Clinical Partnership
SPECIALIST COMMUNITY CARE

Information Governance

Data Protection Confidentiality Policy

Policy Reference: CP/IG/DPC V2

Policy Title	Data Protection and Confidentiality Policy	
Author/Contact	Holly Hellstrom – Information Assurance Manager	
Document Ref	CP/IG/DPC	
Version	2	
Status	Approved	
Publication Date	October 2020	
Review Date	September 2022	
Approved by	Dr James Britton Caldicott & Dr Javed Mohungoo IG Lead	6th October 2020
Ratified by	Information Governance Team	6th October 2020

Version	Date	Comments	Author
1	10/5/2018	Approved by IGT	Information Assurance Manager
2	6/10/2020	Approved by IGT	Information Assurance Director

Contents

Introduction and Aims

The purpose of this Policy is to provide guidance to all Clinical Partnership (CP) employees on Data Protection.

Clinical Partnership (CP) has a duty to safeguard the confidential 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 Clinical Partnership (CP) shall misuse any information or allow others to doso.

During the course of their day to day work, many individuals working within or for Clinical Partnership (CP) 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 they work for or provide services to Clinical Partnership (CP) nor at any time after its termination, disclose confidential information that is held or processed by the company.

All staff working in Clinical Partnership (CP) 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 the General Data Protection Regulation (henceforth referred to as GDPR) and, for health and other professionals, through their own professions' Codes of Conduct.

Clinical Partnership (CP) understands the need for the strictest confidentiality in respect of data. This applies to manual and computer records and conversations about service users' treatments. Everyone working for Clinical Partnership (CP) including temporary staff and contractors is under a legal and common law duty to keep service users' information, held in whatever form, confidential.

The Information Commissioners Office (ICO) can impose penalties upon the Clinical Partnership (CP), and/or Clinical Partnership (CP) employees if non-compliance occurs.

Confidentiality can only be overridden in exceptional circumstances and with the appropriate justification and be fully documented.

Clinical Partnership (CP) will ensure that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that the public can:

- Understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information where necessary;
- gain trust in the way the company handles information; and
- understand their rights to access information held about them.

It is the policy of Clinical Partnership (CP) that all processing of personal information by or on behalf of Clinical Partnership (CP), whether as a Data Controller or as a Data Processor for others, shall be in accordance with the requirements of:

- The General Data Protection Regulation
- Clinical Partnership (CP) Policies and Procedures in relation to the protection and use of personal information;
- processing personal information for deceased patients;
- the Access to Health Records Act 1990 and any subsequent amendments and statutory instruments.

The aims of this policy are:

- To safeguard all confidential information within Clinical Partnership (CP)
- to provide guidelines for all individuals working within the organisation;
- to ensure a consistent approach to confidentiality across Clinical Partnership (CP)
- to ensure all staff are aware of their responsibilities with regards to confidential information;
- to provide all individuals working within Clinical Partnership (CP) access to the documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them. These include:

    - the common law Duty of Confidentiality;
    - Caldicott principles;
    - General Data Protection Regulation;
    - Freedom of Information Act 2000;
    - Human Rights Act 1998;
    - Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures";
    - The Public Interest Disclosure Act 2013;
    - The Computer Misuse Act 1990.

Scope

This policy supersedes CP data protection policy and applies to those members of staff that are directly employed by Clinical Partnership (CP) and for whom Clinical Partnership (CP) has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of Clinical Partnership (CP). Further, this policy applies to all third parties and others authorised to undertake work on behalf of Clinical Partnership (CP).

For the purposes of this policy, confidential information shall include any confidential information relating to Clinical Partnership (CP) and/or its agents, customers, prospective customers, suppliers or any other third parties connected with the company and in particular shall include, without limitation:

- Service user information;
- ideas/programme plans/forecasts/risks/issues;
- trade secrets;
- business methods and business design;

- finance/budget planning/business cases;
- prices and pricing structures;
- sources of supply and costs of equipment and/or software;
- prospective business opportunities in general;
- computer programs and/or software adapted or used;
- policy advice and strategy;
- corporate or personnel information; and
- contractual and confidential supplier information.

This is irrespective of whether the material is marked as confidential or not

The Current Data Protection Act / General Data Protection Regulation

The Data Protection Act 2018 (DPA 2018) incorporates GDPR and brings the requirements of GDPR into UK law. As with the repealed Data Protection 1998, the new Data Protection Act 2018 protects the use of information that identifies individuals.

Under the Data Protection Act 2018 the data protection principles set out the main responsibilities for organisations.

There are 6 principles outlined below:

• Personal data must be processed lawfully, fairly and in a transparent manner in relation to individuals;
• Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
• Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
• Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
• Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures
required by the GDPR in order to safeguard the rights and freedoms of individuals;
• Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The most significant addition is the accountability principle. The Data Protection Act 2018 requires organisations to show how they comply with the principles – for example by documenting the decisions taken about a processing activity.

The Data Protection Act 2018 applies to all personally identifiable information regardless of the form in which it is held, for example; information held within computer databases; videos and other automated media; personnel and payroll records; medical records; manual files; microfiche/film; pathology results; x-rays etc.

The Data Protection Act 2018 only applies to living individuals, however, the Common Law Duty of Confidentiality extends beyond death and we therefore respect the rights of the deceased in the event of processing a deceased person's personal information.

The Data Protection Act 2018 dictates that information must only be disclosed on a need to-know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner. Staff must not disclose information outside legitimate reasons for disclosure.

Any unauthorised disclosure of information by a member of staff will be considered a disciplinary offence.

Individuals Rights

Within the Data Protection Act 2018 the individual to whom information relates is referred to as the 'Data Subject'. The Data Subject has the following rights through the Data Protection Act:

- The right to be informed (through the use of privacy notices)
- The right of access (confirmation that the data subject's information is being processed, access to their personal information, other supplementary information relating to the use of the personal information, who it is shared with, the retention periods and information on how to complain about the use of the data)
- The right to rectification (if information is inaccurate or incomplete)
- The right to erasure (subject to conditions)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased service user's records.

The right to prevent processing for the purposes of direct marketing.

Under the Act, a data subject can prevent processing of their information, such as asking for addresses / telephone numbers to be deleted from marketing lists.

The right to take action for compensation if the individual suffers damage.

If an individual suffers damage as a result of the disclosure of information, for example comments made about treatment undertaken, and then the data subject may bring an action against the person who made the disclosure.

The right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

Consent to process service users' identifiable information for anything other than direct care must be sought from the data subject.

Valid consent is central in all forms of healthcare, from using information to undertaking major surgery.
"Consent" is a service user's agreement for a process to be undertaken, whether this be the sharing of information or the provision of care. For the consent to be valid, the service user must:

- be competent to take the particular decision;
- have received sufficient information to take it; and
- not be acting under duress.

Consent can be written, verbal, or implied (implied consent can only be used in the context of the delivery of direct care by a member of the care team).

Where an adult service user lacks the mental capacity (either temporarily or permanently) to give or withhold consent for themselves, no-one else can give consent on their behalf**.**

Service Users can make advance statements and/or directives regarding giving or withholding consent should they lack the mental capacity (either temporarily or permanently) at some point in the future to do so.

When seeking consent on behalf of children, a child's capacity to decide whether to consent to or refuse proposed investigation must be assessed prior to consent being sought. In general, a competent child will be able to understand the nature, purpose and possible consequences of the proposed investigation or treatment, as well as the consequences of non-treatment. The following should be considered in this instance:

- at age 16 a young person can be treated as an adult and can be presumed to have capacity to decide;

- under age 16 children may have capacity to decide, depending on their ability to understand what is involved (according to Fraser Ruling, (formerly Gillick Competency), whereby a child under 16 is of sufficient maturity to understand the treatment and risks and is able to make a valid consent to treat).

Explicit consent must always be sought from the service user in order to use their personal information in ways that do not directly contribute to or support the delivery of their care.

Remote Working / Remote Access

If there is a business need that remote access to organisation systems is required approval for this, must be sought from your line manager and arranged with the IT service provider through the HR dept. Employees must adhere to the company policies and procedures in regard to Mobile Working.

Any staff members that process identifiable information on mobile devices in order to perform their role (e.g. when working from home or within the community) must obtain Caldicott Approval*. (This does not apply to those members of staff who only record information they create when they treat Service Users in the community).*

The purpose of the agreement is to highlight potential risks, such as mobile devices being lost, stolen or damaged, and minimising those risks as far as possible and provides a documented record of the use of Service User's information.

Handling Health Records and Confidential Information

The handling of Health Records and Confidential information must be conducted with care and in line with organisation Policy and Guidance relating to Information Security, Health Records etc. Health Records and Confidential Information must be disposed of in accordance with the organisation's Lifecycle policy, located on the SharePoint

External Bodies Working Within the Organisation

The organisation and those carrying out functions on behalf of the organisation have a common law duty of confidence to service users and a duty to support professional and ethical standards of confidentiality. It is the responsibility of the organisation to ensure that outside organisations are aware of and agree to the requirements of maintaining confidentiality through contractual obligations.

Any companies contracting services to the organisation must sign an undertaking to confirm that they understand and accept their responsibility to maintain confidentiality.

Managers or health professionals who are responsible for any secondee / work experience placement should ensure that all individuals understand and comply with organisation's confidentiality guidelines.

Awareness Training

All new starters to the organisation are required to read the Information Governance & Data Security polices and undertake the mandatory Data Security and Protection E-Learning as part of the induction process. Additional training in these areas will be given to those who require it, subject to their roles and responsibilities.

All Line Managers must ensure that their staff, whether administrative or medical are adequately trained and adhere to the appropriate policy and guidance.

Roles, Responsibilities and Accountabilities

Caldicott Guardian

The Caldicott Guardian will act as the conscience of the company and oversee all disclosures of patient information with particular attention being paid to extraordinary disclosures.

Information Assurance Director

As a small organisation our IAD acts as our DPO, they are required as part of the changes to the DPA under the regulation of GDPR. The DPO's role is to inform and advise the company and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition, they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Senior Information Risk Owner (SIRO)

The SIRO, under delegated authority will oversee compliance with the DPA/GDPR and the development of appropriate policy and procedure. The SIRO will be advised by the Information Governance Lead and supported by Information Governance Team. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.

Information Asset Owners (IAOs)/Administrators (IAAs)

Under the responsibility of the SIRO:

- Information Asset Owners (IAOs) will be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
- will ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
- will be responsible for the Information Asset assigned to them;
- will ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a SAR;
- will ensure that personal data held in the Information Asset is maintained in line with the company Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.

Line Managers

- All line managers have a responsibility to ensure that their staff are compliant with, and working to, all relevant policy and procedure in relation to the DPA / GDPR;
- where a breach of policy/procedure or near miss occurs, line managers will need to comply with the company Incident Management processes;
- line managers will ensure that anyone providing a service on behalf of the company (directly employed and contractors) completes a confidentiality statement before commencing employment.

All Staff (refers to all CP employees including contractor/temporary staff and workplace students):

- Should adhere to this policy and all related Information Assets and processes to ensure compliance with the DPA / GDPR;
- are subject to DPA / GDPR compliance and accountable via personal liability;
- have a responsibility to inform the IG Team of any new use of personal data immediately; must maintain an appropriate level of awareness of the DPA / GDPR and to attend training as appropriate;
- ensure that all personal information is accurate, relevant, up-to-date and used appropriately, for both electronic and manual Information Asset;
- ensure that personal data is not removed from the company premises except where specifically required for the execution of legitimate functions of the company and, then, only in accordance with appropriate policies;
- ensure that all copies of personal data output, or obtained from the system whether electronic, recorded on paper, microfilm, or any other form, are securely and confidentiality managed and destroyed/erased when they are no longer required for company purposes;
- ensure that the IG Team is advised as soon as possible of any problems or complaints relating to any SAR or unauthorised disclosures/ breaches of confidentiality;
- failure to adhere to this policy and its associated procedures may result in disciplinary action.

Monitoring and Review

Clinical Partnership (CP) will undertake or commission assessments and audits of its framework, policies and procedures to monitor compliance and make improvements where identified.

This policy will be reviewed every two years, and in accordance with the following on an as and when required basis if the following occurs:

- Legislative changes;
- good practice;
- guidance; case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure.

Where there are no significant alterations required, this Policy shall remain for a period of no longer than two years of the ratification date.

Legislation and Related Documents

Legal Acts

Data Protection Act 2018;
General Data Protection Regulation;
Human Rights Act;
Freedom of Information Act 2000;
Copyright, Designs and Patents Act (1988);
Computer Misuse Act (1990);
Terrorism Act (2000);
Human Rights Act 1998.

Supporting Documents

NHS Code of Confidentiality;
Caldicott Guardian Manual 2017;
NHS Information Risk Management;
Records Management Code of Practice for Health and Social Care 2016;
The DSP Toolkit;

Relevant Policies and Procedures

The following policies and procedures should be read in conjunction with this policy:

Information Governance Policy;
Record Management & Lifecycle Policy;
Staff handbook
Sending and Transferring information securely;
Subject Access Request Policy

Clinical Partnership
SPECIALIST COMMUNITY CARE

Title of Service/Policy
Data protection and confidentiality policy.
Is this a new or existing Policy/service?
Existing

1. Would this service or policy be aimed at any particular equality group?			
	Yes	No	If yes……
Age	☐	☒	
Disability	☐	☒	
Gender Identity (transgender)	☐	☒	
Marriage and Civil Partnership	☐	☒	
Pregnancy and Maternity	☐	☒	
Race	☐	☒	
Religion and Belief	☐	☒	
Sex (Gender)	☐	☒	
Sexual Orientation	☐	☒	
Social Exclusion	☐	☒	
Economic Deprivation.	☐	☒	
Rural Isolation	☐	☒	
Social Stigma	☐	☒	

2. Would the service/policy potentially exclude or have a negative impact on any of the equality groups?			
	Yes	No	If yes……
Age	☐	☒	
Disability	☐	☒	
Gender Identity (transgender)	☐	☒	
Marriage and Civil Partnership	☐	☒	
Pregnancy and Maternity	☐	☒	
Race	☐	☒	
Religion and Belief	☐	☒	
Sex (Gender)	☐	☒	
Sexual Orientation	☐	☒	
Social Exclusion	☐	☒	
Economic Deprivation.	☐	☒	
Rural Isolation	☐	☒	
Social Stigma	☐	☒	

3. Are there any known barriers which would obstruct access to this service/pathway			
	Yes	No	Barriers can include physical, geographical, communication.
Age	☐	☒	
Disability	☐	☒	
Gender Identity (transgender)	☐	☒	
Marriage and Civil Partnership	☐	☒	
Pregnancy and Maternity	☐	☒	
Race	☐	☒	
Religion and Belief	☐	☒	
Sex (Gender)	☐	☒	
Sexual Orientation	☐	☒	
Social Exclusion	☐	☒	
Economic Deprivation.	☐	☒	
Rural Isolation	☐	☒	
Social Stigma	☐	☒	

4. What evidence has been used to assist you to make the judgements in questions 1 – 3?		
Demographic data and other status including census findings.	☐	
Result of research findings including studies of deprivation.	☐	
Results of recent consultations and surveys.	☐	
Results of ethnic monitoring data and any equalities data from Local Authority/Public Health etc.	☐	
Information from other agencies or group	☐	
Comparisons between similar policies/services	☒	
Analysis of Patient and Public Involvement	☐	
Analysis of audit reports and review.	☐	
Community Engagement and consultation events.	☐	

CHECKLIST for board sign off Please complete all the below relevant tick boxes

	Yes	No	Comments
By completing and submitting this EIA we agree to all contents being published on the CP website.	☒	☐	
By signing this EIA we confirm that we have made all the necessary enquiries in relation to this service and in good faith that relevant steps and plans are in place to mitigate any potential discrimination in the service we provide.	☒	☐	
We understand that if we identify an action this is absolutely fine and demonstrates that we are willing to review our service and tailor it to the needs of the community.	☒	☐	
We understand that progress on any identified actions will be discussed at the contract review meetings. If required we will ensure that all action plans are available for review at these meetings.	☒	☐	
We understand that this EIA relates to a particular service. Our Equality and Diversity policy may also be requested in order for us to demonstrate our commitment to equality legislation.	☒	☐	
We are aware of the new Equality Act 2010 and are committed to ensuring that all our policies and procedures reflect the legislation. Full details can be found at:	☒	☐	

Date of Screening	October 2020
Risk identified in EIA	None
Review Date	September 2022
Title of person conducting the review	Information Assurance Director
Signature	Holly Hellstrom
Full Assessment Review Date	N/a
Board sign off Date & Committee	IGT – October 2020