Confidentiality Agreement for Third Parties

Contractual Agreement
between
Physiotherapy2fit and
Third Party Contractors

First introduced September 2012
Review Date 1st February 2018
Next Review Due 12th February 2020

Physiotherapy2fit Ltd is committed to ensuring that, as far as it is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on the basis of their age, disability, gender, race, religion/belief or sexual orientation. Should a member of staff or any other person require access to this policy in another language or format (such as Braille or large print) we will do our best to provide this in a format the user is able to access. Physiotherapy2fit Ltd will do its utmost to support and develop equitable access to all policies. The Director is responsible for ensuring staff are aware of Physiotherapy2fit Ltd policies and that staff adhere to them. It is also the Director's responsibility to keep staff up to date with new policy changes.

Staff are responsible for ensuring they are familiar with policies, know where to locate the documents on Physiotherapy2fit's main website, and seek out every opportunity to keep up to date with them

Independent contractors are expected to identify a lead person to be responsible for ensuring staff employed within their place of work are aware of Physiotherapy2fit Ltd policies.

INTRODUCTION

P2F uses the services of third party Contractors, who in their line of their duty, may have access to P2F data.

P2F must ensure that it has formal contractual arrangements that include compliance with information governance requirements with all Contractors and support organisations.

P2F are under a common law duty to ensure that confidential information is protected from inappropriate disclosure. Furthermore, under Principle 1 of the Data Protection Act 1998, personal information must be processed (disclosed) fairly and lawfully. P2F will only be able to comply with these duties where it has ensured that third parties with whom it contracts are subject to, and comply with, patient confidentiality, information security and data protection requirements.

PURPOSE

This document forms a contract, the purpose of which is to:-

1. Maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
2. Implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

SCOPE

This agreement is binding and forms a contract between Physiotherapy2fit Ltd and the named third party Contractor.

GENERAL CLAUSES

The Contractor undertakes:

1. To treat as confidential, all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the Contractor or an employee, servant or agent or sub- Contractor of the Contractor as a result or in connection with the contract
2. To provide all necessary precautions to ensure that all such information is treated as confidential by the Contractor, his/her employees, servants, agents or sub-Contractors
3. To ensure that he/she, his/her employees, servants, agents and sub- Contractors are aware of the provisions of the Data Protection Act 1998 and ISO 27002 and that any personal information obtained from the Trust shall not be disclosed or used in any unlawful manner
4. To indemnify the Trust against any loss, damage and/or costs arising under the Data Protection Act 1998 and/or at common law , or any monetary or other civil penalty imposed caused by any action, authorised or unauthorised, taken by him/herself, his/her employees, servants, agents or sub-Contractors.
5. To notify in a timely manner, P2F of any requests from a data subject to have access to their personal data, and of any requests relating to the P2F's obligations under Data Protection legislation.

6. To comply with the P2F's Information Security Policy, particularly with regard to malware, and back up processes, where appropriate.
7. To provide the P2F with a copy of their own Information Security Policy, Business Continuity & Disaster Recovery Plan, and any certification that they may have obtained, e.g. under ISO 27001.

SUPPLIER CODE OF PRACTICE

1. The following Code of Practice applies where access is obtained to P2F personal data/information, as defined within the Data Protection Act 1998, for the purpose of preventative maintenance, fault diagnosis, hardware or software testing, repair, upgrade, replacement or any other related activity.
2. The access referred to in paragraph 1 above may include:-

    - Access to data/information on the P2F's premises
    - Access to data/information from a remote site
    - Examination, testing and repair of media (e.g. fixed disc assemblies)
    - Examination of software dumps
    - Processing, using P2F data/information

3. The Contractor must certify that his/her organisation is registered appropriately under the Data Protection Act 1998 and legally entitled to undertake the work proposed. (see Appendix 1)
4. All employees, servants, agents and/or sub-Contractors of the Contractor will be required to agree to and sign a confidentiality statement when they come to any of P2F's sites or access P2F data remotely where they may see or have access to confidential personal and/or business information (see Appendix 2).
5. The Contractor must undertake not to transfer the personal data/information out of the UK unless such a transfer has been approved by P2F and is one of the following:

    •a country within the European Economic Area;

    •the country to which information is to be transferred has been deemed to have an adequate level of protection for personal information; or

    •is a USA company which has signed up to a Safe Harbor agreement.

6. The work shall be done only by authorised employees, servants, or agents of the Contractor (except as provided in the paragraph 13 below) who are aware of the requirements of the Data Protection Act 1998 and of their personal responsibilities under the Act to maintain the security of the personal data/information held by P2F.
7. While the data/information is in the custody of the Contractor, it shall be kept in appropriately secure means.
8. Any data/information sent by post from one place to another, by or for the Contractor, shall be secure e.g courier, registered post. These places should be within the Contractor's own organisation or an approved sub- Contractor.
9. Data/Information which can identify any patient/employee of P2F must only be transferred electronically if previously agreed by P2F, and with agreed appropriate security, e.g. secure or encrypted email, password protected attachments to email. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 1998 and ISO 27002.
10. All direct-dial access to a computer held database by the Contractor or their agent will be controlled by P2F, and require contact to open such access on all occasions, and the access will be immediately closed once the task is complete.

11. The data/information must not be copied or otherwise used for any other purpose than that agreed by the Contractor and P2F.
12. Where personal data/information is recorded in any intelligible form, it shall either be returned to P2F on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to P2F.
13. Where the Contractor sub-contracts any work for the purposes in paragraph 6 above, the Contractor shall require the sub-Contractor to observe the standards set out above, and the P2F must be informed that the subcontract is to be entered into.
14. P2F shall, wherever practical, arrange for the equipment or software to be maintained, repaired or tested using dummy data that does not include the disclosure of any personal data/information.
15. P2F reserves the right to audit the Contractor's contractual responsibilities in respect of information security or to have those audits carried out by a third party.
16. Any security breaches or near misses made by the Contractor's employees, agents or sub-Contractors will immediately be reported to the Director.
17. P2F will expect to be a part of an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-Contractors, and to be notified of the outcome of investigations.

Appendix 1: CERTIFICATION FORM

Name of Contractor:

Address of Contractor:

Telephone Number:

Email:

On behalf of the above organisation I certify as follows: -

- The organisation is appropriately registered under the Data Protection Act 1998 and is legally entitled to undertake the work agreed in the contract agreed with the Authority/Trust/Practice and,

- The organisation will abide by the requirements set out above for handling any of the Physiotherapy2fit personal data/information disclosed to my organisation during the performance of such contracts.

Signed:

Print Name of Individual:

Position within Organisation:

Date:

DPA Registration Number:

Appendix 2: AGREEMENT OF PERSONAL RESPONSIBILITY

Confidential information includes all information relating to the business of P2F and its patients and employees.

The Data Protection Act 1998 regulates the use of all personal information and included electronic and paper records of identifiable individuals (patients and staff). P2F is registered in accordance with this legislation. If you are found to have used any information you have gained whilst contracted by P2F, you and your employer may face legal action.

During the course of your time within P2F buildings, or logging on remotely to P2F systems, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties as detailed in the contract between the P2F and your employer. This condition applies during your time within the P2F and after that ceases. Breach of confidence, including the improper passing of registered computer data, will result in disciplinary action, which may lead to your dismissal.

You must ensure that all records, including VDU screens and computer printouts of registered data, are never left in such a manner that unauthorised persons can obtain access to them. VDU screens must always be cleared when left unattended and you must ensure you log out of computer systems, removing your password. All computer passwords must be kept confidential.

I, the undersigned, understand that I am bound by a duty of confidentiality and agree to adhere to the conditions within the Contract between P2F and my personal responsibilities to comply with the requirements of the Data Protection Act 1998.

NAME OF ORGANISATION:

NAME AND POSITION/DESIGNATION (PRINT):

SIGNATURE:

DATE:

Appendix 3: IT CONTRACTOR POLICY

IT Contractor Policy

INTRODUCTION

Use of external support or third party contractors is an essential element of the overall IT infrastructure support. The use of such contracts and external suppliers are used to support and facilitate specialist software, network or hardware services.

PURPOSE

This policy covers the provision of facilities by P2F to enable staff working on its behalf to have secure and reliable access to any of the P2F's information systems for which they have been authorised to use. Access could be from locations other than the P2F's estate to support services.

P2F has produced this policy to provide staff and third party suppliers a clear understanding of their responsibilities and the measures that need to be in place to ensure that any remote or on site works are carried out safely and securely with preventative measures in place for any hazards or risks.

OBJECTIVES

The objectives of this policy are to:

- clarify P2F policy regarding acceptable and unacceptable use of on-site remote working practices.
- provide secure and resilient access to the P2F's information systems.
- preserve the integrity, availability and confidentiality of the P2F's information and information systems.
- manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in security.
- comply with all relevant regulatory and legislative requirements (including data protection laws) and to ensure that the P2F is adequately protected under computer misuse legislation.
- aide the Trust with a concise yet clear audit trail of third party access to P2F information systems.

SCOPE

All staff identified to access P2F equipment or information systems either remotely or on site and on behalf of the P2F is subject to the requirements of this policy.

DEFINITIONS

Person Identifiable Information/Data	Any information relating to an individual (including, but not limited to: name, address, date of birth, district/NHS number, NI number), which, either alone or in combination with other information that may be in the possession of the recipient, may serve to identify the individual.

VPN	Virtual Private Network (VPN) VPN is a connection made between one network and another. VPN is used to connect to the P2F's network in order for an individual to work at a location that is not located within the Trust's estate.

DUTIES

Director

The Director as Accountable Officer for P2F has overall accountability and responsibility for this policy in P2F.

The Director acting as the Senior Information Risk Owner will:

- take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement on Internal Control;
- review and agree action in respect of identified information risks;
- ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- provide a focal point for the resolution and/or discussion of information risk issues;
- ensure all staff are adequately briefed on information risk issues

The Director acting as Head of Quality Assurance/Head of IT Services

On a day-to-day basis the P2F's Information Security Leads will responsible for implementing, maintaining and managing the policy and related procedures

P2F Responsibilities

Third parties are required to sign into IT Services prior to any work carried out.

Before work is carried out a valid confidentiality agreement must be completed and signed by the third party individuals carrying out the work.

Contractors must be escorted to the place where the work is carried out

Workstations allocated for third party use are logged in by P2F staff without disclosing passwords.

Ensure software and hardware required for the third party to carry out their work is readily available.

Ensure that all contracts/orders are valid and up to date to cover the work being carried out. A record of the contracts can be requested from the Director.

Ensure the completed work accurately fits the description in the scope of works and sign off any record/statement of works document.

Third Party Responsibilities

- A mutually acceptable date and time must be arranged in advance prior to commencement.
- Third parties must report to the Director prior to any work carried out

- Respect the staff, working procedures and policies of P2F.
- Keep the working area clean and in line with P2F policies meeting all health and safety regulations.
- Provide adequate insurance for staff and equipment whilst on site.
- Copying, removing any configuration, data or information without written P2F approval is prohibited.
- All third party companies must have signed the 'Third Party Confidentiality Agreement'.
- All data including and especially PID will be treated with care and respect. Any information sent electronically regardless of the direction of the information flow must adhere to P2F policy and be protected.

REMOTE DIAGNOSTIC SERVICES AND THIRD PARTIES

Suppliers of systems/software will sometimes require access to systems to investigate/fix faults, the request may come from either the supplier or P2F. P2F will permit such access and will monitor all activity.

Any VPN tokens or remote tools issued to facilitate will remain with the Director or Admin Manager, only the PIN and the unique number will be provided to the supplier.

Each supplier requiring remote access will be required to commit to maintaining confidentiality of data and information, using qualified representatives, and have signed the third party confidentiality agreement.

Each request for remote access will be authorised by approved computer services staff, who will only make the connection when satisfied of the need. The connection will be physically broken when the fault is fixed/supplier ends the session.

INCIDENT REPORTING

P2F have formal incident recording via P2F process and escalation procedures. All IT related incidents, including information security incidents will be recorded in line with the Policy.

Third parties should report security and confidentiality incidents and must including near misses to the Director.

SERIOUS UNTOWARD INCIDENTS

Information security incidents that are thought to be significant may be referred to the Director and possibly Strategic Health Authority.

Major incident/business continuity control procedures will be used to manage IT serious problems e.g, inability to recover critical live systems.

Loss of PID of other serious breach of the DPA must be reported immediately to the Director to assess if the incident needs to be reported to the PCT, SHA and possibly the information commissioner's office.

REPORTING STRUCTURE

Formal reporting of any incidents or departures from this policy will be through the Information Governance Committee which is held once every two months.

All information security incidents will also be recorded with Risk Management in a timely manner.

POLICY DEVELOPMENT & CONSULTATION

The policy has been written by the Director.

IMPLEMENTATION

This Policy will be published on the internet and will underpin the contracts entered into by P2F and the third party confidentiality agreements.

MONITORING

Any breach of this policy by P2F staff will be investigated in accordance P2F's Disciplinary Policy and any breach by a third party will be reported to the relevant third party company.

Spot check audits will be conducted by P2F to ensure this policy is complied with.

REFERENCES

Policies can be sent to third parties on request.

REVIEW

This policy will be formally reviewed biannually or earlier depending on the results of monitoring.