services, the voluntary sector and local service users and community representatives. Some of Sure Start's activities are healthcare provision, but others are not. NHS bodies have a statutory gateway to support disclosure to Sure Start teams under the NHS Act 1977 where this supports healthcare. Disclosure to a health professional within a Sure Start team to directly and only support healthcare is covered by Model B1. However, where disclosure is also for non-medical purposes (e.g. educational support), it is covered by Model B3 and explicit service user consent is necessary. If confidential service user health information is to be held within the records of partner organisations, parents need to be made

	aware of this prior to any disclosure. Receiving organisations also need to be aware that holding health information imposes particular duties and obligations with regard to confidentiality.

Model B3: Non-medical purposes	
18) To the media	Under normal circumstances, there is no basis for disclosure of confidential and identifiable information to the media. There will be occasions however when NHS organisations and staff are asked for information about individual service users. Examples include: • Requests for updates on the condition of particular service users, e.g. celebrities; • In distressing circumstances, e.g. following a fire or road traffic accident; • In circumstances where a service user or a service user's relatives are complaining publicly about the treatment and care provided. Where practicable, the explicit consent of the individual service user(s) concerned should be sought prior to disclosing any information about their care and treatment, including their presence in a hospital or other institution. Where consent cannot be obtained or is withheld, disclosure may still be justified in the "exceptional" public interest.In distressing circumstances, care should be taken to avoid breaching the confidentiality of service users whilst dealing sympathetically with requests for information. Where a service user is not competent to make a decision about disclosure, the views of family members should be sought and decisions made in the service user's best interests. Where information is already in the public domain, placed there by individuals or by other agencies such as the police, consent is not required for confirmation or a simple statement that the information is incorrect. Where additional information is to be disclosed, e.g. to correct statements made to the media, service user consent should be sought but where it is withheld or cannot be obtained, disclosure without consent may still be justified in the public interest. The service user's concerned and/or their representatives should be advised of any forthcoming statement and the reasons for it. There is a strong public interest in sustaining the reputation of the NHS as a secure and confidential service but there is a competing interest in ensuring that the reputations of NHS staff and organisations are not unfairly and publicly maligned. Disclosures need to be justified on a case by case basis and must be limited to the minimum necessary in the circumstances. In some circumstances a "dignified silence" in the face of media enquiry, may be the best approach for the NHS to take, depending on the nature of the case involved.

Model B3: Non-medical purposes	
19) To Solicitors	Most contacts from solicitors are for subject access requests to medical records for compensation claims which may include: • insurance claims against third parties e.g. following road traffic accidents (RTAs); and • work related claims e.g. for disability awards, early retirement etc. There may also be requests for prosecution purposes in cases of, for example, drink driving, RTAs, GBH and murder enquiries etc. Ideally disclosure should be limited and relevant to the incident concerned. However, if disclosure of the full record is required, this should be complied with as long as it is clear that the service user understands that full disclosure will take place and has consented. On occasions when clinicians or NHS organisations face legal challenges, solicitors acting on behalf of a client may require access to a third party's record. In such cases, explicit consent should be sought from any person or persons to whom it relates. However, if a service user refuses consent, disclosure may still be warranted in the public interest or where a Court Order to support disclosure without consent has been received. It may be possible for a solicitor to make a public interest argument but this would be difficult to judge and best left to the Courts to decide. In all cases a service user should be notified of the disclosure.

Extract from Confidentiality NHS Code of Practice Department of Health, November 2003

Guidance on copying letters to service users

Introduction

The guidance provides the information required for staff within HPFT to implement the Department of Health's 'Copying Letters to Patients strategy'. From 2004, service users have had a right to receive a copy of letters concerning their treatment.

The rationale for the strategy is set out in paragraph 10.3 of the NHS Plan. This document is a guide to the implementation of that strategy. The following extract is from the report of the working group on copying letters to patients to the Department of Health.

"Patients have the option of having much greater information about the treatment that is being planned for them. Patients have the right to see their medical records, though in practice most communication between professionals is not available to the patient concerned. Patients often do not know why they are being referred or what is being said about them. In future, as a result of the NHS plan:

Letters between clinicians about an individual patient's care and treatment will be copied to the patient as of right."

These guidelines are a shortened version of the guidance to assist implementation; the full document can be obtained from the DOH website.

Which health care professionals should copy letters to service users?

All letters concerning NHS service users written to another health or social care professional should be copied if the service user wishes to receive the letter.

What is the definition of a letter?

There are many forms of letters including

- Letters or forms of referral
- Letters from health professionals to social care professionals.
- Letters to primary care from hospital doctors or other health professions following discharge or following an outpatient consultation.
- Letter to non-NHS agencies.

NB: Raw data such as single test results should not normally be sent directly to service users. If they are included in a letter e.g. to a general practitioner then the letter would be copied.

It is especially important that care plans are copied to service users.

Which letters should be sent to service users?

Each service will establish which kinds of communications should be copied to service users.

As a general rule and subject to the service users consent, formal communications from one health professional to another that help to improve a service user's understanding of their health and the care they receive should be copied to that service user.

Who is responsible for providing the letter to the service user?

The person writing the letter should be responsible for ensuring a copy is provided to the service user, having confirmed:

- that they wish to receive a copy
- how they wish to receive it and
- their preferred format.

Service users should be routinely asked during the consultation whether they want a copy of a letter written as a result of the consultation. Their agreement to this should be recorded in the care record at the time of the consultation or be included in the letter itself.

The letter should clearly state that a copy has been sent to the service user.

It is not the responsibility of the NHS professional who receives the letter to send a copy to the service user.

Those responsible for copying letters need to comply with equal opportunities legislation, including the provisions of the Equality Act 2010, the Race Relations (Amendment) Act 2000 and the Human Rights Act 1998. People with special communication or language needs, e.g. those whose first language is not English or who require the letter to be in large print, on audio tape, or Braille should not receive a poorer service than others.

How will the service user receive the copy letter?

The service user should be asked how they would like to receive the letter, for example, they may be concerned about privacy at home. The copies may be sent by post, e-mail or collected from an appropriate place. Consent must be gained if letters will be sent to a non-secure personal email address.

Envelopes must be marked 'confidential' and service users addresses routinely checked. The full name should be used instead of initials as two people with the same initials may live at the same address.

When should a letter not be sent?

Letters are subject to the same criteria under Data Protection Legislation as any other care record. There are some circumstances where it may be impracticable, unlawful or undesirable to copy letters, including where:

- The letter includes information about or given by a third party
- There is potential harm to the service user
- It is a sensitive area e.g. child protection issue
- The letter contains abnormal results or significant information that has not been discussed with the service user, in which case alternative arrangements

should make to discuss its contents before providing a copy for the service user, if they so wish.

Staff must remember that withholding a letter is the same as withholding any request for access to care records and that service users have the right to request access to records underData Protection legislation.

One healthcare professional may wish to comment on the clinical care provided by another and offer advice on the further care of service users with a particular condition or symptoms. In this case the professional concerned should write a separate letter that is not copied to the service user unless there is an argument for copying such information to the service user on the grounds of openness.

What is the position with children and young people?

Initiatives in copying letters have been developed in children's services. Young people aged 16 and 17 should be asked if they wish to receive copies of letters about them. It is up to health professionals to assess the competence of younger children to understand and make a decision.

Where parents are separated it is important to discuss who should receive the copy letters.

What happens if the service user lacks the capacity to request or receive a letter?

There should not be an assumption that the service user is not able to express their views. Whereas it may be judged that a person lacks mental capacity for one purpose, they may have sufficient capacity for another.

This may require, with the agreement of the service user, the involvement of advocates and/or carers to facilitate informed discussion and assist them to make their views known.

Where the service user does not have capacity to give valid consent, confidential information should be shared with the carer where it is in the person’s best interest.

Should letters by copied to carers?

Generally service users want information shared with their carers and with the service user's consent, a copy of the letter can be sent to the carer, e.g. when medication is changed following discharge from hospital.

Occasionally the service user may not want the letter copied or shown to the carer. This is their right and unless there is an overriding reason to breach confidentiality the wishes of the service user must be respected unless there are legal provisions which cover the carer's role.

What style should the letters be written in?

Clinical accuracy and ensuring the professional receiving the letter has all the information they need is the main purpose of the letter and should not be compromised in order to make the letter easier to understand. However, they should not use unnecessary complex language and should avoid subjective statements about the service user.

Templates and standard letters make it easier for health professionals to achieve this balance of technical excellence and correctness and ease of understanding.

The letter should indicate who can be contacted for further information about the contents of the letter or an explanation of the terms.

Monitoring and review

The IM&T/IG Programme Group will monitor and review the progress of the implementation of the strategy.

Appendix 3

Requests from the Police for Confidential Information about Service Users – Adults and Children

The Police may approach health professionals for the following reasons:

- The Police Child Protection and Investigation Unit is carrying out a Criminal Investigation involving one, or both of the parents, a carer or someone else known to the child.

- Criminal Investigations are being carried out by the Police which may amount to a serious charge such as murder or grievous bodily harm, or criminal neglect.

Remember that everyone has a right to confidentiality and the Caldicott Principles are clear about the responsibilities of the Trust in ensuring that confidentiality is maintained.

However, sometimes it is necessary to share information with other statutory authorities either because this is in the best interest of a service user(s) or is in the substantial public interest.

The Police have no automatic right to confidential information about our service users and therefore, provided the service user has capacity, their consent (or their parent's in the case of a child) should normally be sought before any information, or copies of clinical records are disclosed.

Disclosure to the Police can however take place without consent when it is in the substantial public interest and necessary to do so in order to assist the Police to prevent or detect a crime (and seeking consent would prejudice the purpose for which the information is sought) or by order of the Court. For example: -

- Serious crime investigations

- Child Protection investigations where consent has been requested but unreasonably refused. (Section 47 Children Act 1989)

Procedure for Disclosing Confidential Information to the Police
When a request is made by the Police for disclosure to them of confidential information about users of our service (without service user or parent consent, or a Court Order) the Police should be asked to submit a written request (Section 29 form) to the Trust under Data Protection Legislation in a timely manner. This will assist the decision as to whether releasing information is in the substantial public interest or to protect a child from significant harm.

The written request must include:

a) The purpose for which the information is required, and why it is necessary.

b) What information is required (must be specific)

c) Details of the Act and the particular provision of the Act under which the information is considered to be necessary.

d) Why it would prejudice the investigation to ask the service user (or parents) for consent to disclose the information to the Police.

e) The name, rank, number and signature of the officer making the request

A balancing judgement then needs to be made as to which of our duties is paramount,
i.e. the duty of confidence to the service user or the duty to assist the Police when it is in
the substantial public interest to do so.

If disclosure is appropriate then staff should be careful to disclose only the minimum information necessary to satisfy the Police's expressed purpose and record details of the disclosure on the EPR.

General advice on disclosure of service user information can be sought if needed, from the Information Rights and Compliance Team.

In Child Protection cases, the need for records to be shared will often be known and the
judgement of substantial public interest or child protection concerns may be clear-cut. For advice regarding child or adult protection cases contact the Head of Social Work and Safeguarding or Named Doctor.

The police have to apply to the Information Rights and Compliance Team if they require copies of medical or nursing notes as part of the investigation. The Information Rights and Compliance Team can seek the advice of the Trust Solicitor if there is doubt about releasing information.

In exceptional circumstances, the Police may request urgent disclosure for valid reasons and the need to submit a written request would cause a delay. In such cases unless it is a clear-cut Child Protection case, the police should be referred to the Safer Care and Standards Team who will advise on disclosure obtaining Legal advice if necessary.

Inform your Senior Manager prior to disclosing information, and consider discussing it with the Head of Social Work and Safeguarding and /or named Doctor for Child Protection or Adult Protection Manager as appropriate.

Where a death has occurred, the Police may approach you soon after the incident and request a verbal statement. You must inform your immediate Manager and the Named Nurse or Named Doctor for Child Protection or Adult Protection Manager.

Ordinarily, when providing witness statements to the police for the purposes of a criminal investigation, they are still required to put their request in writing and include the points above. Your Manager will discuss with the Police as to whether you can be given some time to provide a written statement. Where there is insufficient time

for this, then you will be interviewed, by a Police Officer. You must arrange for a senior member of staff to be present.

The Police will ask you a series of questions and write down what you say on a statement, which could be submitted as evidence to the Courts. On completion of the interview, you will be asked to sign the statement. Do not do so unless you are completely satisfied as to the content. Staff should ask the Police for a copy of their statement to take away. A copy of your signed statement should be provided to you in advance of the trial and in any event, you should be allowed to see your statement at the Police Station prior to the Court Case, if you wish. Any statement provided may be disclosed to family and Legal representatives.

Only information about you in your professional capacity should be provided as part of your witness statement. You are not obliged to disclose personal data about you (for example your home address) unless it is deemed pertinent to the investigation.

Any staff who have concerns about providing a witness statement should consult the Risk Management Team for further advice.


we are...
you feel...
Our Values
Welcoming
Valued as an individual
Kind
Cared for
Positive
Supported and included
Respectful
Listened to and heard
Professional
Safe and confident


Our Values
Welcoming Kind Positive Respectful Professional