Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL	
Title:	**Access to Health Records Policy**
Version:	**1**
Reference Number:	**IG003**

Scope:

This policy applies to all staff who come into contact with service users, or are in some way responsible for keeping or handling health records.

This policy applies to all health records, both manual and computerised including joint health and social care records.

This policy does not apply to requests for records from:

- Other NHS bodies or Health Professionals for treatment and care. (These types of requests are covered by the Information Sharing policy.)
- Requests from the Coroner's Office or for cases of litigation against the Trust – these are dealt with via the legal department (See TAD_IG003_01 for a list of contacts).
- Case conference reports, court reports or chronologies requested under safeguarding children or vulnerable adults proceedings.

Purpose:

The Purpose of this policy is to provide processes to be followed by Trust staff when dealing with requests for access to health records, and to inform the public how to make a request for health records.

Keywords:

Solicitors, Police, Health Records, Subject Access

Supersedes:

CO2 Version 6

Description of Amendment(s):

This policy was a Corporate Policy (CO2) which has been changed to an IG Policy Group.
Updated to comply with new data protection laws
Standard operating procedures removed
Request forms amended.

Owner:

Information Governance Manager – Paul Byrne

Individual(s) & group(s) involved in the Development:

This document has been developed in collaboration with the following interested parties:

- IG Management Meeting

Individual(s) & group(s) involved in the Consultation:	
The document has been circulated for consultation and comments have been taken into consideration and the document amended accordingly: • Information Governance Assurance Group – 17th May 2018	
Equality Impact Analysis:	
Date approved:	23/05/18
Reference:	IG-EIA003
Freedom of Information Exemption Assessment:	
Date approved:	21st May 2018
Reference:	2018/0735
Information Governance Assessment:	
Date approved:	17th May 2018
Reference:	
Policy Panel:	
Date Presented to Panel:	21st May 2018
Presented by:	Paul Byrne
Date Approved by Panel:	21st May 2018
Policy Management Team tasks:	
Date Executive Directors informed:	22nd May 2018
Date uploaded to Trust's intranet:	24th May 2018
Date uploaded to Trust's internet site:	24th May 2018
Review:	
Next review date:	May 2019
Responsibility of:	IG Manager
Other Trust documentation to which this guideline relates (and when appropriate should be read in conjunction with):	
IG002	Data Protection and Confidentiality Policy
IG001	Information Governance Strategy
CO013	Information Sharing Policy

Policy Associated Documents:	
TAD_IG003_01	List of Contacts
TAD_IG003_02	Application for Access to Health Records
TAD_IG003_03	Definition of Health Professional
TAD_IG003_04	Release Form
TAD_IG003_05	Acceptance of Terms for Medical Records Viewing
TAD_IG003_06	Application to amend or erase information
Other external documentation/resources to which this guideline relates:	
	Data Protection Act 2018
	Information Governance Intranet Page
	Information Governance Internet Page
CQC Regulations **This guideline supports the following CQC regulations:**	

Contents Page

1. INTRODUCTION

Individuals have a right to apply for access to health information held about them and, in some cases, information held about other people. The Trust needs to ensure it has adequate procedures in place to enable service users to exercise this right.

The main legislative measures that give rights of access to health records include:

- **Data Protection laws** – rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf. The information to be supplied, in most cases, free of charge to the applicant and within one calendar month of receipt of the request.
- **The Access to Health Records Act 1990** – rights of access to deceased service user health records by specified persons.
- **The Medical Reports Act 1988** – right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes.

2. PURPOSE

It is important that all staff understand the requirements of the law, and the part that they have to play in ensuring that the Trust complies with these legal obligations.

This policy provides procedures to be followed by Trust staff when dealing with requests for access to health records.

Compliance with Trust policies is a condition of employment and breach of a policy may result in disciplinary action.

Wherever, throughout the policy, the term 'record' is used this means both the manual file and/or the electronic service user record.

3. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

Any enquiries with regard to this policy should be directed to the Information Governance Manager.

The Caldicott Guardian has Executive responsibility for the management of Health Records.

The Information Governance Manager will oversee the day-to-day management of the policy.

It is the responsibility of the 'appropriate health professional' and the Subject Access Team to review the record prior to its release and to decide what information, if any, should be released and what should be withheld (see section 5) In the case of Mental Health Review Tribunals it will be the responsibility of the Mental Health Act Administrator to remove third party information.

4. RECEIVING AN ACCESS REQUEST UNDER THE DATA PROTECTION LAWS

A request for access to health records in accordance with Data Protection laws (referred to as a subject access request), should be made in writing, which includes by email or via social media, to the Trust.

Immediately upon receipt requests should be date stamped with the date the request came in to the department and directed to:

The Subject Access Team

Trust Headquarters

225 Old Street

Ashton under Lyne

Lancashire

OL6 7SR

Tel: 0161 716 3959/3149/3899

pcn-tr.sar@nhs.net

A full list of contacts for the subject access teams are attached at TAD_IG003_01 however the Information Governance department will direct the request to the correct co-ordinator.

If an individual is unable to make a written request it is the Department of Health view that in serving the interest of service users it can be made verbally, with the details recorded on the individual's file.

Requests must contain the following elements:

- Enough information to enable *the identification and location of the information being requested. A form is attached at TAD_IG003_02 that may be used to ensure all the information required is included within the request.*
- Sufficient information to be satisfied as to the identity of the applicant.

  Forms of ID must include one copy of proof of identity and one copy of proof of address. Example forms of ID are:

Proof of Identity	Proof of Address
In order to be acceptable, this document must meet the following criteria 1. It is not expired and is issued by an acceptable source; 2. It contains a photograph affixed by the issuing agency; and 3. It contains the same signature as that on the request.	Generally, documents meeting this requirement will show the following characteristics: 1. The document is system generated, although tenancy agreements and/or correspondence from a solicitor can also be accepted; also correspondence from an agency in the UK government, such as HMRC can be accepted;

There are many ways to meet this requirement, including Passport, Driving licence, EU Identity card, Student Identity card, work pass with photograph etc.	2. The document has a date and is current, usually issued in the last 6 months, but longer periods may apply in some cases, a TV license for example; 3. The document shows the same name and address as given on the request; 4. The document is from an acceptable source and clearly shows that the person has an account or customer identification registered in their name; 5. The document is <u>not</u> a bill for a mobile telephone; and *It is not the same document presented as proof of identity.* Examples include – utility bill, DWP letter

If this information is not contained in the original request the Trust will seek proof as required. Where requests are made on behalf of the individual service user the Trust should be satisfied that the individual has given consent to the release of their information (see section 9)

If a member of staff cannot be sure that someone requesting access to information is who they say they are, or, there is no ID available e.g. the applicant is under the age of 16, the member of staff may require them to provide other proof via a method deemed appropriate for the circumstance. This could be, for example, asking the individual to provide information which has been recorded as personal data by the Trust and which the individual may realistically be expected to know.

Service users do not need to give a reason for applying to access their records, but they do need to give sufficient information to enable the records to be located.

As good practice the Trust may check with the applicant whether all or just some of the information contained in the health record is required before processing the request. However, there is no requirement under data protection laws for the applicant to inform the Trust of which parts of the health record they require.

Where an access request has previously been met data protection laws permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between.

In determining whether a reasonable interval has elapsed, the Trust will consider:

- The nature of the information
- How often it is altered
- The reason for the repeated request(s).

5. WHO CAN MAKE A REQUEST FOR HEALTH RECORDS

Formal access to a record can be made by any of the following:

- the service user
- where the service user is a child (under 16), a person having parental responsibility for the service user can make the request or it may be possible to accept such a request from the child themselves, see section 10
- where the service user is incapable of managing their own affairs, a person appointed by the court to manage those affairs or a person upon whom the service user, when capable, has endowed an Enduring Power of Attorney or a Lasting Power of Attorney (LPA) (see also section 9)
- an agent/representative e.g. solicitor, carer, acting on behalf of an intellectually capable service user with written authority from the service user to make the request on their behalf or, a capable person might appoint someone to be their agent for the purpose of exercising data access rights by granting them a power of attorney
- where the service user has died, the service user's personal representative and any person who may have a claim arising out of the service user's death (see section 11).

However, access may also be requested from the following:

- Criminal Injuries Compensation Authority (CICA) or Department for Work and Pensions (DWP).
- Independent Mental Health Advocate (IMHA) (see section 16)
- The Police, who may wish to have access under the Crime and Disorder Act 1998 (see section 12)
- The Crown Prosecution Service
- The Court via an Order (see section 17)
- Other authorities/people authorised by the Caldicott Guardian

6. SITUATIONS WHERE ACCESS TO HEALTH INFORMATION MAY BE LIMITED OR DENIED

The Data Protection (Subject Access Modification) (Health) Order 2000 (S.I. No. 413)) enables the data controller to limit or deny access to an individual's health record where:

- The information released may cause serious harm to the physical or mental health or condition of the service user, or any other person.

Before deciding whether this exemption applies, a data controller who is not a health professional (as defined in data protection laws – see TAD_IG003_03) is obliged to consult the health professional responsible for the clinical care of the data subject, or if there is more than one, the most suitable one.

The ‘appropriate health professional’ is defined as:

“(a) the ‘appropriate health professional’ who is currently or was most recently responsible for the clinical care of the data subject in connection with the matter to which the information which is the subject of the request relates.”

Where there may be more than one such person, the ‘appropriate health professional’’ will be:

“(b) the ‘appropriate health professional’ who is the most suitable to advise on the matter to which the information which is the subject of the request relates”

In the absence of anyone else who might qualify for the role, the ‘appropriate health professional’’ will be:

“(c) an ‘appropriate health professional’ who has the necessary experience and qualifications to advise on the matters to which the information which is the subject of the request relates”

The appropriate health professional will be asked to sign a release form (TAD_IG003_04) stating they have been consulted and whether the records should be released either fully, partially or whether the request is refused. The purpose of the release form is to prove that the administrative staff have consulted the appropriate health professional.

If information is being denied to the applicant this will go the Caldicott Guardian for the final decision and sign off.

Access may also be limited or denied where it would disclose information relating to or provided by a third person who has not consented to that disclosure **unless:**

- The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the service user.
- The third party, who is not a health professional, gives their consent to the disclosure of that information.
- It is reasonable to disclose without that third party’s consent.

Access to parts of the record containing information relating to the social care of the service user cannot be denied on the grounds that the identity of a third party would be disclosed where the third party is a social worker or other social work professional unless to disclose it would cause the social worker or other social care professional serious harm. Where the record contains information written by social services staff permission to disclose must be obtained from the social services staff responsible for that part of the record. In some cases, this may involve liaising with the legal team of the social services department concerned.

The Subject Access Team will review the records for information relating to third parties and either seek consent from the third party or redact the information.

7. FEES TO ACCESS HEALTH RECORDS UNDER DATA PROTECTION LAWS

Data protection law states that the Trust must supply a copy of the information requested free of charge.

A reasonable fee can be charged when the request is manifestly unfounded or excessive, particularly if it is repetitive. The Trust can also refuse to respond to such requests.

The Trust may also charge a reasonable fee to comply with requests for further copies of the same information.

Any fees charged must be based on the administrative cost of providing the information.

Where the Trust refuses to respond to a request, an explanation will be given to the individual without undue delay and at the latest within one month, informing them of their right to complain to the Information Commissioners Office.

8. TIME LIMITS

Legally, a formal request for Access to Health Records must be actioned and completed within one calendar month.

However, the Department of Health has issued guidance that states that Trust's should be aiming to complete within 21 days.

In all cases it is therefore essential that any formal request is date stamped with date of receipt and sent to the subject access team immediately.

9. REQUEST TO VIEW THE RECORD

Wherever possible in response to a verbal request by the service user, informal access should be allowed by the 'appropriate health professional' to the parts of the record for which they have responsibility.

The 'appropriate health professional' must review the record first to decide if access can be permitted to all or parts of the record (see Section 5). The notes must also be reviewed by the Subject Access team to ensure that any third party information is removed. (see section 5)

The 'appropriate health professional' must then decide whether the access should be supervised by themselves or whether an appointment should be made for supervision by a lay administrator e.g. ward clerk, secretary – with the consent of the service user (see TAD_IG003_05 – Acceptance of terms for medical records viewing). In these circumstances the lay administrator must not comment or advise on the content of the record and if the applicant raises enquiries, an appointment with the 'appropriate health professional' should be offered.

If full or partial access is granted, the service user should make an appointment in which they can view the record. It should be agreed, if there is more than one volume, which volume is to be viewed first. Appointments should then be arranged in consultation with

the health professional/layperson and each appointment should not exceed one hour unless the health professional/layperson agrees otherwise.

For informal access the record must not be removed from Trust premises.

When informal access is granted a full explanation of any abbreviations or medical terminology should be offered by the 'appropriate health professional' and thus any subsequent discussions must be documented clearly in the record.

Access should not normally be granted to someone other than the subject of the records, at least where they are capable of requesting it themselves.

10. DOCUMENTING THE REQUEST

All requests for access to health records under this policy must be logged by the Subject Access Team onto the Safeguard Risk Management System.

A copy of the request and release form should be filed onto the service user record.

11. CONSENT REQUIREMENTS FOR ACCESS TO HEALTH RECORDS

A service users written consent should be less than 6 months old. In relation to Criminal Injury Compensation Authority/Veterans Agency requests the time period may be extended. The Information Governance Manager/Data Protection Officer can be consulted where there is any doubt.

Where the service user has capacity: - A service user may request access to information about themselves through an agent. This must be done in writing and the consent of the service user obtained.

It is best practice to ensure that the service user understands what information is contained within their health record and is being disclosed so that consent can be fully informed.

Where the service user is incapacitated: - As the law stands, nobody is empowered to give consent on behalf of an adult. However, where a person is incapable of giving or withholding their consent, it will be the person in charge of the service users treatment who will decide whether information about them may be disclosed to someone else. A service user may be incapable because they are unconscious or mentally ill, or for some other reason. In many cases, the person in charge of their treatment may be the one identified as the 'appropriate health professional', but this will not necessarily be the case. Disclosure of information may only take place if it is in the service user's 'best interests'. In order to decide whether this requirement is met, the person making the decision must consider everything that is known about the service user (including any wishes they might have expressed while capable), together with the views of relatives or carers.

Where an adult is, or becomes, incapable of making decisions on their own behalf, the law provides that another may be appointed to act on their behalf as an agent.

- An Enduring Power of Attorney (EPA)

Individuals who made provision for a specified party to be appointed to act as their attorney should they become mentally incapacitated did this by way of an Enduring Power of Attorney (EPA) prior to the Mental Capacity Act 2005 coming into force. The scope of the general powers is limited to "the management of property and affairs" of the donor. Persons with EPA have no data protection or common law consent functions. Nevertheless, sometimes it may be appropriate to involve them as the persons who have the authority to make commercial arrangements for service users, including arrangements to provide both accommodation and nursing care. They, on the service user's behalf, may have an interest in securing the best value in a nursing and care package. Where that is the case, it may be necessary to consider whether the vital interests/medical care needs of the service user in question also require the disclosure of all or some of the sensitive personal information in question to the person who holds the EPA. The EPA must be registered with the Public Guardian when the service user can no longer manage their affairs and a copy provided to the Subject Access Team prior to a decision being made regarding disclosure of any information.

The Mental Capacity Act 2005 came into force in October 2007 and replaced the EPA with the Lasting Power of Attorney (LPA). From October 2007 only LPA's can be made but existing EPA's will continue to be valid.

- A Lasting Power of Attorney (LPA)

The Mental Capacity Act 2005 increased the range of different types of decisions that people can authorise others to make on their behalf. As well as property and affairs (including financial matters), LPAs can also cover personal welfare (including healthcare and consent to medical treatment) for people who lack capacity to make such decisions for themselves. The service user can choose one person or several to make different kinds of decisions. An LPA must be registered with the Office of the Public Guardian (OPG) and a copy provided to the Subject Access Team prior to a decision being made regarding disclosure of any information.

- Personal Welfare LPA's

LPA's can be used to appoint attorneys to make decisions about personal welfare, which can include healthcare and medical treatment decisions. Personal welfare LPA's might include decisions about:

  - Where the donor should live and who they should live with
  - The donor's day-to-day care, including diet and dress
  - Who the donor may have contact with
  - Consenting to or refusing medical examination and treatment on the donor's behalf
  - Arrangements needed for the donor to be given medical, dental or optical treatment
  - Assessments for and provision of community care services

- Whether the donor should take part in social activities, leisure activities, education or training
- The donor's personal correspondence and papers
- Rights of access to personal information about the service user, or
- Complaints about the service user's care or treatment

The service user, when making an LPA can add restrictions or conditions to areas where they would not wish the attorney to have the power to act. It is therefore essential that the LPA is registered by the Office of the Public Guardian (OPG) and is carefully reviewed before any information is disclosed.

- Property and affairs LPA's

A service user can make an LPA giving an attorney the right to make decisions about property and affairs (including financial matters). A service user can state in the LPA document that the LPA should only apply when they lack capacity to make a relevant decision. It is essential that the LPA is registered by the OPG and is carefully reviewed before any information is disclosed.

- The Court of Protection

Prior to the introduction of Mental Capacity Act 2005 where a person lost mental capacity or never had mental capacity, the management of a service user's property and affairs fell to the Court of Protection. The new Act increased the remit of the Court of Protection to include dealing with serious decisions affecting healthcare and personal welfare matters. These were previously dealt with by the High Court under its inherent jurisdiction.

An attorney or agent appointed by the Court of Protection would have, under his general powers, appropriate authority to make a subject access request on the service user's behalf.

12. CHILDREN AND YOUNG PEOPLE

A person, with parental responsibility – see 11.5, can make subject access requests on behalf of their children who are too young to make their own request. A young person aged 13 or above can be considered competent enough to understand what a subject access request is. If they are judged to be competent enough to understand they can make their own request and would need to provide their consent to allow their parents to make the request for them. The health professional must use their own judgement to decide whether a young person aged 13 or above is competent enough to make their own request as they do not always have the maturity to do so.

Where more than one person has parental responsibility, each may independently exercise rights of access. In the case where a child lives with their mother and whose father applies for access to the child's records, there is no obligation to inform the child's mother that access has been sought. However, the father may only be given access to

information where he has parental responsibility for the child (see 11.5). Access should only be given with the child's consent if the child is capable of giving consent.

Children of all ages vary in their level of maturity and understanding, and therefore, each case should be dealt with on an individual basis.

Where the child is 13 or above it will be necessary to enquire of the clinician/practitioner who has most recently treated the child as to whether in their opinion the child has reached an age where they have sufficient understanding and intelligence to understand the nature of the application for access to their records. Each application must be assessed on an individual basis.

Not all parents have parental responsibility. Both parents have parental responsibility if they were married at the time of the child's conception, or birth, or at some time after the child's birth. Neither parent loses parental responsibility if they divorce. If the parents were not married, the mother will automatically have parental responsibility at birth, the father will only have it automatically if the child's birth was registered on or after 1st December 2003 and the details were included on the birth registration. However, there are circumstances in which a father who is not married to the child's mother and not registered on the birth certificate may acquire parental responsibility. Furthermore, parental responsibility for a child may be held by, for example grandparents, or by a local authority.

Where a child is "looked after" by the Local Authority permission needs to be given by both the Local Authority and the parents as they share parental responsibility.

Competent young people may also seek access to their own health records.

The data protection laws do not allow disclosure of information whose disclosure is already prohibited in legislation concerning adoption records and reports, statements of a child's special educational needs and parental order records and reports. Health professionals who believe their records may contain such information should seek advice from the Information Governance Manager/Data Protection Officer.

12.1 Child Protection Cases

Section 47 of the Children Act 1989 places certain duties on local authorities where they have reasonable cause to suspect that a child, who lives in their area, is suffering or is likely to suffer significant harm. Local authorities are required to make such enquiries, as they consider necessary to enable them to decide whether any action should be taken to promote a child's welfare.

A corresponding duty is placed upon the Trust to assist with those enquiries by providing relevant information and advice about a child if called upon to do so.

If a request for information about a child is received in the context of proceedings to protect the vital interests of the child, where the consent of the child cannot be obtained, the records may be released where necessary.

It is important that appropriate advice is sought via the Child safeguarding leads and the Information Caldicott Guardian/Data Protection Officer before the records are released if

the request is not accompanied by a Court Order requiring disclosure of the medical records.

If the record contains child psychiatry information the 'appropriate health professional' within child psychiatry should be contacted before access to that part of the record is permitted.

12.2 Children and Proceedings

Where health records of children held by the Trust are requested for the purposes of assisting in criminal or civil proceedings relating to that child, the Trust shall not disclose such records if it is satisfied that access to them is likely to cause serious harm to the physical or mental health or condition of the child, even where, parental consent has been gained by the Crown Prosecution Service or Police.

The Trust shall only disclose health records where the purpose of disclosure is in accordance with that stated in clause 10.14 above when it has been served with a Court Order.

Each request shall be considered on a case by case basis in consultation with the lead clinician involved with the child. Final approval will be sought from the Caldicott Guardian where there is a disagreement between the Information Governance Manager/Data Protection Officer or Legal Department and the Clinician involved.

13. WHERE THE SERVICE USER IS DECEASED

Data protection laws only apply to living individuals. Health records of deceased service users are covered by the Access to Health Records Act 1990, which entitles the applicant to access records made on or after 1st November 1991. Access must also be given to information recorded before this date if this is necessary to make any later part of the records intelligible.

"Where the service user has died, the service user's personal representative is entitled to apply for access to information about the deceased. A service user's personal representative is:

- An executor appointed under the deceased's will,
- Where there is no will, a person appointed as administrator"

If the applicant is not a Personal Representative the dependants of a deceased service user may have a claim arising out of the death. Dependants are defined as including:

- the wife or husband or former wife or husband of the deceased
- any person who:
    - was living with the deceased in the same household immediately before the date of death and
    - had been living with the deceased in the same household for at least two years before that date and
    - was living during the whole of that period as the husband or wife of the deceased

- any parent or other ascendant of the deceased
- any person who was treated by the deceased as his parent
- any child or other descendant of the deceased (including an infant born after the death but who was en ventre sa mare (i.e. conceived but not yet born) at the time of the injury that caused the death)
- any person (not being a child of the deceased) who, in the case of any marriage to which the deceased was at any time a party, was treated by the deceased as a child of the family in relation to that marriage
- any person who is, or is the issue of, a brother, sister, uncle or aunt of the deceased.

Once proof of appointment as a Personal Representative or that the applicant is a dependant who may have a claim arising out of the death has been obtained then it is necessary to consider which part of the records are relevant to the claim. Section 5 (4) of the Access to Health Records Act 1990 states that access shall not be given to any part of the records which, in the opinion of the holder of the records, would disclose information which is not relevant to any claim which may arise out of the service user's death. It is necessary to consider the type of claim envisaged by the applicant and decide which records are relevant to the claim.

In addition, a claim arising out of the Inheritance (provisions for Family and Dependants) Act 1975 would also be a valid claim.

Dependants are defined under the 1975 Act as follows:

- A spouse or former spouse of the deceased,
- A child of the deceased,
- A child of the family,
- A dependant of the deceased at the time of the deceased's death.

Before providing access to healthcare information to any personal representative of the deceased or anyone with a claim arising out of the death of the deceased, the deceased's records should be checked to ensure that the deceased made no request, when they were alive, that their records which are relevant to a legal claim arising out of the death of the deceased should not be disclosed to the applicant. In addition, the 'appropriate health professional' should agree that disclosure would not be likely to cause serious harm to somebody's physical or mental health and any third party information must be removed.

The request must be dealt with by the Subject Access Team.

Any other requests which fall outside the scope of 12.2 – 12.7 above will be considered by the Caldicott Guardian

All requests for access to deceased records, when approved, will generally be provided free of charge as per section 6 above.

14. REQUESTS FOR INFORMATION BY THE POLICE

The Trust wishes to foster good relations with the police, and to play its part in keeping the public safe and protecting it from crime. However, the Trust also has a duty to protect the confidentiality of its service users, whether they are in hospital or in the community, and whether they are alive or dead. The duty is breached where information about a service user – including the mere fact that they are a service user – is disclosed to someone else including the police.

The Trust has a duty to comply with the provisions of the data protection laws. It follows that information may only be disclosed with the consent of the service user, save in exceptional circumstances.

Disclosure may be necessary in the public interest where a failure to disclose information may expose the service user, or others, to the risk of death or serious harm. In such circumstances the information should be disclosed promptly to an appropriate person or authority. Such circumstances may arise where the disclosure is necessary for the prevention of serious crime. The circumstances where this can arise are diverse and will need to be considered on an individual basis. They can include circumstances where a service user or former service user is the victim of an offence or is suspected of having committed an offence.

14.1 Consent

If capable, an adult service user should be asked to give explicit consent to information about them being disclosed unless the police give good reasons why this would be detrimental to the investigation or prevention of a serious arrestable offence. A child of any age may also give such consent, provided they are sufficiently competent to understand the nature of disclosure. If the child is not sufficiently competent, consent to disclose may be given by anyone with parental responsibility for them (see section 11). The consent must be less than 6 months old, and must detail to whom the information is being disclosed, what parts of the record are being disclosed and why the information is requested.

Even if consent has been given, the procedures around permitting access by the 'appropriate health professional' and subject access team still apply.

If the consent of the service user cannot be obtained the following principles apply:

- The police do not have a general right of access to records or information about service users. Unless there is a court order, the final decision about what may be disclosed will rest with the Trust. However, any request for information by the police should be considered by the health professional who is in charge or was in charge of the service user's treatment in the first instance.
- Disclosure of confidential information may be necessary for the prevention or detection of serious crime. If, therefore, a police officer is investigating a "serious offence" the health professional in charge of the service user's care should bear this in mind when deciding whether or not to disclose confidential information. A serious offence would include any offence that may have caused or could cause serious harm to any person.

- A police officer requesting disclosure of confidential information relating to a service user should be asked to provide:
- Confirmation that the offence being investigated is a serious arrestable offence;
- Why it is believed the subject matter of the request has committed or is about to commit such an offence;
- The reason it is believed the provision of the information requested will assist the investigation
- If the request is urgent, the reason for this.
- If time allows the police request form information form 819T should be completed by an officer and retained by the Subject Access Team.
- Only information that is relevant to the police enquiry should be given.
- If the health professional in charge of the service user's treatment decides against releasing information and the Police dispute this then the matter should be referred to the Caldicott Guardian for further consideration. The Caldicott Guardian shall consult with the health professional in charge of the service user's treatment before a decision is made whether or not to release the information.
- Ensuring the request is genuine
- Anyone who claims to be a police officer and to be acting as such should be asked to produce their warrant card. The card is credit card sized and pale blue in colour. It should include:
    - The Greater Manchester Police logo
    - The officer's photo
    - Their warrant number
    - A signature from the chief constable
- In addition, the officer should be asked for their collar number, which should match the number on the warrant card.
- If there is any doubt that the request is genuine verification can be sought by contacting the police on 0161 872 5050.
- Requests received over the phone can also be verified on the above number.
- Request the officer to send the form 819T by email from a work email address.

15. REQUESTS FROM SOLICITORS

These should be made in writing and clarification of whether or not action is intended against the Trust must be obtained.

If action against the Trust is intended the request must be forwarded immediately to the Legal Department who will action the request.

In all other cases the request must be dealt with by the Subject Access Team

Solicitors have no greater right of access to information than is enjoyed by their client.

16. REQUESTS IN RELATION TO TRIBUNAL SERVICE MENTAL HEALTH

These are dealt with by the Mental Health Law Administrators.

17. REQUESTS FROM INDEPENDENT MENTAL HEALTH ADVOCATES (IMHA)

Under section 130B of the Mental Health Act 1983 ("the Act"), for the purpose of providing help to a qualifying service user, IMHAs may require the production of and inspect any records relating to a service user's detention or treatment in any hospital or registered establishment or to any after-care services provided for the service user under section 117 of the Act. IMHAs may also require the production of and inspect any records of or held by, a local social services authority, which relate to the service user.

Under section 130B, IMHAs may only access records for the purpose of providing help to a qualifying service user in their role as IMHA, and where the following conditions are met:

- Where the service user has the capacity (or in the case of a child, the competence) to decide whether to consent to the IMHA seeing the records, the IMHA can only access the records if the service user has consented.
- Where the service user does not have the capacity or competence to consent to this disclosure:
    - Records must not be disclosed if that would conflict with a decision made in accordance with the Mental Capacity Act 2005 on the service user's behalf by a done of lasting power of attorney or a deputy, or by the Court of Protection;
    - Otherwise, the record holder must allow the IMHA access if they think that it is appropriate and that the records in question are relevant to the help to be provided by the IMHA.

In this latter case, the Code of Practice to the Act advises that the record holder should ask the IMHA to explain what information they think is relevant to the help they are providing to the service user and why they think it is appropriate for them to be able to see that information.

Anyone who refuses, without reasonable cause, to produce records that an IMHA has a right to inspect may be guilty of the offence of obstruction under section 129 of the Act.

All requests from IMHA's are dealt with by the Subject Access Team.

18. COURT ORDER / AFFIDAVIT

Often disclosure of medical records of the alleged victim of, or witness to, a crime is requested by the alleged perpetrator's defence lawyers, and occasionally by the Crown Prosecution Service or prosecution team. Initial refusal by the 'appropriate health professional' to release such records will usually be met by a witness summons being issued by the court (under the Criminal procedure (Attendance of Witnesses) Act 1965 in the Crown Court. The defence legal team are only entitled to have access to confidential material that is relevant to the matters in issue in the criminal trial. They are not entitled to trawl through a service user/victim's entire psychiatric history seeking material for cross-examination.

Prior to the applicant (defence/prosecution) requesting a court order to be served on the Trust they should issue the Trust with an affidavit and copy of the application notice to answer within 7 days (crown court rules 1982). This gives the Trust a period of time to decide whether the records should be disclosed or whether it would not be in the best interests of the service user, or the third parties mentioned within the notes, to disclose the whole record(s) to the court. If the service user does not consent to disclosure, the 'appropriate health professional' remains obliged to refuse disclosure on the grounds of confidentiality. The Trust can then either write to court setting out the reasons why it is felt a summons should not be issued or the Trust can attend the hearing for the summons (legal representation would be required if this is the case).

If the Trust is not issued with the affidavit it may be served with a summons to produce the records to the court on a specific date. Failure to comply with the order may be contempt of court, and therefore a very serious matter. A Court Order will usually require a consultant/lead clinician or member of the Subject Access Team to produce healthcare records to the court, and in these circumstances they should not be handed over to the police, defence or prosecution.

It is essential that all original records the Trust holds relating to the service user are taken to the court with a copy of the records. The Subject Access Team will establish what records are held and inform the Information Governance Manager/Data Protection Officer of the order. The Information Governance Manager/Data Protection Officer will liaise with the Subject Access Team and/or lead clinician regarding attendance at court (if required) and production of the records

If an affidavit or court order is issued to the Trust it must immediately be telephoned through to the Subject Access Team on 0161 716 3149/3959/3899 and a copy of the affidavit/order scanned and emailed via secure mail. The Information Governance Manager/Data Protection Officer can advise on the action to be taken if the Subject Access Team is not available.

Where information is disclosed under court order, those who disclose it will usually have a complete defence to any allegation that they have breached confidentiality, but the order must be interpreted correctly and information only be disclosed in accordance with the terms of the order. However, even though the court has ordered production of the notes the 'appropriate health professional' and the Subject Access Team should still review the notes for anything that may harm the service user or any other person. It may then be necessary for the Trust to seek legal representation if it is felt it would not be in the best interests of the service user, or the third parties mentioned within the notes, to disclose the whole record(s) to the court. In these circumstances the Information Governance Manager/Data Protection Officer should be contacted so that, if the Trust agrees, legal representation can be appointed.

19. DISCLOSURES TO MEMBERS OF PARLIAMENT CARRYING OUT CONSTITUENCY WORK

An Order has been introduced because of concerns that organisations sometimes took the view that they could not respond fully to a Member of Parliament's request for information

regarding a constituent without the constituent's consent. In general, Members can safely assume that constituents who have raised matters with them expect that the Member will retain any personal information provided, will disclose it as appropriate and that organisations asked to explain their actions will disclose personal information to Members where this is necessary to provide an appropriate response. In such circumstances the constituents concerned may be reasonably considered to have implicitly consented to processing that is reasonably necessary to pursue their concerns. However, each request should be judged on its own circumstances based on the information requested.

The Order does not place an obligation on organisations to disclose personal data to Members. It merely gives those who want to disclose relevant sensitive personal information, when this is necessary to respond to matters raised on behalf of constituents, a basis to do so.

However, there may be exceptional circumstances when an organisation responding to a Member is justified in contacting the constituent to inform them of intended disclosures despite the effect of this Order. An example would be where an organisation considered that to provide a proper response it was necessary to disclose sensitive personal information outside the likely expectation of the individual concerned where it was possible that such disclosure could cause genuine distress. In such circumstances the duty of confidentiality could dictate that the individual should be alerted to the intended disclosure.

20. DEPARTMENT OF SOCIAL SECURITY (DSS) (INCLUDING BENEFITS AGENCY AND WAR PENSIONS AGENCY)

Requests for information used for Benefit Assessment Purposes

In order to assess the benefit claims of their client it is often necessary for the DSS to request sight of copies of the hospital case notes or to have a factual report prepared. This is in order that the claim can be objectively considered.

The request should not be passed on to the service user's General Practitioner. If approached by the DSS for information the responsibility to provide it lies with the Trust and not a third party. The request will therefore be dealt with by the Subject Access Team who will remove any third party information accordingly.

20.1 Consent to release of information

It is not necessary for service users or their representatives to exercise their rights under the data protection laws to obtain information to support a claim for benefit. The service user will be aware that the DSS may be required to make such requests and the consent from the service user is an integral part of the benefit claim form.

20.2 Response Time

Requests should be met within 10 working days of receipt. Prompt and accurate responses are essential if the DSS is to meet its own obligations to its clients.

Failure to comply with the 10 day "turn round" may result in delay of benefit payment to the client.

20.3 Confidentiality

The DSS is required to handle all information in a manner that is in accordance with NHS Policy on the secure handling of confidential service user information.

21. SENDING THE RECORD TO THE APPLICANT

Only copies of records should be sent to any applicant. Under no circumstances must original records be removed from Trust premises.

All access responses should be enclosed in a sealed tamper proof envelope clearly marked 'TO BE OPENED BY ADDRESSEE ONLY'. Where the address of the service user applicant is different to that shown on their health record, proof of identity and address (e.g. household bill or driving licence) may be required before the records can be sent through the post. The department name and address should be on the reverse of the envelope marked return address in case of non-delivery tamper proof envelopes should be used which are of sufficient thickness to obscure the information contained inside. Best practice is to send the records special delivery.

It would be prudent to clarify with the data subject whether they would prefer the records to be sent via post (special delivery), email or collected in person.

22. RESPONSES COLLECTED IN PERSON

Where an access response is to be collected personally by the applicant, then positive proof of identity (see section 3.4) must be provided before such information is released if the applicant is unfamiliar (Evidence of identity may have already been provided when the applicant made the request, and would not need to be provided again). The records must be signed for and the date collected recorded.

23. DATA SUBJECT RIGHTS

Data Protection laws provide the following rights for individuals:

- The right to be informed of the uses of their personal information
- The right of access to personal information held by organisations
- The right to rectify any information which is inaccurate
- The right to erasure of personal information
- The right to restrict processing of personal information
- The right to data portability
- The right to object to the processing of their personal information
- Rights in relation to automated decision making

24. DEALING WITH COMPLAINTS

If a service user is unhappy with the outcome of their request, for example information withheld from them or they feel their information has been recorded incorrectly within their

health record and a request to amend their record has been refused, the service user should be encouraged to go through the following channels:

- Contact the Data Protection Officer for further guidance
- The health professional may wish to have an informal meeting with the individual in the hope to resolve the complaint locally.
- If the health professional feels that they cannot do anything for the service user locally, the service user should be advised to make a complaint through the Trust's formal complaints procedure (see the Trust's Complaint Policy for further information).
- Ultimately, the service user may not wish to make a complaint through the Trust's complaints procedure and take their complaint direct to the Information Commissioner. The Information Commissioner has such powers to rule that any erroneous information is rectified, blocked, erased or destroyed and can also request an assessment around the non-disclosure of information to the applicant. Any requests for assessment from the Information Commissioner will be investigated by the Information Governance Manager/Data Protection Officer.
- Alternatively, if the service user wishes to do so, they may wish to seek legal independent advice to pursue their complaint.

Useful contact addresses for complaints:

Pennine Care Complaints Department	**Information Commissioner's Office**
The Complaints Manager	Wycliffe House
Pennine Care NHS Foundation Trust	Water Lane, Wilmslow,
225 Old Street, Ashton-under-Lyne	Cheshire, SK9 5AF
Lancashire, OL6 7SR	Switchboard: 01625 545700
Telephone: 0161 716 3000	Fax: 01625 524510

25. WHAT IF CORRECTIONS / ERASURES ARE REQUESTED

Where a person considers that any information contained in a health record or part of a health record to which they have been given access, is inaccurate, they may apply for the necessary correction to be made (an application form is enclosed at TAD_IG003_06 which should be returned to the SAR team).

An extra sheet may be added to the health care record for such corrections.

When such an application occurs, the holder of the health record should either:

- if they is satisfied that the information is inaccurate, make the necessary correction or
- if they are not satisfied, insert a copy of the completed TAD_IG003_06 in the relevant part of the health records, the matters which the applicant alleges to be inaccurate should be discussed and any discussion documented.

The correction should be signed and dated by the holder of the health record and applicant.

The applicant must be provided, without charge, a copy of the correction or the note of the request and any discussion.

When corrections are made, care must be taken not to obliterate information. It is recommended that a single line is drawn through the error and the correction should be dated and signed. The use of obliterating material, e.g. Tippex, must **never** be used.

Should the service user not be satisfied as to the outcome of their application for the record to be amended they can make a complaint using the NHS complaints procedure (see Section 23).

26. TRAINING & CAPABILITIES

In addition to the mandatory on-line Information Governance training, ad hoc training is provided by the Information Governance Manager/Data Protection Officer.

Further guidance and procedures are made available on the intranet and via staff bulletins etc.

27. REPORTING

A quarterly report will be provided to each borough/division via the Information Governance Assurance Group (IGAG) meeting on the following:

- No. of requests dealt with within one month legal timeframe
- No. of requests dealt with within 21 day good practice timeframe set by the Department of Health
- Reasons for any delay in responding within the appropriate timeframe

28. EQUALITY IMPACT ANALYSIS

As part of its development, this document was analysed to consider / challenge and address any detrimental impact the policy may have on individuals and or groups protected by the Equality Act 2010. This analysis has been undertaken and recorded using the Trust's analysis tool, and appropriate measures will be taken to remove barriers and advance equality of opportunity in the delivery of this policy / procedure

29. FREEDOM OF INFORMATION EXEMPTION ASSESSMENT

Under the Freedom of Information Act (2000) we are obliged to publish our policies on the Trust's website, unless an exemption from disclosure applies. As part of its development, this policy was assessed to establish if it was suitable for publication under this legislation. The assessment aims to establish if disclosure of the policy could cause prejudice or harm to the Trust, or its staff, patients, or partners. This assessment has been undertaken using

the Trust's Freedom of Information Exemption Guide, and will be reviewed upon each policy review.

30. INFORMATION GOVERNANCE ASSESSMENT

This Policy has been analysed to ensure it is compliant with relevant information law and standards as in place at the time of approval, and are consistent with the Trust's interpretation and implementation of information governance components such as data protection, confidentiality, consent, information risk, and records management.

Compliance will be reviewed against any changes to legislation / standards or at the next review of this document.

31. SAFEGUARDING

All staff have a responsibility to promote the welfare of any child, young person or vulnerable adult they come into come into contact with and in cases where there are safeguarding concerns, to act upon them and protect the individual from harm.

All staff should refer any safeguarding issues to their manager and escalate accordingly in line with the Trust Safeguarding Families Policy and Local Safeguarding Children/Adult Board processes.

32. MONITORING

The effective application of this policy, including adherence to any standards identified within will be subject to monitoring using an appropriate methodology and design, such as clinical audit.

Monitoring will take place on a biannual basis and will be reportable to the Quality Group via the Clinical Effectiveness and Quality Improvement Team.

33. REVIEW

This policy will be reviewed annually for compliance and re-ratified no more than every three-yearly unless there is a need to do so prior to this; e.g. change in national guidance or legislation.

34. REFERENCES

Guidance for Access to health records requests – Department of Health Feb 2010

Information Commissioner – Data Protections laws

Independent Mental Health Advocates – Supplementary guidance on access to service user records under section 130B of the Mental Health Act 1983

HSC 1999/001 The Provision of Service user Information by NHS Trusts to the Department of Social Security

Mental Capacity Act 2005 Code of Practice