Pennine Care
NHS Foundation Trust

DOCUMENT CONTROL	
Title:	**Data Protection and Confidentiality Policy**
Version:	**1**
Reference Number:	**IG002**

Scope:

All Employees and anyone performing duties on behalf of Pennine Care NHS Foundation Trust

Purpose:

The purpose of this policy is to provide guidance to all Trust staff on Data Protection and Confidentiality and to ensure all staff are aware of their responsibilities with regards to confidential information.

This policy sets out the approach to be taken within the Trust to provide relevant groups and the Board with assurance that a robust Data Protection and Confidentiality framework and associated work programme is in place.

Keywords:

Data Protection, Confidentiality, Information Governance, GDPR, CO59, CO4, CO44

Supersedes:

Data Protection Policy – CO59 V4
Confidentiality Policy – CO4 V7
Information Governance Policy – CO44 V6

Description of Amendment(s):

This is a merged policy incorporating the Data Protection Policy, Confidentiality Policy and the Information Governance Policy and updated to reflect GDPR.

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:	23rd of May 2018
Reference:	IG-EIA002
Freedom of Information Exemption Assessment:	
Date approved:	21st of May 2018
Reference:	2018/0734
Information Governance Assessment:	
Date approved:	21st of May 2018
Reference:	
Policy Panel:	
Date Presented to Panel:	21st of May 2018
Presented by:	Paul Byrne
Date Approved by Panel:	21st of May 2018
Policy Management Team tasks:	
Date Executive Directors informed:	19th of June 2018
Date uploaded to Trust's intranet:	24th of May 2018
Date uploaded to Trust's internet site:	24th of 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):

IG003	Access to Health Records Policy
CO87	Information Governance Strategy
HI002	Electronic Mail Policy
CO13	Information Sharing Policy
CO118	Information Risk Management Policy
CO11	Information Security Policy
CO27	Freedom of Information Policy
CO117	Environmental Information Regulations Policy
	Secure Transfer of Information Guidance
	Records Management Suite of policies and guidance
	IT suite of policies and guidance

	Records Management Suite of policies
	IG Requirements for new process and systems
	Health Informatics Suite of Policies
Policy Associated Documents:	
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

Pennine Care NHS Foundation Trust (henceforth referred to as 'the Trust') has a statutory duty to safeguard the information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with the Trust shall misuse any information or allow others to do so.

This Policy forms part of the overarching Information Governance Framework. Information Governance enables organisations and individuals to ensure that information is handled legally, securely, efficiently and effectively.

For the purpose of this policy the term 'all staff' used henceforth includes all employees and contractors including third parties and others authorised to undertake work on behalf of the Trust, staff covered by a letter of authority/honorary contact, volunteers, agency/bank/temporary staff, work place students and work experience recruits.

During the course of their day to day work, many individuals working within or for the Trust will often handle or be exposed to information which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company or other organisation to which this policy applies shall not at any time during the period of their work for, or provide services to, the Trust nor at any time after its termination, disclose confidential information that is held or processed by the Trust.

All staff working for or on behalf of the Trust are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of Data Protection laws, The Common Law Duty of Confidentiality and, for health and other professionals, through their own professional Codes of Conduct.

The Trust understands the need for the strictest confidentiality in respect of data. This applies to manual and computer records and conversations about service users. Everyone working for or on behalf of the Trust is under a legal and common law duty to keep service users information, held in whatever form, confidential and secure. Service users who feel that confidence has been breached may issue a complaint under the Trust complaints procedure or they could take legal action. The Information Commissioners Officer (ICO) can also impose penalties on the Trust, and/or its employees if non-compliance occurs.

It is the policy of the Trust that all processing of personal information by or on behalf of the Trust, whether as Data Controller or as a Data Processor for others, shall be in accordance with current Data Protection laws.

This policy cannot be implemented in isolation as the management of information plays a key part in all areas of the Trust's operations (including but not restricted to) Clinical Governance, Informatics, Service Planning and Delivery and Performance Management

and Intelligence. This policy, therefore, links into all aspects of the organisation and is to be implemented in conjunction with other specific Trust strategies.

2. PURPOSE

The purpose of this policy is to provide guidance to all Trust staff on Data Protection and Confidentiality and to ensure all staff are aware of their responsibilities with regards to confidential information.

This policy sets out the approach to be taken within the Trust to provide relevant groups and the Board with assurance that a robust Data Protection and Confidentiality framework and associated work programme is in place.

3. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

- The Trust Board – The Chief Executive, supported by the Trust Board has overall strategic accountability for Data Protection and confidentiality and any associated work programme, including the maintaining of an appropriate policy and procedure suite and relevant frameworks.

  To fulfil its obligations, the Board has delegated authority for Data Protection and Confidentiality to the Integrated Governance Group, and operationally to the Information Governance Assurance Group.

  The Caldicott Guardian and Senior Information Risk Owner (SIRO) are both members of the Board (see below)

- Senior Information Risk Owner (SIRO) – The SIRO has responsibility for ensuring compliance with legislation and national policy in relation to security of information, in particular person identifiable information.

  The Trust SIRO is the Director of Service Development and Sustainability.

- Caldicott Guardian – The Caldicott Guardian plays a key role in ensuring that the Trust satisfies the highest practical standards for handling patient identifiable information. Acting as the ‘conscience’ of the Trust the Caldicott Guardian also support the work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information, as required.

  The Trust Caldicott Guardian is the Medical Director.

- Line Managers and Senior Managers – All line managers and senior managers have responsibility to ensure that all staff are compliant with and working to all relevant policy and procedures in relation to Data Protection and Confidentiality, and completion of all relevant associated training modules. They also have responsibility for ensuring any incidents or policy breaches in relation to Data Protection and Confidentiality principles are reported immediately.

- All Employees' and anyone performing duties on behalf of Pennine Care NHS Foundation Trust – All staff have responsibilities for Data Protection and Confidentiality on a day-to-day basis, whether they work in a clinical or non-clinical environment. All staff must:
    - Adhere to this policy and all related policies and processes to ensure compliance with Data Protection laws
    - Inform the Data Protection Officer of any new use of personal data
    - Complete annual Data Protection and Confidentiality training
    - Ensure all personal information is accurate, relevant, up-to-date and used appropriately
    - Ensure that personal data is not removed from the Trust premises except where specifically required for the execution of legitimate functions of the Trust
    - Inform the Data Protection Officer immediately of any incident involving the known or suspected loss, damage or misuse of personal information in paper or electronic form. Any incident should also be reported via the Trust incident reporting system.
    - Detailed information and guidance for staff on Data Protection and Confidentiality procedures and processes is available in the Information Governance Staff Handbook available on the intranet.

- Information Governance Manager – The Trusts Information Governance (IG) Manager will ensure the Trust complies with all relevant legislation and NHS Policy in relation to Data Protection laws, Freedom of Information, Records Management, Caldicott, confidentiality and information security.

  The IG Manager shall ensure the function is adequately resourced and report any identified weaknesses or risks to the Trust IG compliance to the SIRO and ultimately the Trust Board.

  The IG Manager is responsible for ensuring the completion of the annual Data Protection and Security Toolkit assessment and management of the Information Governance Assurance Group.

- Data Protection Officer (DPO) – The Data Protection Officer (DPO) function for the Trust will be performed by the Information Governance Manager, supported by the Information Governance Department. The DPO will act as a central point of contact for

Data Protection within the Trust ensuring the Trust complies with all Data Protection laws and appropriate policies, procedures and practices are formulated and adopted by the Trust. They will ensure all actual or suspected breaches of Data Protection law and confidentiality are managed according to national procedures, monitored and reported to the appropriate group/committee.

- Records Manager – The Trusts Records Manager is responsible for the overall development and maintenance of records management practices throughout the organisation. In particular, the Records Manager is responsible for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

- Privacy Officer – The Trust has a dedicated Privacy Officer who is responsible for monitoring system access, including Paris and Summary Care Record, for any inappropriate access. This is done via regular auditing and spot checks of access and 'break glass' processes. Any inappropriate access will be investigated and escalated as applicable.

- Information Asset Owners (IAOs) – The Trusts Information Asset Owners (IAOs) support and drive the information governance agenda and provide the Trust Board – via the SIRO – with the assurance that effective information governance best practice mechanisms are in place within the Trust.
  The IAOs are Board level/Director/very senior management level members of staff who have overall accountability for the assets within the services under their remit. They will assist in identifying strategic threats and vulnerabilities, both internally and externally, to their services and will advise on the impact of such risks would have at a strategic level.
  They will also ensure information risk assessments are reviewed each quarter on all information assets where they have been assigned ownership. The IAO will report directly to the SIRO and will be responsible for nominating appropriate Information Asset Managers for each information asset.

- Information Asset Manager (IAMs) – Information Asset Managers (IAMs) are Service/Departmental Manager level staff and will coordinate the identification of information assets within their remit and will assign an Information Asset Administrator for each asset.

  The IAM will have a thorough understanding of their information assets; their importance to the organisation, their links and dependencies on other assets, tactical

threats and vulnerabilities facing the assets and the direct and indirect impact these risks would have on the Trust.

The IAM will nominate an appropriate Information Asset Administrator (IAA) for each asset.

- Information Asset Administrators (IAAs) – The Trusts Information Asset Administrators (IAAs) can be any member of staff with an in-depth knowledge of the asset and data flows, ideally Operational Manager (e.g. supervisor or team leader), but can be any officer, as appropriate. The IAA will have a thorough understanding of how the asset is used on a day-to-day basis, and how and when information is added and removed from the asset.

  IAAs ensure that policies and procedures are followed regarding the asset. They will proactively and reactively recognise actual or potential security incidents, and will consult their IAO/IAM regarding incident management. They will assist in the identification of threats and vulnerabilities within the asset, documenting the flow of their assets, and in determining the value of the asset.

4. LEGAL COMPLIANCE AND AWARENESS

The Trust regards all identifiable personal information relating to service users or staff as confidential

It is important to the Trust to protect its legitimate business interests and in particular its confidential information. Breaches of confidentiality, of any sort, may result in legal action taken against the organisation and/or the individual and could result in disciplinary action

If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, they must report it immediately to their line manage and complete an incident form

Everyone in the Trust must be aware of the importance of confidentiality. All staff need to be aware of their responsibilities for safeguarding service user confidentiality and keeping information secure

The duty of confidentiality is written into employment contracts. Breaches of confidentiality of any type are a serious matter and is a disciplinary offence which could result in dismissal and/or prosecution

It is a disciplinary offence to access records/information that you have no legitimate reason to view; this includes records about yourself, your family, friends, neighbours,

acquaintances etc. If you do not have a legitimate reason to access, do not browse. All transactions are auditable

The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements

The Trust will establish and maintain policies to ensure compliance with the following:

- Data Protection laws
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Caldicott Principles
- Freedom of Information Act 2000
- The Public Interest Disclosure Act 1998
- The Computer Misuse Act 1990
- Access to Health Records Act 1990
- Environmental regulations
- Regulation of Investigatory Powers Act
- Department of Health guidance

5. WHAT IS PERSONAL CONFIDENTIAL DATA / INFORMATION?

Personal Confidential data/information is anything that contains the means to identify a person e.g. name, address, postcode, data of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Information that identifies individuals personally must be regarded as confidential, and should not be used without a justifiable and legal purpose

Whenever possible, anonymised data, that is where all personal details have been removed and which therefore cannot identify the individual, should be used

Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent

Confidential information may also include sensitive personal information (as defined in Data Protection laws) regarding race, health, sexuality etc.,

Confidential information is subject to the same requirements regardless of the medium they are stored on.

6. CONDUCT

All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of personal confidential data

- Ensure the physical security of all confidential documents and/or media, including storage of files on PCs.
- Never leave confidential information unattended and must keep it secure when not in use
- Only use authorised Trust equipment to process personal confidential data, which is encrypted to national standards
- Comply with password guidance by not disclosing passwords to anyone, including colleagues
- Have due regard for Data Protection laws
- Comply with this policy whilst working with the Trust and thereafter for as long as the information remains personal confidential data.

Detailed information on Data Protection and Confidentiality procedures and processes is available in the Information Governance Staff Handbook which is available on the intranet

Individuals shall not be restrained from using or disclosing any confidential information which:

- They are authorised to use or disclose by the Trust
- Has entered the public domain unless as a result of an unauthorised disclosure
- They are required to disclose by law
- They are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regard to the provision of the Act

7. DATA PROTECTION LAWS

From 25th May 2018, the European General Data Protection Regulation will be translated into UK law by the Data Protection Bill.

This, and all Trust policies or other relevant documentation and processes that have any purpose or content that is effected by data protection laws, will be bound by the requirements of the law as established in the UK.

8. TRAINING & AWARENESS

The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of Data Protection laws and their obligations. This will be carried out by the mandatory Information Governance training. All new staff will be required to complete the Information Governance training as part of their induction.

All staff are mandated to undertake annual Information Governance training

Where staff have specific roles in the Trust i.e. Caldicott Guardian, SIRO, IAO etc., additional Information Governance training will be required.

Additional training will be made available to all staff, where it is required e.g. for staff handling health records. Further guidance is available in the Information Governance Training Plan

To maintain high staff awareness, for Data Protection and confidentiality staff will be directed to a number of resources:

- Policy, Strategy and Procedures
- Manuals
- Specific training courses
- Other communication methods e.g. monthly staff bulletin, team meetings and information available on the staff intranet

9. INFORMATION GOVERNANCE STAFF HANDBOOK

Detailed information covering all Data Protection and Confidentiality procedures and processes is available on the intranet, for all staff, in the Information Governance Staff Handbook.

The handbook aims to provide an overview of all the key legislation and national guidance regarding Data Protection and Confidentiality, which is referenced throughout the document.

Help and guidance is available in the Handbook to enable staff to establish working practices that effectively deliver the patient confidentiality that is required by law, ethics and policy.

10. 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

11. 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.

12. 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.

13. 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.

14. 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.

15. REVIEW

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

16. REFERENCES

Information Governance Manager
Pennine Care NHS Foundation Trust HQ
225 Old Street, Ashton under Lyne, OL7 6SR
0161 716 3225
pcn-tr.ig@nhs.net

Data Protection Officer

Pennine Care NHS Foundation Trust HQ address as above
pcn-tr.dpo@nhs.net

Further information is available at: https://www.penninecare.nhs.uk/about-us/accessing-information/information-sharing/how-we-use-your-information/