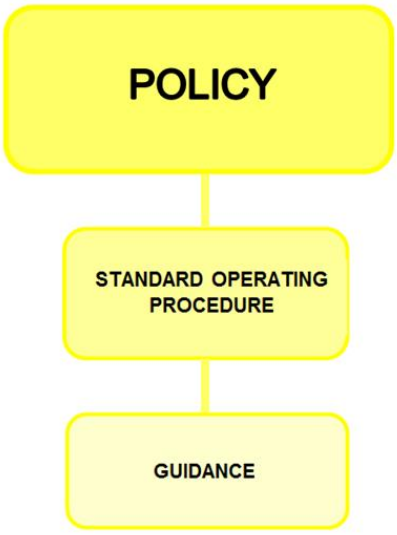
Lancashire Care NHS
NHS Foundation Trust

Access to Records Policy

UNIQUE POLICY REFERENCE	IMT009
APPROVAL DATE	December 2017
REVIEW DATE	March 2019
POLICY AUTHOR	Clinical Coding & Health Records Lead
ACCOUNTABLE DIRECTOR	Chief Finance Officer/Senior Information Risk Owner
APPROVED BY	Chief Finance Officer

TRUST GOVERNANCE STRUCTURE
POLICY LINKED TO *Corporate Governance & Compliance Sub Committee*



POLICY VERSION CONTROL

This record shall detail all previous versions of the Policy, including versions that have been known by other names and the date of when a new version was created.

Previous Versions (Title)	**Date Reviewed**	**Why was a new version created?**
Access to Health Records Policy	*July 2009*	*Original release date*
Access to Health Records Policy	March 2016	Policy updated to include staff guidance on how to deal with Police requests
Access to Health Records Policy	*March 2017*	*Policy updated as part of review process. Policy title changed to cover access to all records held by the Trust not just Medical Records.*

1. TRUST POLICY STATEMENT

The Trust is required to ensure that good mechanisms are in place for handling and processing request for access to Personal Identifiable Data (PID)

For information to be personal data, it must relate to a living individual and allow that individual to be identified from it, either on its own or along with other information likely to come into the organisation's possession.

The Data Protection Act 1998 (DPA) is based around eight principles of 'good information handling'. These give people specific rights in relation to their personal information and place certain obligations on those organisations that are responsible for processing it.

Under current legislation (DPA) and new legislation General Data Protection Regulations 2018 (GDPR) Data Subjects are entitled to request a copy of the information that we hold about them. This may include Health Records, Occupational Health Records, Employee Records, email exchanges and text messages. This list is not exhaustive.

The Trust will comply with all requirements of the DPA and subsequently the GDPR in carrying out its duties as a Data Controller and will share information, where appropriate in accordance with other legislation such as:

- Access to Health Records Act 1990
- DoH Guidance for Access to Health Records Requests (Feb 2010)
- Mental Capacity Act 2007
- The Access to Medical Reports Act 1988
- Gender Recognition Act 2004
- The Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005
- Prevention of Terrorism Act (1989) and Terrorism Act (2000)
- The Road Traffic Act (1988)
- Police and Criminal Evidence Act (1984)
- The Crime & Disorder Act (1998)
- Multi Agency Public Protection Arrangements (MAPPA) (includes the Probation and Prison Services)
- NHS Codes of Practice.
- General Data Protection Regulations (to be implemented in May 2018)

2. APPLICATION

Chief Executive Officer (CEO)
The CEO has overall Trust accountability for this Policy and provides assurance to the Trust Board of statutory and regulatory compliance.

Caldicott Guardian (CG)
The CG is the senior person responsible for protecting the confidentiality and security of Service Users information and ensuring that information sharing is safe, secure and appropriate. Serious breaches will be reported to the CG and recorded on the CG log.

Senior Information Risk Owner (SIRO)
The SIRO is accountable for Information Risk Strategy and seeks assurance in respect of compliance with this Policy and procedure.

Information Governance, Assurance and Compliance Lead
The IG Lead is responsible for ensuring that the organisation meets its statutory and corporate responsibilities and engenders public confidence in the handling of personal and corporate information.

Health Records Lead
The Health Records Lead is responsible for writing and promoting the use of this Policy and associated documents across all areas of the Trust.
They will offer guidance and support to Information Asset Owners and Managers on implementation and compliance.
The Health Records Lead is responsible for ensuring that the Trust is compliant with legislative requirements when dealing with requests for personal information relating to Health Records.

Data Protection Act Administrator (DPA Admin)
The DPA Admin will be responsible for co-ordinating and facilitating the processing of subject access requests received by the Trust. They will ensure that documented local processes and procedures are in place to handle any requests and will provide training to those staff identified as Subject Access Handlers across the Trust. The DPA Admin will be responsible for administration and maintenance of the Trusts central register and will monitor compliance with legislative guidelines and time scales.

Information Asset Owners (IAO) and Information Asset Administrators (IAA)
IAO and IAA's will also support the SIRO in the overall Information risk management function and ensure the use and protection of the Corporate asset. This will be achieved by maintaining an Information Asset register which is reviewed as a minimum annually.

The IAO and IAA roles will document, understand and monitor;
- What information assets are held and for what purpose
- How information is created, amended or added to overtime e.g. access to the correct version
- Who has access to the information and why
- Understand and address the risk to the asset, providing assurance to senior management

All staff

All staff are required to familiarise themselves with the Policy and associated procedures and guidance and to comply with the expectations set out. Staff are expected to seek

assistance from their line manager with any issues relating to compliance or understanding of the Policy or associated documents.

3. IMPLEMENTATION

In order to comply with the Policy staff must ensure that they have access to and familiarise themselves with this policy and associated procedures and that they understand the responsibilities set out in them.
If individuals are unsure about any aspect of a Policy or procedures they must seek clarification from their line manager, Health Records team or the Information Governance team.
Staff must ensure that they are compliant with all legislation when dealing with Subject Access Requests and any foreseeable problems must be addressed through the proper line management channels.
It is the role of the Chief Finance Officer / SIRO to ratify Trust Corporate policies in respect of IG Policies, taking into account legal and NHS requirements. The board is also responsible for ensuring that sufficient resources are provided to support requirements of this policy.

This Policy should be read in conjunction with:

- Health Records Management Policy & Procedure
- Information Governance Policy & Procedure
- Corporate Records Policy & Procedure
- Health Records Security & Confidentiality Policy
- Clinical Records Keeping Policy
- Sharing/Disclosure of Service User Related Information Policy
- Freedom of Information Policy
- NHS Codes of Practice - Records Management & Confidentiality

All Managers (including IAO's) are responsible for ensuring that the Policy and its supporting standards and guidance are built into local processes and that there is on-going compliance on a day to day basis. Any breaches or suspected breaches of confidentiality or information security including cyber security events must be referred for immediate investigation.

4. COMPLIANCE

Evidence of effective systems for processing subject access requests forms part of the Information Governance Toolkit Requirement 205.

Staff identified as Subject Access Request (SAR) Handlers must receive adequate training from the DPA Administrator in the content of the Policy and its associated procedures and in the use of the Trust Central Register.

The handling of SAR's is reported quarterly to the Clinical Records and Information Governance Group. Reports on compliance are also sent to the Corporate Governance and Compliance Sub Committee.

Annual audit of compliance with the Policy will be planned and carried out by the DPA administrator in conjunction with IAO's which will also support the Information Governance Toolkit Requirement 205.

5. COMMUNICATION

This Policy and associated procedures will be communicated via Meta Compliance. This method will provide a report of how many staff have received and agreed their understanding of it.

The Policy will also be sent out using the Trust weekly news bulletin – The Pulse.

The Policy and other associated documents will be available on the Trusts Policies and Procedures page of the Trust Intranet.

6. MONITORING INTEGRITY OF THE SYSTEM

Updates or changes in legislation or regulation may affect this Policy. Any proposals for changes to the Policy will be carried out with the agreement of the Clinical Records & IG Group which is chaired by the Deputy Caldicott Guardian/Chief Clinical Information Officer.

In addition, the policy will be reviewed as part of a Corporate Policy risk assessment to ensure that the Policy remains fit for purpose and supports compliance with statutory legislation.

The Health Records Lead will be responsible for maintaining this Policy and its associated documents.