Information Governance and Data Protection Policy

Distribution: Staff, Clinical Partners, Clients on request
Date of issue: September 2014
Review date: January 2018
Review date: January 2020
Next review: January 2022

Author - Barny Guthrie, CEO

Clinical Partners
It's about getting better

Contents

Information Governance and Data Protection Policy

1. Introduction

Clinical Partners Ltd. (the Company) recognises the importance of reliable information and the contribution it makes to the objective of the company which is to provide access to the highest quality mental health outpatient care. Clinical Partners is committed to operating robust arrangements for information governance to ensure that its uses data in a secure and effective way. The organisation is always mindful of the clients right to be assured of confidentiality and in a way that seeks always to minimise the risk of loss or misuse of personal identifiable data.

The Board of Clinical Partners recognises its responsibilities under the Data Protection Act 2018 and the GDPR, to maintain the security and confidentiality of all person identifiable data that it handles and has developed procedures to ensure that this occurs. Clinical Partners seeks to work in a transparent and accountable manner when handling information relating to individuals.

2. Purpose and Principles of Data Protection

The Information Governance (IG) Policy sets out the how the Company will ensure that information is used effectively, efficiently, securely and legally, and the steps that it will take to minimise loss/breach of confidential data that it manages. The principles of GDPR are based on accountability. The organisation will ensure that all information relates to the following principles:

- It is lawful, fair and transparent
- It is collected and retained for a specific purpose
- The information is relevant and accurate
- Information is held securely
- Individuals' rights are observed

3. Scope

This policy covers the use and management of information in all formats, (e.g. paper, electronic) including the security, availability, collection, processing, storage, communication and disposal of information.

The introduction of GDPR 2018 applies across the whole of the EU and affects any non- EU business offering services to EU citizens.

The policy applies to all employees and contractors working for or supplying services to or for the Company.

4. Definitions

The following terms will be used in this policy:

Information Governance – Relates to the way the organisation processes or handles information in a legal and secure manner.

Personal Data – Information held by the organisation on individuals accessing their services

Data Subject – This is an individual who can be identified from information recorded about them and to whom the information relates

Data Controller – This is how the organisation controls and manages the information they hold

Data Processor – This is a third-party organisation that manages, processes and stores data on behalf of the organisation. An example would be outsourced payroll.

Under GDPR there are new responsibilities for Processors which will include the Data Controller ensuring the Processor is complaint with GDPR in terms of diligence and data protection and if necessary auditing their processes.

5. GDPR – What has changed?

In May 2018 GDPR came into force and affects all European Countries or those countries who provide services to European citizens. The changes will affect:

- Consent
- Scope
- Accountability
- Children
- Rights
- Processors
- Breaches
- Fines

5.1 Consent

This involves organisations having clear messaging and a positive opt – in tick box rather than an assumption of opt in. Consent for information must be recorded without detriment and an individual can withdraw consent at any time.

5.2 Scope

As above

5.3 Accountability

The organisation must demonstrate compliance and record all processing activities. All actions should be documented both by the Data Controller and Processor.

5.4 Children

All communication with children must have child friendly messaging. There must be Guardian consent where applicable with age verification.

5.5 Rights

This relates to the individual's right to be informed and have access requests. Individuals will have the right to have data erased (unless required by law) and the right to move or transfer data. No charges can be levied for providing personal data to that individual.

5.6 Data Processors

The Data Controller must ensure that any Data Processor is complaint with GDPR and this should be documented in any contractual agreement or terms along with specific responsibilities. Under GDPR there are new responsibilities for Processors.

5.7 The Data Processor must carry out GDPR diligence and data protection. The following should be considered when reviewing the lawfulness of processing:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

5.8 The basis for the processing referred to in point (c) and (e) of paragraph 5.7 shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Breaches and Fines

Any breaches need to be notified to the data subject and recorded as a minimum. There needs to be a notification to the regulatory body. Examples of notification requirement are accidental deletion or a lack of privacy where an individual's data has been deliberately or otherwise seen by an unauthorised individual. Other breaches include errors in Data retention and Processing.

Fines for any breach can be up to 4% of global turnover or 20m Euros.

6. Duties and Responsibilities

Chief Executive Officer

The CEO has ultimate responsibility for all elements of governance, including information governance within the Company. The CEO will work with staff and the Governance and Risk Adviser, together with externally contracted experts to ensure that Clinical Partners takes all reasonable steps to develop and implement systems and processes that effectively protect confidential data about patients, staff and clinicians engaged by the Company.

Data Protection Officer

The CEO is the Data Protection Officer and can be contacted at Clinical Partners Unit 6 Chaldicott Barns, Tokes Lane, Semley, SP7 9. Where necessary they will seek guidance from experts in Data Protection to ensure compliance with GDPR. As part of the compliance process there should be a programme of audit of data systems and policies.

This policy documents Clinical Partners' approach to Data Protection and this provides internal guidance for staff. New staff will receive training in their Induction regarding compliance and Data Protection.

All Staff and Partners supplying clinical services via the Company

All staff working for the company and Partners engaged to provide patient services via the Company must work within this policy by remaining vigilant to information risks; actively risk assessing elements that they are responsible for, and for identifying and escalating any risks that are (via assessment or because of an incident) outside of their control to allow mitigation to an acceptable level.

7. Procedures for Maintaining Effective Information Governance

7.1 Meeting Legal Compliance

- The Company is registered for holding personal data as required under the Data Protection Act 2018 and GDPR 2018. Requirements for legal compliance are referred to above.

- The Privacy Policy for Clinical Partners has been reviewed and rewritten considering the GDPR changes 2018. This can be accessed on the Clinical Partners website and all prospective users of Clinical Partners services are encouraged to read the Privacy policy and accept its terms.

- All clinical staff and Clinical Partner employees have been informed of the data changes made by Clinical Partners in relation to the GDPR and how they may change, if at all, the way we communicate with clients.

- The Company will ensure Digital compliance by undertaking regular analysis of data, documenting and actioning system changes.

- Where Data Processors are involved the Company will ensure compliance through audit and contractual terms.

- The Company regards all identifiable personal information relating to clients, partners, staff and contractors as confidential, and will ensure data is held in secure ways (e.g. locked filing cabinets for paper data and on secure servers (not on hard drives) of company computers)

- When data subject identifiable data is held by the company this will be treated as confidential and will only accessed on a 'needs to know basis' for the delivery of the services of the company or to undertake administrative processes necessary for the delivery of those services

- The Company will fully cooperate with any official audit[1] of its practices in relation to information security if required to by statutory agencies and/or purchasers of the Company's services

- The Company regards all identifiable personal information relating to staff/ contractors as confidential except where national policy on accountability and openness requires otherwise or where required for fraud investigation.

- Data subjects, for whom data is recorded, or held in paper format by the Company are entitled, in law, to request details of information held about them, have the information erased or transferred. The Company must respond under arrangements in the Data Protection Act and GDPR 2018.

7.2 Information Security

The Company will maintain effective security arrangements for the access to and management of confidential information through

- Full HR checks prior to appointment of staff to the Company.

- Privacy Policy for employees outlining the use and retention of their data by the Company

- a requirement for all staff and contracted clinicians working for the Company to be issued with and accept in writing a statement of personal responsibility in relation to confidentiality.

- rigid enforcement of systems for the use of individual access passwords to all electronic data/materials held by the Company, with disciplinary action / loss of contractual rights (Clinical Partners) being taken in the event of a wilful breach of data security.

- Clinical Partners uses an industry standard data management product Clinic Office version 5[2] which provides industry level security of personal information

- All records will be held electronically on an externally hosted web accessed, password controlled server, and no paper records will be made of personal details /financial details of our patients.

- Financial management of patients invoices is handed via an externally hosted web based secure provider; 'Card safe'[3], which is a division of World Pay

- When paper records are held e.g. complaints correspondence this will always be held in a locked filing cabinet and access will be limited on a 'needs to know' basis

[1] In the case of an official audit e.g.
by the Information Commissioner full cooperation will always be given. In the event of a potential supplier wishing to conduct their own Information Govern ace Audit this will be limited to an audit of systems and processes and no confidential data (data subject or financial data) will be subject external inspection

[2] http://www.pioneersoftware.co.uk/

[3] http://www.cardsave.net

- The Company will ensure all Data Processors used by them are compliant to GDPR 2018 through compliance audits.

7.3 Rights of the data subject

You have the right to request:

- Access to the personal data we hold about you, free of charge; however we hold the right to refuse requests that are unfounded or excessive. (See 7.4)
- The correction of your personal data when incorrect, out of date or incomplete.
- That we stop holding your personal data for direct marketing purposes.
- That we stop any consent-based processing of your personal data after you withdraw consent.

If you would like us to stop holding your data, have concerns about the data we hold, or would like it transferred to another medical practitioner – please email help@clinical-partners.co.uk or call 0203 326 9160.

If we choose not to action your request we will explain the reasons for our refusal. You have the right to complain about this refusal to the supervisory authority (ICO).

To protect the confidentiality of your information, we will ask you to verify your identity before proceeding with any request you make. If you have asked someone else to submit a request on your behalf, we will ask them to prove they have your permission to act.

7.4 Right of access by data subject

The Data Protection Act 2018 (DPA) governs access to the health records of living people. The DPA is not confined to health records held by NHS bodies. It applies equally to the private health sector and to health professionals' private practice records. It also applies to employers who hold information relating to the physical or mental health of their employees if the record has been made by, or on behalf of, a health professional in connection with the care of the employee. The Act applies to all of the UK. Subject to the conditions explained in this guidance, individuals have a right to apply for access to health records irrespective of when they were compiled.

These include:

- Competent adult patients
- Children and young people - Legally, there is no automatic presumption of capacity for people under 16 in England, Wales and Northern Ireland, and those under that age must demonstrate they have sufficient understanding of what is proposed. However, children who are aged 12 or over are generally expected to have the capacity to give or withhold their consent to the release of information from their health records. Where, in the view of the appropriate health professional, the child is not capable of understanding the nature of the application for access, Clinical Partners as the holder of the record is entitled to refuse access.
- Parents - Parents may have access to their children's records if this is not contrary to a competent child's wishes. Where more than one person has parental responsibility, each may independently exercise rights of access. For a child who lives with his or her mother and whose father applies for access to the child's records, there is no obligation to inform the child's mother that access has been sought. Where a child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility. In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court. A local authority acquires parental responsibility (shared with the parents) while the child is the subject of a care or supervision order. If there is doubt about whether the person giving or withholding consent to access has parental responsibility, legal advice should be sought
- Individuals on behalf of adults who lack capacity - When patients lack mental capacity, Clinical Partners are likely to need to share information with any individual authorised to make proxy

decisions. Both the Mental Capacity Act in England and Wales and the Adults with Incapacity (Scotland) Act contain powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults. The Court of Protection in England and Wales, and the Sheriff's Court in Scotland, can also appoint deputies to do so. This may entail giving access to relevant parts of the incapacitated person's medical record, unless Clinical Partners can demonstrate that it would not be in the patient's best interests. These individuals can also be asked to consent to requests for access to records from third parties. Where there are no nominated individuals, requests for access to information relating to incapacitated adults should be granted if it is in the best interests of the patient. In all cases, only relevant information will be provided.

- Police - If the police do not have a court order or warrant they may request voluntary disclosure of a patient's health records under section 29 of the DPA. However, while Clinical Partners have the power to disclose the records to the police, there is no obligation to do so. In such cases Clinical Partners may only disclose information where the patient has given consent, or there is an overriding public interest. Disclosures in the public interest based on the common law are made where disclosure is essential to prevent a serious threat to public health, national security, the life of the individual or a third party, or to prevent or detect serious crime. This includes crimes such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people. Serious harm to the security of the state or to public order and serious fraud will also fall into this category.
- Solicitors – Clinical Partners releasing information to solicitors acting for their patients will ensure that they have the patient's written consent to disclosure and, where there is any doubt, confirm that the patient understands the nature and extent of the information disclosed.

Any data subject, or person authorised by the data subject may request copies of any personal data held about them and this will be supplied. Since GDPR 2018 no fee will be required. (See Appendix 1. 2 and 3 for procedures and templates).

The only exceptions to supplying documents is

- if the holder of the record believes that disclosure could do harm to the individual or another person
- if the controller demonstrates that they are not in a position to identify the data subject.

In the case of dispute about disclosure the company will seek legal advice.

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;

- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

No personal data held by Clinical Partners is transferred outside United Kingdom.

Any client seeking access to clinical records not held by Clinical Partners will be asked to direct their request in writing to their clinician who will be responsible for responding to the request.

7.5 Right to erasure ('right to be forgotten)

The data subject shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay and the controller shall have the obligation to erase personal data without undue delay, unless required to be kept by other legislation, where one of the following grounds applies:

- the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent and where there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data has been unlawfully processed;
- the personal data has to be erased for compliance with a legal obligation;
- the personal data has been collected in relation to the offer of information society services referred to in Article 8(1).

7.6 Responding to data related incidents

If an actual or potential breach of confidential information occurs the person identifying the incident must report it to the CEO via the Incident Reporting Procedure. The CEO will then be responsible for investigation and will call on experts as required to assist this investigation.

In the unlikely event that the Company suffers a security breach (data loss through theft, hacking or other means) the CEO will report the breach to the Information Commissioner as required under the Data Protection and GDPR 2018.

8. Process for maintaining confidentiality under the requirements of the Data Protection Act 2018 and GDPR 2018

8.1 Data Security and Disclosure

All staff /contractors working for the Company are responsible for ensuring that:

- They avoid holding person identifiable data as far as possible
- Any personal data which they hold is kept securely either electronically in a password protected system or in a locked cabinet
- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party,
- That they will take all reasonable efforts to ensure data is not disclosed accidentally.

8.2 Retention of data

As the Company is concerned with the delivery of clinical services the Company will adopt data retention recommendations set out by the Department of Health, in accord with advisory times required to deal with legal disclosure

- Person identifiable data held on clients will be held for a minimum of 8 years following the last contact (or lifetime in relation to cases related to adoption).

- Person identifiable data on staff (e.g. related to employment etc.) 5 years from termination of employment

- Person identifiable information on clinician's engaged to provide services via contract (clinical partners) 21 years from the end of the contractual arrangement (in light of the clinical work being in mental health, the recommended retention period for all mental health records is 21 years)

- Person identifiable information on potential contractors/contractors professional information to be held for as long as there is a professional relationship between person/organisation and the Company. If a contractual agreement is entered into the information will be retained for 8 years after the conclusion of business.

- Where data relates to adoption cases, client information needs to be kept for a lifetime. Clinicians are asked to send client records, via recorded delivery, to Clinical Partners Head Office as and when they stop working with Clinical Partners.

9. Process for Monitoring Compliance with this policy

9.1 When considering compliance, the following need to be considered:

- Users Rights
- Security
- Training
- Policies
- Review

9.2 A rolling programme of audits will be established to ensure the robustness of local systems for the storage and access of confidential data. Results of these audits and any action plans will be included in the CEO's report to the Board

9.3 In the event there is an actual breach of confidentiality the CEO will report on the results of the investigation (if any) and the steps taken to minimise risk of recurrence. The effect of any changes will be monitored by analysis/ audits.

9.4 Effectively managing GDPR compliance will install trust and confidence in Clinical Partners clients and future clients.

9.5 The data subject has the right to lodge a complaint with Information Commissioners Office if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

9.6 Managing compliance will start with:

- Single point of contact – Data Protection Officer
- Audit data, systems and policies
- Document approach to data protection and ensure policies are in place
- Internal documentation and guidance for staff
- Training staff
- Maintain compliance and keep up to date

10. Related Policies and Procedures and references

- Clinical Partners Risk Management Strategy and Policy
- GDPR 2018
- Information Commissioners web site http://ico.org.uk/
- Incident Reporting Policy

References

Data Protection Act 2018 and General Data Protection Regulations (GDPR)

Appendices 1

1 Patient Procedure for making a Subject Access Request.

Verbal requests

You can make a subject access request verbally, but we recommend you put it in writing if possible because this gives you a record of your request.

If you are making a verbal request to Clinical Partners, try to:

- use straightforward, polite language;
- focus the conversation on your subject access request;
- discuss the reason for your request, if this is appropriate – work with us to identify the type of information you need and where it can be found;
- ask Clinical Partners to make written notes – especially if you are asking for very specific information; and
- check our understanding – ask them to briefly summarise your request and inform them if anything is incorrect or missing before finishing the conversation.

However, if you make your request verbally, we will send you a summary of your request and ask you to sign that you have agreed to the requested information and proved your identity if deemed necessary.

Written requests

It will make it easier and quicker for us to deal with your subject access request if you use our template request form available on our web site or include the following I any correspondence:

1. Give your letter a clear tittle **Subject access request**
2. Include your relevant details to help us identify you.
    a. your full name (including any aliases, if relevant);
    b. any other information used by Clinical Partners to identify or distinguish you from other individuals (e.g. customer account number or employee number);
    c. your up-to-date contact details;
3. Give specific details of where to search for the personal data you want, for example:
    - my personnel file;
    - emails between 'person A' and 'person B' (*from date to date*)
    - my medical records (between 2014 and 2017) held by Clinical Partners;
    - any telephone recordings on *x date* between *x am and x pm*;
    - details of any payments or financial transactions (between *date and date)* held by Clinical Partners relating to you.

Confirmation of where you would like the information sent and how you would prefer to receive the data; in a particular electronic format, or printed out. If you make a request electronically, we will provide the information in a commonly used electronic format, unless you request otherwise.

Subject access requests on behalf of patients.

You can authorise someone else to make a subject access request for you. However, you should consider whether you want the other person to have access to some or all of your personal information.

Depending on the nature of your request, the other person could gain access to information that you may not want to share with them, such as your medical history.

Examples of individuals making requests for other people include:

- someone with parental responsibility, or guardianship, asking for information about a child or young person (for further information, please read our guidance for organisations on requests for information about children);
- a person appointed by a court to manage someone else's affairs;
- a solicitor acting on their client's instructions; or
- a relative or friend that the individual feels comfortable asking for help.

An organisation receiving the request needs to be satisfied that the other individual is allowed to represent you.

They may ask for formal supporting evidence to show this, such as:

- written authorisation from you; or
- a more general power of attorney.

It is the other person's responsibility to provide this when asked to do so.

Maintaining your request records

Whenever possible, we strongly recommend that:

- you keep a copy of any documents or written correspondence for your own records;
- you keep any proof of postage or delivery (such as a postal reference number), if available; and

Please also consider making a written log of your request. This should include key details, such as:

- the date and time of your request;
- the details of any contacts you have interacted with;
- notes about any personal information you asked for;
- any further information that the organisation may have asked you to provide;
- any reference numbers given to you; and
- any other relevant information.

This will provide helpful evidence if you wish to:

- follow up your request;
- raise concerns; or
- complain about an organisation's response, at a later stage.

Appendices 2

Clinical Partners response to Subject Access Requests

1. Timescales for response

Clinical Partners will respond to a subject access request promptly and in any event within 28 calendar days of receiving it.

If more time is needed to respond to complex requests an extension of another two months is permissible. Clinical Partners will communicate this to the data subject as soon as possible after the need for an extension of time becomes apparent, but within the first month. If Clinical Partners cannot provide the information requested, it will inform the data subject on this decision without delay and at the latest within one month of receipt of the request.

2. **On receipt of a SARs Clinical Partners will:**

1. Log the request on its SAR's log sheet.
2. Verify whether it is the controller of the data subject's personal data. If it is not a controller, but merely a processor, Clinical Partners will inform the data subject and refer them to the actual controller.
3. Verify the identity of the data subject. If needed, Clinical Partners will request further evidence on the identity of the data subject.
4. Clinical Partners will establish if the request is sufficiently substantiated and determine whether the SAR is clear regarding what personal data is requested. If Clinical Partners is uncertain of what data is required, it will request additional information from the data subject.
5. Verify whether requests are unfounded or excessive (in particular because of their repetitive character). If so, Clinical Partners may refuse to act on the request.
6. Verify whether Clinical Partners processes the data requested. If Clinical Partners does not process any data it will inform the data subject accordingly.
7. Clinical Partners will, at all times ensure this internal SAR policy is followed and progress is monitored.
8. Ensure data is not changed as a result of the SAR. However, routine changes as part of the processing activities concerned are permitted.
9. Verify whether the data requested also involves data on other data subjects and will make sure this data is filtered before the requested data is supplied to the data subject. If data cannot be filtered, Clinical Partners will ensure that other data subjects have consented to the supply of their data as part of the SAR.
10. Clinical Partners will promptly acknowledge receipt of the SAR.

3. **Where data on the data subject is processed, Clinical Partners will provide the following information in the SAR response:**

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data, such as Binding Corporate Rules1 or EU model clauses2;
d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with the Information Commissioner's Office ("ICO");
g) if the data has not been collected from the data subject, the source of such data;

h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

i) Provide a copy of the personal data undergoing processing.

Procedure to be followed on Receipt of a Subject Access Request

A Subject Access Request may be received by any member of staff or partners, therefore, all staff and partners are to be aware of the following procedure.

On receipt of a Subject Access Request the following actions must be completed:

1. On receipt of a subject access request, the person receiving it must forward it immediately to the CEO.
2. The CEO will log the request on its SAR's log sheet.
3. The CEO will identify whether a request has been made under the Data Protection legislation.
4. The CEO may ask any member of staff, and as appropriate, partner, to locate and supply personal data relating to an SAR and make a full exhaustive search of the records to which they have access.
5. All the personal data that has been requested must be provided unless an exemption can be applied.
6. The CEO will respond within one calendar month after accepting the request as valid.
7. Subject Access Requests must be undertaken free of charge to the requester unless the legislation permits reasonable fees to be charged.
8. The CEO must ensure that the staff and partners are aware of and follow this guidance.
9. Where a requester is not satisfied with a response to an SAR, Clinical Partners must manage this as a complaint.

In Managing a Subject Access Request the CEO as Clinical Partners Caldicott Guardian must:

1. Notify the Chair of the Information Governance Group upon receipt of a request
2. Ensure where a request has been received in writing that the data subject is asking for sufficiently well-defined personal data held by Clinical Partners relating to the data subject.
3. Clarify with the requester following any verbal request what personal data they need.
4. Ensure that Clinical Partners has valid evidence to prove the requesters identity and address.
5. Depending on the degree to which personal data is organised and structured, search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs), telephone recordings, paper records in relevant filing systems etc. which Clinical Partners have responsibility for or owns.
6. Ensure Clinical Partners does not withhold personal data because it is believed it will be misunderstood; instead, an explanation should be provided with the personal data.
7. Provide personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms.
8. Supply the personal data in a format as agreed by the requester and Clinical Partners.

9. Redact any exempt personal data from the released documents and provide an explanation of why that personal data is being withheld is to be provided.
    - Third party
    - Could cause serious harm to the physical or mental health or condition of the Data Subject, or any other person (refer to the Exemption from Article 15 of the GDPR – Serious Harm
    - Legal Privilege – information that relates to legal advice is classed as legally privileged and is therefore exempt from the GDPR provisions
10. Inform patients of their rights and the information it holds on its website and on forms.
11. Maintain a database allowing Clinical Partners to report on the volume of requests and compliance against the statutory timescale, action taken following a request and reasons for any action or refusal of a request.
12. Advise the requester that they may complain to the Information Commissioner's Office ("ICO") if they remain unhappy with the outcome.

Appendices 3

Clinical Partners
Subject access request form
Data Protection Act 2018 and General Data Protection Regulation (GDPR)

Section 1: Details of the data subject (person to whom the information relates)	
Title:	
Forenames:	
Surname	
Address (for correspondence):	
Telephone number:	
E-mail address:	
Preferred communication method	

Section 2: Identification	
Identity documentation may be required in order for us to process your request. Please provide us with a copy of either your passport or driving licence, and a copy of one utility bill showing your current residential address. Please complete the checklist below to indicate what you have enclosed with this form. **Please Note** – The copy identity documentation will be shredded once we have verified your identity.	
ID supplied	**Tick**
Copy of passport / driving licence	
Copy of utility bill	

Section 3: If applicable the details of person acting on behalf of the data subject	
Title:	
Forenames:	
Surname:	
Address:	
Telephone number:	
E-mail address:	
Relationship to data subject	

Preferred communication method	

To authorise another person to make this subject access request on your behalf, please sign the statement below.

I hereby give my authority for _____

(Full name of the person) to make a subject access request on my behalf under the Data Protection legislation to Clinical Partners.

Signed: _____ Date: _____

Print name: _____

NOTE: The data subject must also sign the declaration in Section 5.

Section 4: Details of information that you believe we hold and to which you require access.

Please describe the information that you believe we hold and to which you are seeking access. If you can be specific about the information that you would like, it will assist us to local it (if we hold it). If we require further details about the information that you are requesting, we will contact you.

Section 5: Data subject declaration

I certify that the information given on this form is true. I understand that Clinical Partners may need to obtain further information in order to comply with this request

Data Subject

Signed: _____ Date: _____

Print name: _____

Please return this form with proof of identity to:

Clinical Partners
Unit 6 Chaldicott Barns
Tokes Lane
Semley
SP7 9AW

Template response letters

Acknowledgement Letter to Applicant (delete header before sending)

(Insert name and address of applicant/representative)

Clinical Partners
Unit 6 Chaldicott Barns
Tokes Lane
Semley
SP7 9AW

Dear (insert title and name of applicant/representative)

Ref: Subject Access Request under the Data Protection Act 2018.

Thank you for your correspondence of (insert date of request) with reference to your application for access to personal information in respect of (insert name of data subject)

The statutory timescale for responding to a Subject Access Request made under the Data Protection Act 2018 is a calendar month. I can confirm that we will make every attempt to respond to your request within a 28 calendar day

period. If your request is complex or we believe we may not be able to meet the 28 calendar day period we will inform you of this.

If the applicant is unknown to us or wishes to use a third party or they have not applied in writing with a clear request insert:
The law allows us to take reasonable steps to establish and confirm your identity before providing any personal information. The 28 calendar day period may be suspended whilst your identity is checked. We would be grateful if you would provide a copy of your;

a) Driving licence or Passport or birth certificate
b) Additional proof of address, e.g. a utility bill (no longer than 3 months old) etc.
c) Completion of the Subject access request form with details of the person who may act on your behalf.

Please return all documentation to the address identified above.

Yours sincerely