Freshney Pelham Care Ltd

DATA PROTECTION AND CONFIDENTIALITY POLICY

Author	Nicola Ashton
Date of Issue	9th December 2019
Version Number	Revised v3 – 18th December 2023
Date of Review	18th December 2026 Every 3 years or as required
Signed & Dated **Manager** **Clinical Governance Lead**	…… ……

UPDATE / AMENDMENTS RECORD			
Version	**Author**	**Nature of Change**	**Date authorised by Directors**
V1	N Ashton	New policy regarding GDPR regulations	12/12/2019
V1.1	N Ashton	Retention and Disposal added to appendices	12/2/2020
V2	N Ashton	Policy Reviewed	8/11/2021
V3	N Ashton	Policy reviewed and updated	18/12/23

CONTENTS PAGE

1. DATA PROTECTION STATEMENT 4
2. INTRODUCTION, SCOPE, PURPOSE & DEFINITIONS 4
   - 2.1. Introduction 4
   - 2.2. Scope 4
   - 2.3. Purpose 5
   - 2.4. Definitions 5
3. ROLES & RESPONSIBILITIES 6
   - 3.1. Management Responsibility 6
   - 3.2. Individual Responsibility 7
4. PRINCIPLES & PROCEDURES 7
   - 4.1. Data Protection Act 2018 & GDPR 7
   - 4.2. COLDICOTT Report 8
   - 4.3. Data Processing 8
   - 4.4. Access to IT systems 9
   - 4.5. Access to Records 9
   - 4.6. Communicating Personal Information 9
   - 4.7. Disclosure & Sharing of Personal Information 10
   - 4.8. Disposal of Personal Information 10
   - 4.9. Breach of Policy 10
5. IMPLEMENTATION 11
6. MONITORING, COMPLIANCE & EFFECTIVENESS 11
7. EVALUATION AND REVIEW 11
8. REFERENCES 11
9. APPENDICES 12

Appendix A – Guide to secure transfer of data 12
Appendix B – Guide to the Disclosure and Sharing of Information 15
Appendix C – Data Flowchart 17

1. DATA PROTECTION STATEMENT

Data is central to all that FPC (Freshney Pelham Care) does; FPC collects and uses personal data in order to carry out its business activities and to provide nursing and health care services.

The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) sets the legal framework by which we can process personal information. It applies to information that might identify any living person. The common law of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act 1998, article 8, provides a person with the right to respect for private and family life. The key rights provided by this legal framework are also set out in the NHS constitution (section 3A).

The legislation sets out a number of data protection principles, and whilst these principles do not provide hard and fast rules, they embody the spirit of the legislation and are fundamental to embedding good data protection practice, and FPC compliance within this.

The six Data Protection Principles are:

- Processing shall be lawful, fair and transparent
- The purpose of processing shall be specified, explicit and legitimate
- Personal data processed shall be adequate, relevant and not excessive
- Personal data shall be accurate and kept up to date
- Personal data processed for any purposes shall not be kept for any longer than is necessary
- Personal data shall be processed in a secure manner.

This legislation also stipulates that those who record and use personal data must be open about how the information is used and follow good handling practices. This applies to the whole lifecycle of information including the collection, use disclosure, retention and destruction.

FPC are committed to fulfilling all its obligations under data protection legislation, and this policy provides a guide to the key elements of the legal framework governing information handling and responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling.

2. INTRODUCTION, SCOPE & PURPOSE OF THIS POLICY

2.1. INTRODUCTION

FPC cannot operate effectively if the patients we need to treat do not trust us to provide confidential and effective care. Part of this trust is being able to provide confidential information to clinicians and other staff and be confident that it will remain confidential and only shared when necessary.

This document provides guidance for everyone on the processing of information in accordance with the principles and legal obligations outlined by the DPA 2018, GDPR and common law of duty of confidentiality. It explains how we can comply with best practice for information handling within the NHS as described in the NHS Code of Confidentiality, Data Protection and Security Protection Toolkit and the COLDICOTT Reports.

2.2. SCOPE

This policy provides guidance to ensure that information processed by FPC is handled in a safe and secure manner which complies with current legislation and best practice relating to data protection and confidentiality.

It will apply to all areas of the organisation and all staff who handle information. It will be of particular relevance to staff members who handle personal and sensitive information relating to both patients and staff.

Data Protection and Confidentiality is a key component of Information Governance and as such this policy and associated procedures form part of the overall Information Governance Framework.

2.3. PURPOSE

The purpose of this policy is to enable us to ensure we:

- Comply with all data protection legislation and requirements in respect of the personal data we process.
- Protect the personal data and respect the rights of everyone we process the data of.
- Follow good practice in our processing of personal data.

This policy applies to anyone accessing personal data, using our systems or equipment, or processing personal data on our behalf.

2.4. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified or identifiable person who can be directly or indirectly identified by a particular reference or an identifier.
Special Categories of data	Is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual habits.
Criminal convictions and offences data	Is personal data relating to criminal convictions and offences or related security measures. This covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. It includes not just data which is obviously about a specific criminal conviction or trial but may also include personal data about unproven allegations and information relating to the absence of allegations. It also covers a wide range of related security measures, including personal data about penalties; conditions or restrictions placed on an individual as part of the criminal justice process; or civil measures which may lead to a criminal penalty if not adhered to. It does not cover information about other individuals, including victims and witnesses of crime, however we determine this information to be sensitive and will take particular care when processing it.
Data Controller	The person (or company) who determines the purposes for which and the manner in which any personal data are, or are to be recorded. In our case the Data Controller is FPC.

Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person who processes data on behalf of the data controller.
Direct care	The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider. Examples include assessment, performing procedures and implementation of a care plan.
Duty of confidence	A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.
Explicit consent	A form of consent normally given orally or in writing and is where a patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.
Information Governance	Information Governance (IG) is a combination of legal requirement, policy and best practice designed to ensure all aspects of the information processing and handling are of the highest standards.
Legitimate relationship	A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides justification for those users to access a patient record.
Processing	This term covers the collection, recording or holding of information or data, or carrying out any operation(s) on the information or data, including but not restricted to alteration, retrieval, disclosure and disposal or destruction of the data.
Non care or secondary purpose	Purposes other than direct care such as health care planning, commissioning, public health, clinical audit and governance, benchmarking, performance, improvement, medical research and policy development

3. ROLES & RESPONSIBILITIES

3.1. MANAGEMENT RESPONSIBILITIES

The CEO is responsible for the overall leadership and management of FPC and has ultimate responsibility for ensuring compliance with the DPA 2018, GDPR, Human Rights Act 1998 and the Common Law Duty of Confidentiality. The CEO delegates aspects of their responsibility to relevant Directors and the Management Team.

The CEO takes the role of Senior Information Risk Officer (SIRO). The SIRO has overall responsibility and accountability regarding Data Protection and is required to provide assurance that all risks are effectively managed and mitigated. They have delegated compliance of Data Protection to the Data Protection Officer.

The Operational Business Manager takes the role of Data Protection Officer and holds responsibility for all day to day Data Protection, Security and Confidentiality matters.

Dr Collett takes the role of COLDICOTT Guardian.

The Clinical Lead Manager, Practice Educator, LTC Manager and Team Leaders are responsible for the implementation of this policy within their areas of responsibility.

3.2. INDIVIDUAL RESPONSIBILITIES

Everyone working for FPC (within the NHS contract) has a legal duty to keep information about patients and clients and other individuals such as staff and volunteers confidential. They are required to adhere to confidentiality agreements i.e. Common Law Duty of Confidentiality, Contract of Employment, and NHS Confidentiality Code of Practice.

The terms and conditions within FPC employment contracts includes specific conditions relating to confidentiality as follows:

> *You shall not use or disclose to any person either during or at any time after your employment with the Employer, any confidential information. For the purposes of this clause 16, confidential information means any information or matter about the business or affairs of the Employer or its patients, or any of its business contacts, or about any other matters which may come to your knowledge in the course of your employment, and which is not in the public domain or which is in the public domain as a result of your breach of this agreement.*

All staff are responsible for ensuring they keep up to date with Information Governance Training in accordance with FPC Statutory and Mandatory Training, as this training covers relevant data protection and confidentiality requirements.

This requirement also applies to anyone working for FPC (i.e. contractors / temporary staff) who may have access to personal information and FPC will ensure they have adequate training before working with FPC.

4. PRINCIPLES & PROCEDURES

4.1. DATA PROTECTION ACT 2018 & GDPR

The DPA 2018 and GDPR sets out the legal requirements and duties placed on data controllers (i.e. FPC), and data processors (anyone processing data on our behalf) and explains the information rights held by data subjects (people we hold information about).

FPC are required to register annually with the Information Commissioner as a Data Controller. The Registration Number for FPC is ZA500493.

The DPA sets out 6 data protection principles which describe legal requirements in regards to processing data. These principles are the key rules for data handling and any processing of data which breeches one or more of the 6 principles is unlawful.

Although the DPA 2018 does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive.

Under GDPR each controller of information must decide under what basis it is processing personal information. If there is no relevant basis, then processing is likely to be illegal.

Under Article 6, our basis for processing personal information is:

> "The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law."

As FPC process special category information – which includes health data then it must have a second basis (under Article 9) which are:

- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity the employee, medical diagnosis, the provisions of health and social care or treatment or the management of health and social care systems and services on the basis of Union or Member State Law or pursuant contract with a health professional and subject to the conditions and safeguards.

- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State Law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose in accordance with Article 89(1) based on Union or Member State Law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

4.2. COLDICOTT REPORT

The COLDICOTT Report was published in 1997 (updated in 2013 and 2016) and focused on the protection and processing of patient identifiable information within the NHS. The reports provided the NHS with a series of principles to adhere to:

- Justify the purpose for collecting or holding patient-identifiable information
- Do not use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

The appointed COLDICOTT Guardian advises the Board of Directors on matters of patient confidentiality and promotes the safe and secure handling of patient data.

4.3. DATA PROCESSING

Data processing covers the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintaining confidence between FPC and its patients, staff and others with whom we deal.

The DPA requires that the processing of information held by FPC must be both fair and lawful. This requires that the processing meets the fair processing criteria and satisfies one or more 'conditions of processing' set out in the DPA.

To ensure 'fair processing' we must be lawful, fair and transparent about the way we will use the personal data we hold. We must demonstrate that we:

- Are open and honest about our identity
- Tell people how we intend to use any personal data we collect about them
- Usually handle their personal data only in ways they would reasonably expect
- Do not use their information in ways that unjustifiably have a negative effect on them
- Help people understand their rights

A Data Protection Impact Assessment (DIPA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient or staff information.

4.4. ACCESS TO IT SYSTEMS

It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing or inappropriate access. The IT support (F4 IT) have detailed guidance on security of FPC IT systems.

Staff should not attempt to access or use electronic record systems where they have not been trained to use it or have authorised access. Existing system users should not allow others to access systems using their log in credentials. Sharing system passwords is a disciplinary offence and viewed as a serious breach of Company procedure.

4.5. ACCESS TO RECORDS

FPC has access to thousands of individual patient records in various formats. In addition it also holds records for present and past employees and others it does business with. While it is clearly necessary for many members of staff to routinely carry out their work, it is important that staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful. All electronic patient databases incorporate an audit tool to track usage and activity and is monitored by the practice management teams.

Our clinical systems allow users to access any individual record held in the system. Users should only access individual records for those data subjects they have authorisation to access for a specific purpose or in case of patient records were they have a 'legitimate relationship' with the patient.

Staff have no right to access personal information held in records about their relatives or friends unless the circumstances meet the criteria for data access. The same applies to staff accessing their own data held in records without specific authorisation.

For details on obtaining access to copies of personal information held by FPC, please speak to the Operational Business Manager.

Any member of staff found to be inappropriately accessing their own or other people's data may face disciplinary action.

4.6. COMMUNICATING PERSONAL INFORMATION

All individuals who work within, or under contract to, the NHS have a responsibility for the security of information they create or use in performance of their duties. Based on the COLDICOTT Principles (1 to 4) the principles for transferring information are:

- Information should only be transferred for a justifiable purpose
- The transfer should only take place when absolutely necessary
- Only the minimum information necessary should be transferred
- The information should be transferred on a need to know basis

In order to provide effective care services there is a need to transfer information between FPC and other organisations and individuals. In order to comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

Any data containing identifiable information transferred by FPC outside of the company, must be securely encrypted during transfer. Any data transfer outside of the EEA (Economic European Area) must only be carried out if appropriate security controls are in place.

A guide on transfer of data by post or by hand, or by email and the use of portable media is in Appendix A.

4.7. DISCLOSURE & SHARING OF PERSONAL INFORMATION

Sharing Personal Information for Care Purposes

In order to provide safe and effective care, personal information about patients will need to be shared with all those caring for an individual. In addition to the clinical team providing care the care team may include social care, specialist care teams and administrative staff supporting the process.

In accordance with both the DPA 2018, GDPR and COLDICOTT Principles, information shared for care purposes should be relevant, necessary and proportionate. In applying this principle, care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

The COLDICOTT Principle 7 (Duty to Share) emphasises the need to share information in certain circumstances where the duty to share information clearly outweighs the normal duty of confidentiality owed. This would be the case when there is a threat to the safety of others and the sharing of the personal information about individuals (e.g. vulnerable adults and children) with the police and other agencies may prevent that threat materialising.

Sharing Personal Information for Non Care Purposes

Non care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using anonymised data. This removes the need to consider consent issues.

In certain circumstances the law requires that confidential information should be disclosed when consent may not be provided. Examples of this include a direction within a court order or the requirement to notify Public Health Officials where the patient is suspected of suffering from a notifiable disease. Further in formation around this is within Appendix B.

4.8. DISPOSAL OF PERSONAL INFORMATION

It is a principle of DPA that data should ‘not be kept for longer than necessary’. FPC follow NHS guidelines for retention and disposal of records. Please refer to FPC’s Retention and Records Policy.

All printouts, reports and printed copies of records containing personal data should be kept secure at all times.

Any documents containing personal data should be disposed of securely and not discarded in waste and recycling bins. Documents should be placed within the confidential waste disposal box, this is emptied twice a month.

The disposal of any electronic equipment / medical devices which may hold personal data (pc, laptop, phones etc.) should be carried out through the IT support team to ensure all data is removed before disposal.

4.9. BREACH OF POLICY & PROCEDURE

Any breach of data protection and confidentiality can have severe implications for the company, our patients and staff and, where significant numbers of patients are involved, can impact on ours and the NHS reputation as a whole.

Breaches of confidentiality or unauthorised disclosure of any information subject to the DPA 2018 constitutes a serious disciplinary offence or gross misconduct under the Disciplinary

Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including dismissal.

The office of the Information Commissioner's Office (ICO) regulates Data Protection and is charged with upholding individual's information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of a financial penalty up to £20m.

Staff who wish to report incidents relating to data protection and confidentiality should follow the Whistleblowing Policy, or speak to the Business Manager. This should be done immediately.

5. IMPLEMENTATION

This policy will be distributed amongst staff and held within the Policy Folders in the Training Library. IG training must be completed in accordance with FPC mandatory training requirements.

The FPC leaflet for patients (How we use your Health Records) contains key information published in this policy.

6. MONITORING, COMPLIANCE AND EFFECTIVENESS

The purpose of monitoring is to provide assurance that the agreed approach is being followed – this ensures that we get things right for the patients, use resources well and protect our reputation. Our monitoring will therefore be proportionate, achievable and deal with specifics that can be measured.

Monitoring will be around breaches in procedure, legitimate access to personal information and compliance to NHS Best Practice and Legal requirements.

Where monitoring identifies deficiencies, action plans will be developed to address them.

7. EVALUATION & REVIEW

This policy will be reviewed in 2 years unless a substantial change in policy or legislation takes place, where an earlier review will be undertaken.

This policy should be read in conjunction with:

- Disciplinary Policy
- Freedom of Information Policy
- Subject Access Request Policy
- Records Retention Policy
- Whistleblowing Policy
- Terms and Conditions of Employment

8. REFERENCES

- Information Commissioner's Website - https://ico.org.uk/
- ICO Guide to Data Protection - https://ico.org.uk/for-organisations/guide-to-data-protection/
- A Guide to Confidentiality in Health and Social Care - https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care

APPENDIX A

Staff Guidance on the Secure Transfer and Communication of Personal Data

Introduction

Public Sector organisations continue to report a high level of data breaches, many of which relate to the unsecure transfer and inappropriate disclosure of sensitive personal information. It is therefore important that all staff are aware of best practice and guidance for the secure transfer and communication of personal data.

Guidance for staff in relation to this is outlined within this appendix.

Circumstances may arise where a transfer of personal data needs to take place, but for some reason it is not possible to follow best practice and the proposed transfer poses a degree of risk. In these circumstances the sender must conduct a simple risk assessment and consider if the perceived need to communicate the data by the method selected outweighs the risk associated with the method of transfer.

Post

It is acceptable to use first and second class post for routine clinical correspondence such as appointment letters and non-urgent results. Post Office signed for and special delivery tracking services provide an increased level of security and the selection of the appropriate service should be made based on the risk assessment.

Patient records, personal files, letters including sensitive information and transfers of bulk data should be sent using one of the signed for services or a recognised courier service.

When using postal services to transfer personal information the following guidance should be followed:

- Ensure that the information in the envelope is correct and no additional pieces of paper or documentation has been included in error.
- Ensure the envelope is robust enough to protect the contents and sealed correctly (do not use unsealed internal envelopes for the transfer of personal information)
- Ensure the full and correct name and address of the recipient is clearly shown
- Mark the envelope ‘private & confidential’
- Add the senders details onto the back of the envelope
- Ask external recipients to confirm safe delivery
- Do not use window envelopes for any bulk mailings
- CD’s and removable data must NOT be sent via the post

Email

NHS policy is that emails that include personal data should be sent securely to avoid the risk of accidental disclosure through misdirection or interception. This is best achieved by ensuring that the email is encrypted during transit so the contents cannot be read other than by the intended recipient.

The simplest way to comply with NHS Policy and securely send personal data outside the organisation network is by using NHSmail. An email sent between NHSmail accounts is automatically encrypted and remains secure during transit.

If you need to send an email containing patient information outside NHSmail, write **[SECURE]** at the start of the email subject (this must include square brackets). Doing this ensures that the information is encrypted during transit, and the response from the recipient will also be secure when replying to you. If the email account you are sending to is not secure, then the recipient will be asked to log into the encryption software prior to the information being released to them.

The simple use of password protection on files attached to the email which contain personal data can be used. Please provide the password for the file via another means of communication.

Email guidance

- All emails must be processed in line with the Email and Internet Policy and associated guidance.
- Users must ensure that any confidential information is sent to the mailbox of a person authorised to see that information and that no unauthorised persons have access to that mailbox.
- Confidential or special categories of personal data should not be sent to shared or group email boxes unless completely sure of the user group members and their security arrangements.
- When sending confidential information, staff must not include personal confidential data in the heading or main body of the email. Please ensure that any attachments are double checked for sensitive/personal/confidential information. This could include any backing data, hidden cells or other sheets in a spreadsheet document.
- Users must confirm the email address and spell any awkward words and where appropriate send a test message.

In all instances, whether the email is encrypted or not, the following guidelines must be observed:

- Consider if email is the best way to send the data – e.g. could the document be placed on a shared drive for both parties to access.
- Limit the number of recipients to the message to as few as possible.
- Double check that you have the correct recipients before sending the email.
- Messages containing personal data sent to the wrong recipient will be classed as a breach of confidentiality.
- Limit the amount of data to only that which is needed for the purpose it is being sent.
- Mark the message confidential in the subject as well as in the message properties.
- Be aware that your original email can be forwarded by the recipient without your consent.
- Use the minimum personal identifiable information, particularly in subject titles, document names etc.
- Include a note to say that the receiver of patient identifiable data is responsible for the security and confidentiality of that data.
- Do not keep personal data on email for any longer than is necessary.

Telephone

Incoming calls may provoke a sensitive / confidential conversation and caution should be exercised to ensure these conversations are not overheard, and that only appropriate information is discussed.

Confidential information received over the telephone must be processed appropriately and the following security protocols used:

- Ensure the caller has a legitimate right to have access to the information before the information is given out and provide information only to the person who has requested it.
- Confirm the name, job title, department and organisation of the person requesting the information, ensuring that you are speaking to the correct person.
- Take a contact number e.g. a main switchboard rather than a direct line / mobile number.
- Ring back to confirm that person's identity.
- Confirm the reason for the request.
- Do not leave any personal data on an answerphone machine as you may inadvertently breach patient confidentiality.
- Never use 'speaker' mode as this effectively turns the confidential conversation call into a 'tannoy' message.

Use of Removable Media

Many of the most highly publicised losses of data in the public sector have involved data held on memory sticks. The risk of theft or loss of these devices is high and therefore it is essential that any identifiable data being transferred onto a portable device is always encrypted.

Memory sticks should only be used for the short term storage of personal data.

Transferring of Personal Information by Hand / Taking Information Off Site

Transferring data manually is often seen as a quick and effective way to deliver information to another person or organisation. When transferring personal data by hand, or taking information off site to meetings etc., the risks from loss or theft can increase. The following points should be considered and if necessary action taken to mitigate any identified potential risks proportional to the amount of sensitive date being transferred:

- The Medium
    - Consider if the information can be saved on an encrypted data stick or laptop for transit rather than using a printed medium
    - If using this method consider how you will print/download/access the information on arrival
- Security in Transit
    - During the transfer maintain security of the information by using a lockable case
    - If using public transport retain the information with you at all times
    - If travelling by car, secure the information in the boot of the car
- Labelling
    - Consider how you can identify and label the material in some way so if it is lost or stolen and then subsequently found it can be identified as FPC property and safely returned
- Overnight Storage
    - The need to store personal data at home should be avoided if possible
    - If unavoidable, personal information should be stored in a lockable container which is not accessible by anyone else living in the home.

APPENDIX B

Staff Guidance on the Disclosure and Sharing of Personal Data

Introduction

Information Governance policy and procedure is designed to support best practice in information handling and should not be a barrier to the sharing of personal information when necessary and appropriate. However, it is recognised that some circumstances produce complex situations which require careful consideration, and if unsure about a specific issue staff should seek guidance from their Team Leader or a member of the Management Team.

Disclosing Information to Relatives and Carers

- It is good practice to establish and record if the patient wishes to place any restrictions on the information provided about them to others.
- Where restrictions are placed on information to be provided about patients, it is important that all staff are made aware of the details to avoid a breach in confidentiality.
- If suspicious about the motives of a person making an enquiry about a patient, then information should not be passed on, but the details of the person making the request recorded and a discussion held with a Team Leader or member of the Management Team to seek advice before making contact again.

Disclosing Information to the Police

Section 29 of the DPA 1998 provides a lawful basis for the company to disclose personal data about a person in the absence of their consent where this will support certain aspects of law enforcement, and in particular:

- The detection and punishment of a crime
- The identification, apprehension and prosecution of offenders

Most enquiries made by the police for information using this provision will be made through the Management Team; where an enquiry is made outside of office hours, the query must be passed on to the Management Team at the earliest opportunity. Even when the information is required within a strict timeline, it is acknowledged that decisions might need to be made quickly, however, staff should not be pressured into disclosing information when they feel it is not in the patient's best interest.

Whilst the law permits disclosure in certain circumstances outlined above, it does not compel the company to comply with such information requests. Each case should be considered on the individual merits of the request. Where consent to disclose information to the police is not provided or refused, the company has to consider the duty of confidentiality owed to the data subject and the public interest in maintaining a confidential service and balance this with the wider public interest in making the requested disclosure to support law & order purposes. Striking the appropriate balance in some situations can be challenging and in these instances specialist advice should be sought from the ICB IG Team.

In addition to the police, it should be noted that other agencies such as the Home Office, HMRC and NHS Counter Fraud Services may request information about patients using this exemption.

Access to Information for Audit, Service Improvement and Research Purposes

Clinical Audit

Clinical Audit is recognised as a necessary tool to check the care provided by FPC meets acceptable standards and is safe and effective. Access to patient personal information without consent for the purpose of clinical audit is normally permissible. The audit should be internal to FPC and not part of a multi-site/organisation audit. Where these criteria are not met, then advice should be sought from the CCG IG Team before sharing or allowing access to those records.

Service Improvement

Dependent on the circumstances access to patient personal information without consent for the purpose of conducting a Service Improvement project, may also be permissible. The term 'service improvement' is widely used to cover a range of improvement activities and caution should be exercised to ensure the boundaries between service improvement and research activities are not blurred.

Research

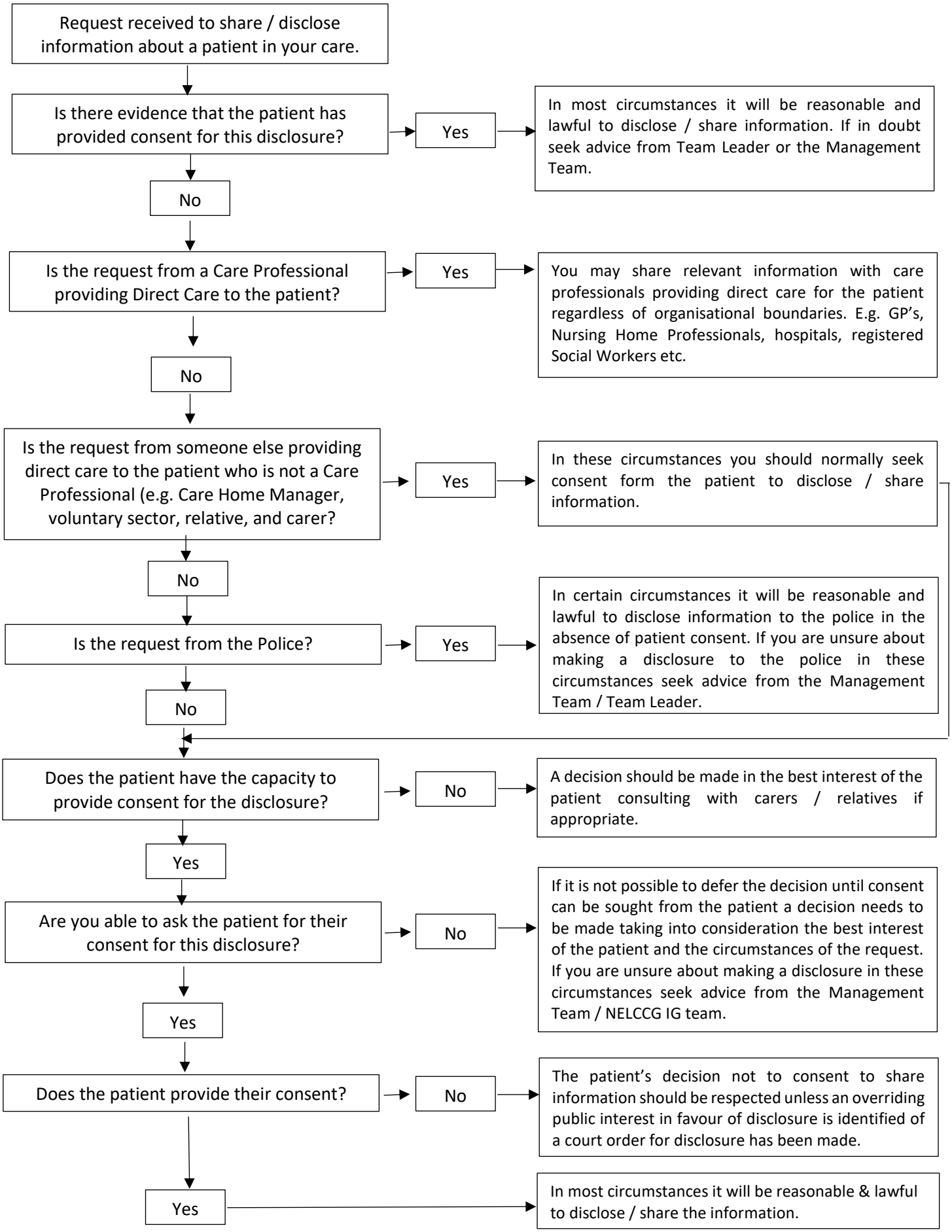
Most research activity requires formal approval and patient consent is normally required before access to any patient information is provided or made. The need to obtain patient consent can be waived in some circumstances following formal application to the NHS Research Authority (NHSRA).

Sharing Information for Safeguarding Purposes

COLDICOTT principle 7 makes clear that in certain situations the duty to share information is as important as the considerations of confidentiality. This is particularly the case in matters of safeguarding where in the past public authorities have failed individuals by not sharing information they have held which if passed on may have prevented someone harming them.

Where an individual is thought to be at risk, relevant information should be shared between agencies involved with the individual if the provision of that information might reduce or eliminate the identified risk. If it is possible to obtain consent from the subject to share their data this should be done, but the absence of or refusal to provide consent should not deter staff from sharing information where it is felt to be appropriate and justified to support a safeguarding purpose.

APPENDIX C - FLOWCHART - RESPONDING TO A REQUEST FOR INFORMATION



Equality Impact Assessment Form

Step 1 – Identify the policy

Policy title	Data Protection and Confidentiality Policy
Department responsible for the policy	FPC Ltd
New or previously approved policy?	Reviewed policy
Date of approval / last review (if known)	8th November 2021
Name and role of Assessor(s)	Nicola Ashton – Operational Business Manager

Step 2 – Further information

1. Describe the main aims, objectives and purpose of the policy	This policy provides a guide to the key elements of the legal framework governing information handling outlines and responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling.
2. Who is expected to benefit from this policy?	All patients, stakeholders and staff employed by FPC Ltd and users and partners of the service
3. Who was consulted on this policy?	Senior Managers, Directors, NELCCG, NHS

Step 3 – Assess the impact on different groups of people

4. In the table below, please tick whether the policy affects particular groups of people – the Equality Target Groups below -- in different ways, compared to other groups. Here are some examples:

- **Positive impact:** a policy or practice where the impact on a particular group of people is more positive than for other groups, e.g., accessible website design. It can also include legally permitted positive action initiatives designed to remedy workforce imbalance, such as job interview guarantee schemes for disabled people.
- **Negative impact**: a policy or practice where the impact on a particular group of people is more negative than for other groups (e.g., where the choice of venue for a staff social occasion precludes members of a particular faith or belief group from participating).
- **Neutral impact:** a policy or practice with neither a positive nor a negative impact on any group or groups of people, compared to others.

Equality Target Group	Positive impact	Negative impact	Neutral impact	Reasons / comments
Men			X	This policy and procedure applies equally to all staff, regardless of gender, race, disability, sexual orientation, religion or age.
Women			X	As above
People from black and minority ethnic communities			X	As above
Disabled people			X	As above
Gay, Lesbian and Bisexual People			X	As above
Transgender people			X	As above
Older people (50+)			X	As above
Younger people (17 – 25)			X	As above
Faith or belief groups			X	As above

Signed by Assessor:

Date: