DATA PROTECTION & CONFIDENTIALITY

1. INTRODUCTION

1.1. Rationale

Partnerships in Care (PiC) maintains many records containing personal information and the duty of confidence and other legislation, especially the Data Protection Act 1998 apply equally to these records (e.g. service user records, staff records, complaints records, forms etc.).

PiC is committed to following the patient confidentiality model as described in the NHS Confidentiality Code of Practice:

- Protect – look after the patient's information;
- Inform – ensure that patients are aware of how their information is used
- Provide choice – allow patients to decide whether information can be disclosed or used in a particular way and,
- Improve – always look for better ways to protect, inform and provide choice.

This policy should be implemented within the context of PiC Values:

- Valuing people – respecting our staff, patients, their families and communities
- Caring safely – for ourselves, our patients, our customers and communities
- Working together with everyone
- Uncompromising integrity, respect and honesty
- Taking quality to the highest level

The purpose of this policy is to lay down principles that must be observed by PiC staff and who have access to person-identifiable information or confidential information.

PiC has a legal duty to data subjects e.g. patients, carers and staff, to protect personal information, inform them how information is being used, of their rights to access information and where appropriate seek consent before disclosing to other parties.

This means ensuring all personal information is processed lawfully, fairly and transparently, so that they:

- Understand the reason for collecting, storing and sharing personal information (processing)
- Give consent for the use and disclosure of personal information (where applicable)
- Have confidence in the way PiC handles personal information
- Understand their rights, including the right to access information held about them or the right to give consent to others to access this information on their behalf

1.2. Scope

All employees (substantive, agency, and contractor, temporary, those in partnership / under contract or volunteers) are bound by a legal 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 within the common law duty of confidence and the Data Protection Act 1998.

This policy sets out requirements placed on staff when sharing information for Healthcare and between NHS and non NHS organisations. This would also include all personal staff and business information that is of a confidential nature. It also reinforces responsibilities of Information Asset Owners and their requirement to ensure confidentiality within their systems.

1.3. Principles

PiC always works on the basis that sharing information to support patient care and to prevent risk to data subjects or others is essential. It is not acceptable that the care a patient receives might be undermined because organisations providing health and care to an individual do not share information effectively. Sharing personal information effectively is a key requirement of good information governance and Health and social care professionals should have the confidence to share information in the best interests of their patients.

Caldicott Principle 7: *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 patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.*

People should feel confident that health and social care bodies handle confidential information appropriately. PiC will always respect the confidentiality of service users, families, carers, current and ex-employees and other third parties and not disclose personal information without consent, unless there is a legal basis to allow the sharing, if there is an overriding public interest (e.g. to prevent a serious crime), or if there are reasons to believe that failing to share information could put someone at risk. Individuals will never be placed at potential risk through a lack of information sharing.

An individual may express an objection to uses of his/her personal information on occasions. Such objections may limit the use of their information for certain purposes. However, there are other purposes for which an individual does not have a right to prevent data about them being used, for example, the use of personal data to prevent the spread of infection of notifiable diseases and to prevent further outbreaks in future or for the prevention of a serious crime.

All staff must ensure service user information is processed fairly, lawfully and as transparently as possible. All staff have a responsibility to meet the standards outlined in this policy in accordance with the standard terms and conditions of their employment.

All staff must ensure the following principles are adhered to:

- Person-identifiable / confidential information must be protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable / confidential information must be on a need-to-know basis.
- Disclosure of person identifiable / confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Comply with the Duty of Candour – the general duty to act in an open and transparent way in relation to care and treatment provided to service users.

2. POLICY

2.1 Overview

Any breach of this Policy could jeopardise the confidentiality of service users and the security of clinical information, and could breach the Data Protection Act (1998).

Breaches will be reported as incidents and will be managed in line with PiC's incident reporting procedures. They will be investigated locally, supported by the Information Governance Team and may lead to disciplinary action against staff or penalties against the Organisation by the Information Commissioner's Office.

Confidential information should be used for healthcare purposes and unless appropriate circumstances are present, can only be disclosed with the informed consent of the patient. Where the patient lacks capacity and is unable to consent, information should only be disclosed in the patient's best interests. Possible circumstances for disclosure of information when the service user had capacity are when statute law requires us to do so, when there is a court order and when disclosure may be necessary in the public interest.

All requests to access records should be processed by following the PiC Operational Policy – *Access to Health Records*.

2.2 Definition of Terms

For clarity there are a number of terms that PiC will adopt in relation to Confidentiality. These are explained in section 8 of the policy.

2.3 The 8 Data Protection Principles

The 8 principles of the Data protection Act states that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes (e.g. Healthcare)

3. Adequate, relevant and not excessive
4. Accurate and up-to-date
5. Not kept any longer than necessary
6. Processed in accordance with the rights of the data subject
7. Protected by appropriate security (practical and organisational)
8. Not transferred outside European Economic Area without adequate protection

3. PROCEDURE – ACHIEVING THE POLICY

3.1 Records / Information covered

This policy covers all records / documents that contain personal or confidential information. Confidential information within the NHS is commonly thought of as health information; however, it can include information that is private and not public knowledge or information an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes PiC confidential business information.

PiC will also apply the duty of confidence to clinical records of deceased clients, as suggested by NHS guidance.

3.2 General Responsibility for Confidentiality

All employees (substantive, agency, and contractor, temporary, those in partnership / under contract or volunteers) are responsible for maintaining the confidentiality of information whilst working within PiC and after they have left the Organisation.

Staff must only access personal information if they have a genuine 'need to know / legitimate reason'. Unauthorised access or use of information will be investigated and may lead to disciplinary action and could be actioned under the Data Protection Act.

Everyone working for PiC should be aware of their responsibilities in order to comply with law (including the Caldicott Principles).

All staff must ensure they know of, understand and apply recommended practical measures to maintain confidentiality when obtaining, sharing, storing or disposing of personal information in different communication forms. PiC has a number of procedures and guidance document for staff which are available on the Intranet.

3.3 Training

IG training must be completed in line with the Training Programme for all staff and more specific training can be requested via the Information Governance Lead.

3.4 Information Collection

- As soon as an individual is accepted as either a potential service user or employee, records must be created. Staff are responsible for keeping these records accurate, up-to-date, and confidential and ensuring they are not shared outside the Organisation unless required to do so.

- On initial contact with PiC the patient must be given information, *orally* and in writing, explaining the Organisations requirement to keep records, how these may be shared and service users' rights to access their information.
- Lead Clinicians must periodically discuss information recording and sharing with patients to confirm understanding, identify any issues and note if consent to share information is not given (we must record consent). All such discussions must be documented in CAREnotes. Some service users (e.g. employees, relatives of employees or professionals who may be in contact with the Organisation in their professional capacity) may feel the need to ensure their records are further protected from unauthorised access by requesting their details to be anonymised. Such requests need to go through an anonymisation procedure and be authorised by the Caldicott Guardian and SIRO.

3.5 Keeping Patients Informed

It is neither practicable nor necessary to seek the consent of a patient or other informants each time there is a need to share personal information. **Therefore, patients, carers and family (as appropriate) need to be fully informed to the best of our ability of how the information which they give may be used at their first appointments. This will be achieved in a number of ways:**

- PiC will inform patients of the purposes for which information is collected, and the categories of people / organisations information may need to be passed on to. This can be achieved by a patient information leaflet being available, publicity materials are not considered sufficient on their own and all staff are responsible for ensuring that patients are made aware of the potential to share information.
- Where information is required to be shared, patients are to be advised before they are asked to provide it, and should have the opportunity to discuss any aspects that are special to their treatment or circumstances.
- Advice must be presented in a convenient form and be available both for general purposes and before a particular programme of care or treatment begins. In cases of multi-agency working for example, integrated health and social care teams, explicit consent may be required via a consent form. Consent is not always required however, e.g. if there is an actual / perceived risk or safeguarding concerns.

There is a general duty on all health service bodies to act in an open and transparent way in relation to care and treatment provided to service users. This Duty of Candour is an NHS Standard Contract contractual duty, and encompasses the principles of openness and transparency.

3.6 Secure Transfer of Personal Identifiable Information

All transfers of personal identifiable information are subject to strict governance and technical security controls. All staff intending to undertake in-bound and/or out-bound personal identifiable information transfers must ensure it complies with all PiC policies including the *Computer Use & Security Policy*.

Staff must consider:

a) What information is to be transferred (only transfer minimum information required for the purpose)
b) Purpose of transfer
c) Nature of recipient
d) Method of transfer (e.g. is the email secure?)
e) Physical and technical security measures proposed by the sender and the recipient

3.7 Requests for Access to Information

Data subjects have the right of access to their own personal information. These rights are embodied within:

- The Data Protection Act 1998 – entitles individuals to a copy of personal information held about them (both manual and automated)
- Access to Medical Reports Act 1988 – in respect of reports prepared for employment or insurance purposes
- The Human Rights Act 1998 – the means by which certain 'rights and freedoms' contained in the European Convention of Human Rights have become a direct part of UK law
- Access to Health Records Act 1990 – for applications relating to deceased persons only, right of access are to manual health records made after 1 November 1991 and earlier records if they are necessary to understand the later ones

PiC will always work on the principle of being open and accountable and look to share as much information with service users, the public etc as possible.

Individuals, or an appointed representative, have a right to request copies of personal data (e.g. staff records, clinical notes, complaints) under Data Protection Act. We have a duty to check the validity of requests and once confirmed are legally required to respond within 40 calendar days. Information on how to deal with requests is detailed in the PiC Operational Policy – *Access to Health Records* and can be found on the Intranet. In the first instance, all such requests must be directed to the Local MHA Team.

Where a request to disclose personal information has been received and is considered appropriate, the decision to disclose, what to disclose and the reasons for this decision must be recorded. The current / most recent clinician in charge for a patient or line manager for a staff member has responsibility for determining what information is disclosed- they are required to ensure the information is reviewed prior to disclosure and that no inappropriate information is released.

Guidance is available on reviewing records and the organisation process will ensure actions are monitored and logged for evidential purposes. When a patient gives consent to disclose information about themselves, clinicians should make sure that the patient understands what will be disclosed, the reasons for the disclosure, the likely consequences and record this information on CAREnotes.

If it appears a patient does not have capacity to consent to sharing of information, clinicians should carry out a formal assessment of capacity, recording this on CAREnotes. If the test demonstrates a **lack of mental capacity** the clinician must ensure nobody else has a right to make the decision (a done of lasting power of attorney for welfare decisions or a Court of Protection appointed deputy). If there is nobody authorised to make the decision for the patient, the clinician should make a decision in the patient's best interests and record this decision on the appropriate form and on CAREnotes.

3.8 Regular Sharing

The Organisation must agree an **Information Sharing Protocol** / contractual arrangement with any partner organisation where it is anticipated regular information sharing will be required for personal data. This does not need to happen if the sharing is already covered as part of a contract.

The protocol will lay down the principles under which information can and should be shared, how the information will be shared (e.g. hard copy, electronic), security, and details of the information to be shared in line with legislation.

Staff being asked to release service user information must be familiar with the relevant protocol and only release the minimum information required to fulfill the obligation and meet the request, in line with the arrangements in the protocol. Protocols will recognise that the duty to share information can be as important as the duty to protect confidentiality and provisions exist to allow sharing in all appropriate circumstances.

Where an information sharing request is received from an agency with whom PiC has no information sharing protocol the requests must be passed to the Head of Information Management who will determine if there is a valid / legal reason to disclose and acceptable conditions at the receiving organisation, consulting with Clinicians where appropriate. Any disclosure must only be made in line with this policy.

3.9 Transferring Information Securely

Where personal identifiable information needs to be shared electronically safeguards must be in place to ensure confidentiality (e.g. use of NHS.net (secure email) or encrypted devices). Advice is given in the PiC Operational Policy – *Computer Use & Security*.

3.10 Disposing of Confidential Information

Disposal of records must be in accordance with the NHS Records Management Code of Practice and the PiC Operational Policy – *Document Retention*.

Where confidential information needs to be disposed, care must be taken to ensure it is destroyed safely so that confidentiality is not breached and that the decision to destroy is recorded in the destruction register (if advice is needed please speak to the Medical Records Coordinator).

Disposal of confidential information on magnetic media (e.g. CDs, DVDs, memory

sticks) must follow IT Department procedures.

3.11 Handling of Confidentiality Breaches / Incidents

Any incident involving the actual or potential loss of personal and/or confidential information, should be considered as serious and should be logged within 24 hours of notification. All incidents and issues which may include a breach of confidentiality and/or information security must be recorded on the incident system in a timely manner.

Breaches will be reported to and reviewed by IG Team as well as the SIRO, the DPA Lead and the Caldicott Guardian, who will ensure appropriate actions are taken to minimise the risk of such incidents reoccurring. Nominated senior managers will formally investigate serious breaches and where appropriate use the PiC Disciplinary Procedure.

Staff who breach their duty of confidentiality may be subject to disciplinary action which could lead to dismissal.

3.12 Children and Young People

Young people aged 16 or 17 are regarded as adults for purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults.

Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are entitled to decide whether personal information may be passed on and generally to have their confidence respected (for example, they may be receiving treatment or counselling about which, they do not wish their parents to know). However, the child should be encouraged to involve parents or other legal guardians.

In other instances with regard to children, decisions to pass on personal information may be taken by a person with parental responsibility in consultation with the health professionals concerned.

Under the Children Act 2004 key people and bodies have the duty to make arrangements which ensure their functions are discharged with regard to the need to safeguard and promote the welfare of children. This extends to the member agencies of the LSCB and services they commission. Information sharing is fundamental for complying with this statutory regulation. Child protection is an area where information may be shared without the consent of the child or their parent. In child protection cases, if the health professional (or other member of staff) has knowledge of abuse or neglect relevant information will be shared with others on a strictly controlled basis so that decisions regarding the child's welfare can be taken in the light of all relevant information.

When information regarding an individual indicates that a child may be at risk from that individual there is a duty to share that information with the appropriate agency.

3.13 Complaints

Complaints from patients regarding confidentiality of their information will be dealt with

through either the PiC Operational Policy – *Complaints Policy & Procedure* or the health professionals' administrative bodies, with support from the Information Governance Team. PiC will support the statutory right of patients to complain to the Information Commissioner, as well as rights to take action for compensation if the individual has suffered damage (physical and/or mental) as a result of the breach of confidentiality. Also, to have any inaccurate personal information corrected or erased.

3.14 Passing of Information for Relatives, Friends and Carers

PiC will, where possible, support the patient's wishes for disclosure of information to relatives, friends and/or carers in line with the guidance outlined in the NHS Confidentiality Code of Practice. Carers may also have to be informed, for example, to make arrangements for continuing care on discharge from hospital.

In this context, the term 'carers' relates not only to a patient's family or friends who may assist and provide care to the patient on a regular basis but can also refer to the healthcare team who are at that time, involved in caring for the patient and may therefore be given information about a patient unless the patient has indicated otherwise. Explicit consent should be sought wherever possible and the individual's wishes recorded in CAREnotes.

3.15 Research

- Research records should be subject to the same rigour regarding confidentiality as clinical records.
- The patient's hospital number should be used for identification purposes and for staff, each individual should be given a special numeric code and the coding sheet kept locked and separate from any paper copy that might be made.
- It is not permitted for research data to be transferred on a memory stick or disc for subsequent interrogation outside of the host institution.
- It is a mandatory requirement that the research supervisor informs the supervisee of the obligations for the proper collection and storage of confidential data and that the supervisee signs an undertaking before the project commences that these will be adhered to. The research supervisor will also periodically audit this.

3.16 Clear Desk

PiC implements 'clear desk' this means that all staff should ensure that when they are not at their desks there is no confidential information on display and that all relevant processes and procedures have been implemented to ensure that confidential information is secure.

3.17 Non-Displaying of Confidential Information

PiC implements non-displaying of confidential information, please ensure that all areas adhere to this and that there is no confidential information on display.

3.18 No Printing from Non-Networked Printers

All staff should only print to network or PiC authorised printers. If you feel you need to print to a printer that is not connected to a network an individual request needs to be

put into IT Helpdesk.

4. ROLES AND RESPONSIBILITIES

4.1 Caldicott Guardian

The Executive Medical Director is the Caldicott Guardian. The Caldicott Guardian has accountable for the safe management of patient data. However each member of staff is responsible for patient confidentiality.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is the Director of Information Management and Assurance, and a mandated role which has overall responsibility for managing information risk across PiC. The SIRO is a member of the Executive team and is assisted by:

- The Data Protection Lead
- The Information Governance Lead
- The Director of IT
- The Caldicott Guardian

4.3 Information Governance Lead

This role will lead the Information Governance agenda for PiC and is managerially accountable to the Director of Information and Assurance. They will have day to day operational responsibility for all aspects of Information Governance.

4.4 Managers

It is the responsibility of managers and supervisors of temporary staff, students and contractors who have access to sensitive personal information to ensure staff are aware of the need for confidentiality under the Data Protection Act 1998 and complete annual IG training. Any staff who are not covered by a PiC employment contract should sign a confidentiality agreement.

4.5 Information Asset Owners

Information Asset Owners (IAO) are individuals involved in running / administrating relevant systems - asset. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law and confidentiality and provide written input to the SIRO on the security and use of their asset.

4.6 All Staff

- All members of staff must be aware of the confidential nature of their work and sensitive information they may come across. All staff are provided with an introduction to Information Governance standards during their corporate induction and are expected to familiarise themselves with organisational policy in relation to these issues.

- All staff are required to undertake mandatory information governance training on an annual basis.
- A breach of confidentiality may result in disciplinary action in accordance with the disciplinary policy and is seen as a serious offence which will be treated as gross misconduct and could result in dismissal (see PiC Human Resources Policy – *Disciplinary*).

5. REFERENCE DOCUMENTS

- Common Law of Confidentiality
- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 200
- Access to Health Records Act 1991
- Computer Misuse Act 1990
- Caldicott Review 2013
- Confidentiality NHS Code of Practice 2003 (and supplementary guidance dated November 2010)
- Confidentiality: Protecting and Providing Information (GMC 2004)
- Mental Capacity Act 2005
- NHS Act 2006

APPENDIX A

SUPPORTING INFORMATION

Caldicott Principles for handling personal confidential data:

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate Guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes. Healthcare organisations should be aware of the research conducted within the organisation, and should ensure research teams are accountable to them (from MRC Executive Summary – Personal Information in Medical Research).

5. Everyone with access to personal confidential data should be aware of their responsibilities

The organisation must ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Understand and comply with the law

Every use of personal confidential data must be lawful. The Caldicott Guardian (Executive Medical Director) is responsible for ensuring PiC complies with legal requirements.

7. 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 patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators & professional bodies.

APPENDIX B

DATA PROTECTION CONSIDERATIONS

The Data Protection Act 1998 provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing information and the Act applies to all forms of media, including paper and images.

The Data Protection Act prohibits processing unless conditions set out in two particular schedules are met. Schedule 2 conditions apply to all processing whereas Schedule 3 provides additional and more exacting conditions that only apply to the processing of sensitive personal data, such as health information.

You can find full copies of both schedules within the Data Protection Act.

It is important to understand the role of consent in relation to these schedules. Whilst consent is one of the conditions in each Schedule that might be satisfied, only one condition in each Schedule needs to be satisfied and NHS bodies processing personal health information for legitimate medical purposes may satisfy a condition in each Schedule without needing to obtain patient consent. Note however that, in addition to these schedules, there is a general requirement, within the Data Protection Act 1st principle, for all processing to be lawful. This includes meeting common law confidentiality obligations, which are likely themselves to require consent to be obtained. The Data Protection Act provides a comprehensive framework of required good practice that extends far wider than confidentiality. Requirements include notification (formerly registration) with the Information Commissioner, commitment to data quality, effective information security and the extension of a range of rights to patients. More information on the Act's requirements can be found at www.informationcommissioner.gov.uk.

APPENDIX C

SCHEDULE 1 THE DATA PROTECTION PRINCIPLES: PART 1 – THE PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) At least one of the conditions in Schedule 2 is met, and
   (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.