Information Governance Policy

Nominated Individual	Richard Drakeford
Registered Manager	Robin Page
Date Policy Completed	February 2025
Version no.	1.0
Previous Review Dates	2/26
Review Date	February 2027(or when updates are required)
Applicable to	All staff and contractors
Policy Signed By	RICHARD DRAKEFORD

Contents

1.0 Introduction

The purpose of Information Governance is to give assurance to service users and staff that their personal information is managed legally and securely. Where data is stored effectively, people will receive safe and effective care.

Re-Pat Ltd recognises the importance of effectively managing information across the service.

Re-Pat Ltd will use appropriate policies, procedures, management accountability and structures as part of their information governance framework.

Policy Statement

It is the responsibility of all employees to follow this policy.

Re-Pat Ltd will ensure that all employees are aware of this policy and receive adequate training in information governance.

Information Governance training will be classified as a statutory requirement as part of the employee induction programme.

All new team members will receive information governance training relevant to their role, as soon as employment is commenced. The training will be annual and guidance and support on this subject will be available to all employees if needed.

Re-Pat Ltd will ensure personal data will be:
• obtained, held and processed fairly
• held for specific purposes and used only for these purposes
• processed in accordance with the rights of the data subject
• relevant, accurate and kept up to date
• corrected if shown to be inaccurate
• kept for no longer than necessary and destroyed when no longer required, in line with best practice
• protected against loss or unauthorised or unlawful processing, accidental loss and destruction or damage using appropriate technical or organisational measures.

2.0 Scope

This policy applies to all Re-Pat Ltd employees and to all personal data processed by the company relatable to any identifiable living person.

3.0 Definitions

- Data subject: the individual about whom personal data has been collected.
- Data Protection Act 2018: an Act of Parliament that updates data protection laws in the UK. Following UK departure from the European Union, DPA 2018 continues to apply, and provisions of the EU GDPR were incorporated directly into UK law. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context.

- Personal data: any information about a living person including, but not limited to, names, email addresses, postal addresses, job roles, photographs, CCTV and special categories of data, as defined below.
- Process or processing: doing anything with personal data, including, but not limited to, collecting, storing, holding, using, amending or transferring it. You do not need to be doing anything actively with the personal data; at the point you collect it, you are processing it.
- Special categories of data: has an equivalent meaning to 'sensitive personal data' under the Data Protection Act 2018. Special categories of data include but are not limited to, medical and health records (including information collected as a result of providing health care services) and information about a person's religious beliefs, ethnic origin and race, sexual orientation and political views. Data controller: the main decision-maker over the management of the data in question. They exercise overall control over the purposes and means of the processing of personal data.

For the purposes of this policy, Re-Pat Ltd considers itself to be a data controller with respect to all team members and service users. Data processor: acts on behalf of and only on the instructions of the relevant controller. For the purposes of this policy, Re-Pat Ltd considers that they are the data processor in relation to the service delivered to its service users.

4.0 Roles and Responsibilities

Employees

Employees handle information in various ways. Employees, who in the course of their work, create, use, or otherwise process information have a duty to adhere to relevant legislation, case law and national guidance.

All employees of Re-Pat Ltd are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

Director

The Company Director/Nominated Individual has overall responsibility for information governance within the company. Re-Pat Ltd is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

Senior Information Risk Owner (SIRO)

The role of Senior Information Risk Owner (SIRO) in the company has been assigned to – **The Registered Manager**

The SIRO is responsible for leading on Information Risk and for overseeing the development of this policy.

The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk.

Caldicott Guardian

The role of Caldicott Guardian has been assigned to the Company Director.

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of service information and enabling appropriate information sharing.

Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) will lead on all matters pertaining to Information Governance. The DPO will maintain the confidence of service users, employees and the public, through advice and

guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle data.
This includes ensuring that the company is fully compliant with all information governance-related legislation and that the company meets statutory and mandatory obligations through the development of strategy and implementation of Information Governance policies.
The Registered Manager is the company's Data Protection Officer.

5.0 Procedures

Information Asset Register
Any computerised or manual filing system which contains information relating to an individual who can be either directly or indirectly identified i.e. name, ID number, location or online identifier must be logged in the information asset register.
Re-Pat Ltd.'s information asset register will record:

- The area of the service to which the entry relates
- The name of the computer system, manual files or both where the information is kept
- Who the information is about
- The nature of the information held (including sensitive information)
- How the data is protected (i.e. restricted access, two-factor authentication etc)
- How long the data will be retained for
- The information asset owner.

Personal Identifiable Data Audits (PID)
Re-Pat Ltd will carry out PID Audits to identify personal data being processed and to keep the Information Asset Register updated.
This will be the responsibility of Re-Pat Ltd.'s Data Protection Officer (DPO).
PID Audit forms will be available from the DPO.
The audit will include the following information:

- Whom the information held is about
- What the information is
- If the date is sensitive, personal data
- The format of that data i.e. name, address, phone Number
- How the information is stored
- Why the information is being held by the company
- How it was collected
- Whom it was collected from.

Access to Information and Disclosure Outside of Re-Pat Ltd
All employees will have access to the information required to carry out their roles.
It is all employee's responsibility to share the information on a need-to-know basis and respect confidentiality.
If Re-Pat Ltd deems it necessary to share PID the correct parameters of appropriateness will be maintained in accordance with relevant protocols and agreements in place between organisations. For example, employees will not disclose details of an employee's sexual orientation if only their name and National Insurance Number are required by HMRC.

Security Breach Notification and Investigation

A data breach is classed as a security incident that has affected the confidentiality, integrity or availability of personal data.
If the data is lost, destroyed, corrupted or disclosed or if someone accesses the data or passes it on without proper authorisation this is considered a breach. It is also considered a breach if the data is

made unavailable, for example, when it has been encrypted by ransomware or accidentally lost or destroyed
Suspected or actual GDPR breaches will be reported immediately to the DPO. As much information as possible should be provided by the party involved.
The DPO will then investigate and produce a report for the senior management team, advising if the breach needs to be reported to the Information Commissioner's Office (ICO).
The DPO will use the information provided on the ICO website regarding the reporting of breaches.
Re-Pat Ltd will be required to notify the ICO of any breach that presents or is likely to present a risk to the rights and freedoms of the data subjects.
Any decisions not to report a breach must be rationalised, documented and kept on record.
Any lessons learned as a result of the potential breach should be shared in line with Re-Pat Ltd.'s Incident Management Policy.

Individual Rights

Subject Access Requests (SARS)
Individuals have the right to submit a SAR to an organisation if they wish to gain access to their personal data to verify if it is being processed lawfully.
If an SAR is submitted and then validated Re-Pat Ltd will provide access within 1 month. However, if the requests are numerous or complex Re-Pat Ltd reserves the right to extend this period to two months. If the latter is the case then Re-Pat Ltd will inform the individual within 1 month of the receipt of the initial request.
The DPO must be informed of any SARs and verification of identity must be sought prior to any information being released. Re-Pat Ltd will keep a record of all SARs.
Information will be provided free of charge for the initial copy if all the above conditions are met however, if further copies are required Re-Pat Ltd may charge a small fee to cover administrative costs.
Manual data requests will be reviewed first and any information pertaining to third parties will be removed or anonymised unless prior consent is obtained.
Electronic requests will be responded to in an electronic format.
Re-Pat Ltd reserves the right to refuse any SARs which are deemed to be unfounded or excessive. In these circumstances, the requester will be informed of the rationale for the decision not to share the information within one month of the request and signposted to the ICO.

The Right to be Informed

Re-Pat Ltd will supply all employees with an easily accessible privacy notice detailing how the company will process their personal information. The notice will be written in plain, concise language which is transparent and easy to understand.
In circumstances where data has been obtained both directly and indirectly from a data subject the following information will be supplied within the privacy notice –

- the identity and contact details of Re-Pat Ltd and the Data Protection Officer
- the purpose of and the legal basis for processing the data
- the legitimate interest of Re-Pat Ltd (if applicable) or a third party
- any recipient categories of recipients of the personal data
- any international transfers of data
- length of time the data will be stored for
- existence of the data subject's rights, including the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

The privacy notice should also refer to any online information collated such as cookies. In relation to cookies, Re-Pat Ltd will:
• inform people accordingly
• explain what the cookies are for
• ask for the person's consent to store a cookie on their device. New consent may be required if the use of cookies changes over time.

Right to Rectification

Where personal data held is found to be inaccurate, individuals hold the right to have any inaccuracies rectified.
If the inaccurate data has been disclosed to third parties, Re-Pat Ltd will inform them of the rectification and inform the individual to which third parties the data has been disclosed.
Re-Pat Ltd will respond to the rectification request within one month, with an extension of two months if the rectification is complex.
If rectification is deemed unnecessary Re-Pat Ltd will inform the individual of the decision not to rectify and the rationale for doing so within one month of receipt of the initial request. The individual will then be sign-posted to the ICO should they wish to take the matter further.

The Right to Data Portability

Re-Pat Ltd recognises that individual has the right to use their personal data for their own purposes across a variety of services. Data can be moved across IT environments as long as this is done securely.
The right to data portability is only recognised in the following situations:
• personal data that has been provided by an individual to a data controller
• processing is based on consent or is contractual
• automated processing.
Re-Pat Ltd will provide personal data free of charge in a structured, machine-readable format.
If the personal data concerns more than one individual, Re-Pat Ltd will take that individual right to privacy into consideration.
Requests for portability will be responded to within one month unless the request is deemed complex or a number of requests have been received, in which case Re-Pat Ltd's response time will be within two months.
If no action is to be taken regarding a portability request, Re-Pat Ltd will explain the reasoning behind this to the individual and sign and post them to the Information Commissioner's Office should they wish to raise a complaint. This will be done within one month from the receipt of the request.

Right to Removal of Data

If there is no justifiable or compelling reason for the continuation of personal data being processed Re-Pat Ltd is aware of an individual's right to request that data be removed or deleted.
In order for the right to erasure to be recognised the following criteria should be met:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected
- Consent to process the data has been withdrawn
- The individual objects to the processing and there is no overriding legitimate interest for processing to continue
- The personal data has been processed unlawfully
- There is a legal obligation to erase the personal data.

Re-Pat Ltd will refuse data removal if this has been processed for the following reasons:

- to exercise the right of freedom of expression and information

- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes
- the exercise or defence of legal claims.

If personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, Re-Pat Ltd will inform the other organisations who process the personal data to erase the personal data in question.

Right to Restrict Processing

Re-Pat Ltd recognises that individuals have the right to stop their personal data from being processed. In these circumstances, Re-Pat Ltd will store but not process the data in order to ensure that this restriction is respected in the future.
Re-Pat Ltd will restrict the processing of personal data in the following circumstances:

- The data processing is deemed unlawful and erasure is opposed by the individual
- Re-Pat Ltd no longer requires the data however, the individual requires the data in relation to a legal claim
- If the accuracy of the data is being contested Re-Pat Ltd will restrict processing until the accuracy has been verified.

Any third parties to whom data has been shared will be informed by Re-Pat Ltd regarding the restrictions on the processing of personal data unless the effort to do so is considered impossible or disproportionate.

Fair and Lawful Processing

Re-Pat Ltd will ensure any data processed is done in accordance with GDPR principles.
To do this, when processing data Re-Pat Ltd will ensure:

- Consent has been obtained from the data subject

Processing is necessary due to one or more of the following:

- compliance with legal obligations
- for public best interest purpose
- contractual obligations
- protection of interests pertaining to the individual
- official authority vested in the controller
- for the purpose of the legitimate interest pursued by the controller or a third party, unless those interests are in conflict with the interests, freedoms or rights of the individual.

Sensitive Data

Sensitive data is information that is not accessible to everyone and that might result in the loss of an advantage or level of security if disclosed to others. Sensitive data can include personal information such as racial or ethnic origin, political opinions, religious beliefs, sexual orientation, health or genetic information, or criminal record
Re-Pat Ltd will only process sensitive data under the following conditions:

- For purposes advised directly or non-directly within the Register of Data Controllers published by the ICO
- In order to comply with the law
- In order to carry out contractual obligations or to establish a contract
- If it is in the organisation's legitimate business interests.

In the case of Sensitive data, Re-Pat Ltd will always obtain explicit consent unless:

- The data has been obtained in order to monitor a protected characteristic i.e. Racial/ethnic origin for the purpose of ensuring equality
- The data is related to the employment of individuals
- The data is required for the provision of advice or support but the data subject is unable to or cannot be expected to give explicit consent.

Re-Pat Ltd will not disclose any personal data to third parties unless:

- There is a legal or ethical obligation to do so
- The data subject is physically or legally incapable of consenting
- To facilitate the establishment, exercise or defence of legal claims
- It is in the public best interest on the basis of UK law, which is proportionate to the aim and contains appropriate safeguards
- For the purposes of medicine, for assessing the working capacity of employees, medical diagnosis, the provision of health, social care, treatment, management of health, or social care systems and services on the basis of UK law or a contract with a health professional
- 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 healthcare and of medicinal products or medical devices
- For archiving purposes in the public interest, scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Any disclosure of personal data to a third party must be documented in the relevant personnel or service user record, authorised by a member of the management team and limited to the minimum information required.

Data Privacy Impact Assessments (DPIA)

Re-Pat Ltd will always act in accordance with GDPR requirements by using a privacy-by-design approach.
Re-Pat Ltd will ensure that a DPIA will be carried out for any processing operation that is “likely to result in a high risk to the rights and freedoms of natural persons”. Re-Pat Ltd will use DPIAs to ensure the organisation complies with data protection obligations or when using new technology.
All DPIAs will include the following information:

- a description of the processing operations and purposes
- an assessment of the necessity and proportionality of the processing in relation to the purpose
- an outline of the risks to individuals
- the measures implemented to address risk.

Retaining Information

Re-Pat Ltd understands its obligations regarding the retention of personal data.
If a retention period is not specified Re-Pat Ltd will only hold information if we are required by law to do so and for as long as it is required for its purpose.

Re-Pat Ltd will follow the most up-to-date statutory and best practice guidelines in relation to data retention. All records will be retained in accordance with the relevant legislation or guidance i.e. The NHS Records Management Code of Practice
All healthcare records will be retained in line with the Private and Voluntary Health Care (England) Regulations 2001.

Disposal of Data

Any paper records held by Re-Pat Ltd which are no longer required will be disposed of securely and confidentiality.
Re-Pat Ltd will ensure that paper data is disposed of securely i.e. shredding and the use of a confidential waste bin.
Electronic data will be permanently deleted when required from Re-Pat Ltd's IT system, by an ISO-accredited IT specialist.
Should any removable storage media become no longer fit for purpose i.e. external hard drives, Re-Pat Ltd will ensure all data is wiped and that the equipment is disposed of appropriately.

Cease of Trade

Should Re-Pat Ltd cease trading due to being purchased by another organisation, all data will be transferred over to the new service.
Should Re-Pat Ltd cease trading altogether, the company will ensure all records are stored securely in an electronic format. All records will continue to be stored in line with statutory guidelines and best practices.
Re-Pat Ltd recognises the legal obligation held relating to how long data should be retained for, ICO registration and that data protection laws continue to apply.

Data Collection

Re-Pat Ltd will offer service users and employees an opportunity to confirm the accuracy of personal data held. Any changes highlighted will be updated promptly on the appropriate computer system and saved in the relevant care record or personnel file.

Disclosure of Data

Re-Pat Ltd will ensure any data held is protected from unauthorised access by using appropriate security methods in relation to the access and storage of the data.
Personal data will not be disclosed to data processors unless a contract/confidentiality agreement is in place defining authorised data usage.
Employees at Re-Pat Ltd will not disclose any personal data via the telephone unless the requesters' identity can be formally verified.

Disclosing Data to Third Parties

Re-Pat Ltd will not disclose personal data to a third party unless their identity can be formally verified and one of the following conditions are met:

- Re-Pat Ltd has given consent to the sharing of the information with the third party
- The data subject or individual holding Lasting Power of Attorney for the data subject has given consent to share the information with the third party or for the third party to request the information
- Sharing the data is essential for the lawful purpose for which the data is being processed
- Disclosure is subject to the terms of a formal Information Sharing Protocol
- The information must be shared in order to prevent or detect a crime, in relation to the apprehension or prosecution of an offender or for purposes pertaining to the assessment or collection of tax

Re-Pat Ltd will only share sensitive information with a third party if the data subject has given their consent for disclosure for the third party to request the information, or if disclosure is deemed a best interest decision made in line with the Mental Capacity Act.
Sensitive information will also be disclosed to a third party if Re-Pat Ltd is required to share the information by Law or if the disclosure is in the vital interest of the data subject.
In the above circumstances, authorisation must be sought from the DPO before disclosure can take place.
Any information shared with third parties will be the minimal amount required to satisfy contractual or legitimate requirements.
Consent in relation to sensitive data must be explicit to the purpose and the decision to disclose should be recorded on the appropriate IT system.

Secondary Uses of Data
On occasion, Re-Pat Ltd may wish to use data for purposes not directly related to the care of the service user i.e. research or audit purposes, commissioning, performance or capacity management. In such cases, pseudonyms will be used in order to protect anonymity and maintain confidentiality.

Security of Information
Re-Pat Ltd has systems in place to manage risk and identify needs in relation to the security of information throughout the organisation.
Risk management is necessary to ensure data is protected and regulatory requirements are met.
Re-Pat Ltd will undertake the following actions to ensure information is handled and stored securely:

- The implementation of a clear desk policy within our office space so that no personal or sensitive information is left unattended and accessible to those unauthorised to view the information
- Company IT devices and emails are encrypted
- All information assets and processing facilities are protected securely from unauthorised access
- Unsupported systems (i.e. software, hardware or applications) are easily identified so they can be removed, replaced or risk assessed
- Confidentiality and integrity of information is a priority and will be maintained
- Re-Pat Ltd's requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities are met
- All legal and statutory obligations are met
- Security of information will be maintained as per Re-Pat Ltd's business continuity plan.

Users will only have access to Re-Pat Ltd.'s systems, data and network if they have formally agreed to comply with this policy.
This will form part of all employee and contractor contracts and will also be part of mandatory training requirements.
Unauthorised and illegal use of information assets and information processing facilities is prohibited.
Use of non-company-approved web applications to process confidential information is not permitted without this being approved for use by the directors.

Computers
Employees are not permitted to store PID on non-company-owned equipment.
IT assets will have a named information asset owner responsible for the security of information relating to that asset. The information asset register will be maintained by the IT Team.

All new information systems must be designed to take into account information security and data protection requirements and the management of computers and networks should be controlled through documented procedures.
The Information Asset Owner is responsible for ensuring the security of data stored in the named system. Any changes to information systems, applications or networks should be reviewed and approved in accordance with a documented change management process.
All information products will be licensed, and systems will be in place to ensure that users cannot install unauthorised software onto any company-owned property.
Equipment and sensitive data files will be encrypted and password protected.
No personally identifiable data will be stored on hard drives unless authorised by the DPO.
Files should be stored on Re-Pat Ltd secure network and backed up centrally by the IT team.
Files containing individual person-identifiable information on portable computers should be password-protected. Files stored on network drives do not require password protection, as a password is needed to log on to the network and access to folders is restricted.
Users should not leave devices logged in whilst unattended and screens should be locked if the user is not present.
Computers should not be transferred between users or disposed of, other than through the IT team as they have the means of transferring or removing all data from the hard drive.

Portable Devices

If an employee is using a company-owned laptop, tablet, handheld computer, mobile phone or a combination of these this presents a risk to data security.
Users of portable devices must ensure that their device is logged on to the network on a regular basis in order to receive regular updates to software and anti-virus signature files.
If a virus is discovered it should be immediately reported to an IT specialist and the device and any media used with it, quarantined immediately for inspection and cleaning.
Re-Pat Ltd will use software countermeasures and management procedures to protect itself against the threat of malicious software.
It is the individual employee's responsibility to always keep their devices safe and secure.

Email

Employees are not permitted to use their emails for work purposes. PID can only be sent through a secure, encrypted email address or as a password-protected file.
Steps should be taken to ensure that confidential/sensitive information is sent to the mailbox of the person or persons authorised to see that information. Use must be made of the email tracking Options where available, to notify that a message has been delivered and/or read or the sender must be telephoned to confirm receipt.

Telephones

Employees at Re-Pat Ltd understand they have an obligation to not divulge any information about service users or fellow employees over the phone to anyone without the authority to receive that information.
If the employee taking the call has any doubts about the identity of the requester, they should contact the DPO for advice.
If the caller claims to be from an organisation with a right to obtain information about a particular data subject (i.e. NMC), the telephone number should be obtained and checked to verify its validity and identity.

Video Conferencing

In the event that video conferencing is utilised by Re-Pat Ltd for any reason, a Data Protection Impact Assessment will be carried out to identify and manage any potential risks to an individual's rights to privacy.
Re-Pat Ltd will ensure that:

- Adequate privacy settings are in place on all software being used to facilitate the conference
- That the data subjects' rights have been taken into consideration
- Employees are using an appropriate background with no identifiable information visible, and no other unauthorised party is able to hear the conversation from the room or anywhere nearby
- The conference is not recorded without the consent of all persons involved

Use of Third Parties to Manage/Process Data

Re-Pat Ltd will always carry out robust risk assessments and due diligence checks when using a third party to manage or process data.
All information security requirements will be detailed in a contract between Re-Pat Ltd and the third party.
Re-Pat Ltd will use the following reputable and secure third parties to store, manage or process data: HLTH Manage.

Record Keeping

Re-Pat Ltd will ensure that all service user care records are accessible to all authorised employees who require access to such records in order to perform their duties.
All service user care records should be:

- Clear concise and free from technical terminology or jargon
- Free from abbreviation
- Factually accurate and relevant
- Free from personal opinion or irrelevant information
- Clearly marked with the date and time if the record pertains to care provided or a service user incident
- Any paper records should be legible and written in indelible, black ink
- Alterations to paper records should be scored out with a single line. Correction fluid may not be used if an error is made

Re-Pat Ltd.'s service user care records will be documented and stored securely, and electronically. Paper records will only be used in the event of a system failure and these will be scanned and updated onto the system once the fault is rectified, then disposed of securely.
All service user care records will be documented in a consistent, professional manner and will adhere to Health Care Record Keeping Standards.

Freedom of Information

Re-Pat Ltd is only required to provide information under the Freedom of Information Act 2000 in respect of the activities that it carries out whilst under contract with a public authority. As such, Re-Pat Ltd is not required to respond to FOI requests received directly from members of the public in relation to any other of its commercial activities. If such a request is received, the Registered Manager should refer the requesting party to the scope of the legislation and politely decline to provide the information.

Upon receipt of an FOI request, the Registered Manager will endeavour to ensure that the requested information is collated and returned to the contracting public authority to allow them to meet the 20-working day deadline of the legislation. Prior to sending any information it should be checked for any personal data, which should be redacted prior to sending.

In certain circumstances, Re-Pat Ltd may be asked for our views as to whether certain information should be released before the public body decides how to respond. The person responsible for making this decision for Re-Pat Ltd would be the Registered Manager.

If Re-Pat Ltd provides any information to a public body on the understanding that it is confidential, this should be highlighted on the documents provided. If the information has not been provided to a public body on a confidential basis, the public body may consult with Re-Pat Ltd as to whether any exemptions under the legislation may apply (for example prejudicing commercial interests).

6.0 Monitoring

The Data Protection officer for Re-Pat Ltd is responsible for monitoring this policy. This policy will be monitored as part of the monthly Management Team meeting and on an individual 1:1 basis with employees. The contents of this policy will be reviewed on an annual basis, sooner should changes in the law or legislation dictate.

7.0 Related Policies and Procedures

Quality, Governance and Risk Policy
Business Continuity Policy
Record Keeping Policy
Booking Policy

8.0 Legislation and Guidance

Data Protection Act 2018
Freedom of Information Act 2000
UK General Data Protection Regulation
Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003
Private and Voluntary Health Care (England) Regulations 2001
The Information Governance Review (publishing.service.gov.uk)
UK GDPR guidance and resources | ICO
information-security-policy-v4.0.pdf (england.nhs.uk)
The Private and Voluntary Health Care (England) Regulations 2001 (legislation.gov.uk)
Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)