Data Protection Policy

Statement of Policy

PMC Physiotherapy aims to achieve the best possible standards of protection for all the data, including personal data, which it collects and processes. It is committed to compliance with the requirements of the Data Protection Acts and the General Data Protection Regulations of May 2018.

PMC Physiotherapy Clinic recognises its responsibilities, and will comply with, all relevant statutory legal requirements. It recognises its obligations to manage and achieve adequate standards of Data Protection on behalf of any patients, employees or others, who provide it with Personal Data. It recognises its responsibilities in terms of the collection of, storage of, retention of, sharing of, providing access to and the correction of inaccurate information. It recognises the rights of individual patients / data subjects to access to, to correction of, deletion of or portability of their data, and will comply with the GDPR in this regard – or will provide a full explanation where any conflict arises as set out in this policy.

It will carry out a regular audit of the types of personal data which it holds and processes. It will assess the risks associated with the data it processes and will takes the necessary measures to keep it safe and to comply with the legislation. It will provide appropriate instruction, training, information and supervision of any person who may process the data. It will provide for review periodically, in light of experience and changing circumstances in the future, but at least annually.

The legal basis for the processing of data in this clinic is by explicit consent and as a necessary requirement for the provision of physiotherapy / health care, for diagnosing a condition and for the treatment of that condition. The processing may also comply with the legitimate interests of the therapist and the patient.

The purpose of collecting personal data from patients is to use this to arrive at a diagnosis and to inform the treatment plan.

The data may be stored in a variety of means as set out in this policy. All data is kept secure and considered confidential. Data may be shared with patients GP or other referring source, and will only be shared with other third parties with the written consent of the patient as set out in this policy.

The retention period for personal data is normally 7 years (beyond the age of maturity in the case of a child) except in exceptional circumstances.

It is recognised that in co-operating with this policy patients, employees and others will comply with the requirements of this policy. They will report any concerns about data protection to the practice without delay so that such concerns can be investigated.

Signed: _____ Date: 25th May 2018

Lead Physiotherapist and Owner

PMC Physiotherapy Clinic Profile

PMC Physiotherapy Clinic is a small private practice offering out-patient physiotherapy services to the general public. There is one lead Physiotherapist and 3 contractors. Some services are provided outside of the practice premises – sports physiotherapy,ergonomic consulting, S and C consultations, training, and some home based physiotherapy services.

The clinic occupies its own premises with its own entrance off a commom foyer. The clinic is laid out in six rooms – a waiting / reception area leading to a latge studio room. Off this there are 3 treatment rooms and a gym. There is access to a toilet off the studio. Also off the studio is a storage area. This area contains a locked filing cabinet clinic consumeables.

The practice PC's are located in the studio, at reception and in the Cardio treatment room, all linked to the internet. All are password protected. All files are cloud stored using Cliniko Practice management systen.

The practice uses Cliniko management software programme to collect demographic details for each patient, a diary function to keep records of attendances and can provide business related statistical reports as needed. This program is password protected for each individual with access to it. Therefore the system maintains a log of access. Clinical notes are also stored on this system.

Clinical Records are produced on Cliniko. Some paper notes were used when the practice started and these are kept lovked in thefiling cabinet. A record is maintained of each visit / attendance by a patient. Any reports, letters or other relevant materials are scanned and the originals returned to the patient. DVD disks may be reviewed from time to time with MRI or other information on them but no copy is made – a note is made of anything relevant from them on the patient record. Clinical leters are stored on each patients file. Other business letters are stored in a separate password protected folder on the PC.

All patient records are sored using Cliniko.
Long term discharges (>7 years since last contact) will be archived and stored securely up to the present. A programme of deletion of these records will be undertaken when these files reach 7 year maturity.

Employment Details

The Clinic employs 1 person full time, the owner, lead Physiotherapist, clinic principal.

The clinic principal is the Data Controller for the purposes of this policy.
Any other employee(s) will act as Data Processors.

From time to time part time locum chartered physiotherapists may be employed, either on a contract or on a self-employed basis as required.

From time to time third party contractors are employed to complete development or routine maintenance works. All such persons report directly to the practice principal. The practice principal is usually present during these works. If they are unsupervised steps are taken to ensure all personal data is left secure, safe, protected from them and unavailable to them.

Persons working in the clinic will normally work alone.

(Employee) Co-operation

All locum employees, or others attending this clinic as patients, visitors or contractors, will co-operate fully with the arrangements made by the clinic, as set out in this policy, for the protection of Personal Data.

Anyone with concerns about Data Protection issues should immediately report all such concerns to the practice principal, so that they can be investigated and acted upon appropriately without delay.

Any locum employee, or other person, is expected to comply with the requirements of this policy so that the clinic may remain compliant with the Data Protection Acts and the GDPR

Any locum employee, and other person, is expected to avoid causing a breach of Data Protection by any of their actions.

Any locum employee, working as a data processor, is reminded that they have specific statutory responsibilities under the Data Protection Acts and the GDPR.

Compliance & Disciplinary Policy

When advice and persuasion fail, and a patient, an employee, or other person continues to fail to comply with the requirements of the Data Protection Policy, it is the policy of PMC Physiotherapy Clinic to pursue the matter through an appropriate disciplinary code or other appropriate action.

Compliance with the arrangements set out in this Data Protection Policy is required of all employees, patients and visitors – it is not optional!

Compliance with the arrangements set out in this Data Protection Policy will be a requirement of securing contracts / the provision of services or products. Where a contractor fails to comply with, or to heed, representations made to him / her by the practice principal, then the clinic may seek to cancel the contract forthwith.

Communication + Consultation

A statement of Policy will be prominently displayed in the waiting / reception area.

The Data Controller for this business is the practice principal, Paul Conneely

All personal Data is collected and used for the following purposes.

1. To provide demographic + Contact Details of patients, and other persons, necessary for the normal running of a physiotherapy practice business – i.e. Patients, doctors, consultants, legal advisors, business managers, other employers etc.

2. To provide Clinical Information necessary for the development of a clinical picture, to be able to make an appropriate clinical evaluation of a patient's condition and to arrive at an appropriate diagnosis in order to develop a treatment plan and to accurately record any treatment given and opinions arrived at.

3. To provide a basis for developing Physiotherapy Reports for medical referees, GPs, Consultants and others who may reasonably require them. Patient's data will not be shared, other than with the original source of a referral, without the patient's permission. Where the patient specifically requests it they will be notified of any communication with the source of referral also.

4. To provide an accurate record of all contact with, all clinical evaluations and opinions, treatments, response to treatment and professional opinions

5. To provide reasonable business related information to facilitate the normal business activity of a commercial physiotherapy practice – HR information, pay related information, taxation related information.

Patients or others with any concerns about matters related to Data Protection should discuss these directly with the practice principal, who is the Data Controller, and as such has the ultimate responsibility for such matters.

For the purposes of this policy the Data Protection Officer is also the practice principal / the Data Controller as it a small business with a minimal management structure.

The practice principal will consider all such concerns expressed and will act to minimise any risks identified as he sees fit. In the event of a Breach of Data Protection he will respond in accordance with the procedures set out in this policy.

Because of the size of the clinic no formal system or arrangement has been made for consultation with patients, employees or others in matters of Data Protection. All such matters should be discussed directly with the practice principal.

Personal Data Audit (Collection)

The Personal Data that this practice collects and processes is as follows

- Personal contact details of individuals may include

1. Title
2. Name
3. Address details
4. Telephone numbers – landline + mobile
5. Email addresses
6. Age / Date of Birth
7. Male or Female Gender

- Patient's clinical information may include the following

1. Subjective examination – what the patient tells me on questioning
2. Any reports, letters of referral etc.
3. Objective evaluation – what I find on clinical testing of the patient
4. Clinical Assessment / diagnosis / Professional opinion
5. Treatment Plan
6. Treatment provided
7. Clinical Summary / Discharge Summary

- Employee Details / Locum Details

1. Personal contact details as above
2. A Curriculum Vitae
3. Human Resources Information – performance reviews, employment contract, letters of commendation, letters of complaint, accident reports, sickness certificates / sickness records, CPD records and other related material
4. Financial related information – PPS number, Tax Status etc.

- Contact Details of other Individuals Businesses + of their Management.

1. May include some financial and banking details for SEPA payments
2. Sports Clubs Personnel including Team managers, coaches and club management
3. Professional Body contact details.
4. Course attendee listings / contact lists

Personal Data Audit (Storage + Retention)

This practice stores the Personal Data records it has collected in the following manner

- On its patient management computer program (Cliniko) on the practice PC

1. Patient contact details
2. Body Region Injured
3. Number of attendances / non attendances
4. Type of billing item – treatment, product
5. Referral Source
6. Subjective examination
7. Objection Examination
8. Clinical / professional opinion
9. Treatment plan
10. Treatments provided
11. Date of attendance
12. Letters to Patients, their Doctors, referral Sources,
13. Email addresses for business and some patient related communication
14. Health + Safety / Ergonomic reports
15. Non-Current Patient records
16. Ergonomic Assessment + Reports
17. HR Records
18. Business Related Records – Accounts, taxation, insurance, investment
19. Archived records for Health + Safety consultancy
20. Archived Ergonomic Reports
21. Archived Letters – including business and clinical letters

- On shelving Unit, paper based records in ring binders

1. Aged Financial Records

Child Data

This Practice shall seek appropriate valid consent from the child / patient and from their parent / guardian before any personal data is collected or before any physiotherapy is initiated in accordance with the ISCP policy on consent.

The need for data and how it will be processed will be explained to a child in a manner they can understand.

The personal data of child patients will be retained for 7 years past their 18th birthday, or beyond their last attendance

Children's data is used only for clinical purposes and no other use is permitted

For the purposes of this document the following definitions apply

1. *Child* – is a person under the age of eighteen (other than a person who is or has been married).
2. *Parent* – is the natural parent, the adoptive parent or the adopting parent in respect of a child, or is the person(s) acting in loco parentis to the child.
3. *Guardian* – is a person having the right and duty of protecting the person, property or rights of another who has not the legal capacity or is otherwise incapable of managing his/her own affairs.
4. *Legal guardian* - in relation to a child, means any person who is the guardian of a child pursuant to the Guardianship of Infants Act, 1964 or who is appointed to be his or her guardian by deed or will or by order of a court; (Children Act, 2001)..
5. Treatment and Intervention - are used interchangeably throughout the document.
6. Patient and Client - are used interchangeably throughout the document.

Minors between their 16th and 18th birthday may give their own consent to medical, dental and surgical procedures. (The Non-Fatal Offences Against the Person Act) This practice will normally also try to inform the parents / guardian of the proposed examination and treatment. It is normally preferred to have a parent / guardian present during all assessment and treatments of patients under the age of 18 years

A parent or guardian can/must consent to treatment for the child. Sufficient information will be provided to ensure that such decisions are made on an informed basis.

Only persons who have guardianship (parental responsibility) can consent on behalf of a child. Consent for a child can be given by the following person(s):

1. The mother
2. The child's father if married to the mother currently or in the past

3. The child's father who, if not married to the mother, has acquired guardianship via a court order (guardianship rights in relation to his child).
4. The child's father when a guardianship agreement has been established between the mother and father.
5. The child's legally appointed guardian, appointed by a court or by a parent with parental responsibility in the event of their own death.
6. A person in whose favour a court has made a residence order concerning the child.

The Health Service Executive can give consent in relation for a child who is under Statutory Care i.e. an Order has been made by the Court under Section 18 of the Child Care Act, A variety of situations may exist and clarity should be sought as appropriate for those in Voluntary care, Emergency Care Order, Interim Care Order, Care Order and Foster Care.

The Parent is themselves a Child similarly some clarification should be sought as a child by definition is legally incapable of providing a valid consent themselves.

In situations where the parent him / herself is a child, then:

In loco parentis have limited rights to act *in loco parentis,* until the person with guardianship (parental responsibility) can be contacted.

Consent Policy

This Practice shall seek appropriate valid consent from the patient before any personal data is collected or before any physiotherapy is initiated, in accordance with the ISCP policy on consent.

Consent for Data Protection Purposes

There are new and specific requirement with regard to consent when collecting and processing personal data. This data / information must be

- freely given,
- specific,
- informed
- unambiguous
- verifiable
- include a positive indication of agreement

A patient has the right to withdraw consent for Data processing at any time and exercise of this right must be notified to Any Physio.

The practice principal in this clinic, Paul Conneely - the Data Controller, will provide a form on which to record consent for data processing. This consent form will form part of the audit trail.

This policy applies to all Chartered Physiotherapists working within the Practice

It is the responsibility of all Chartered Physiotherapists to ensure that consent is obtained for all interventions.

Treatment and Intervention are used interchangeably throughout the document.

Patient and Client are used interchangeably throughout the document.

Obtaining Consent

Consent is a patient's agreement for a Physiotherapist to collect their personal Data. This consent will be recorded on a consent form.

Consent is also patient's agreement for a Physiotherapist to provide care. It is a basic requirement under common law. Consent must be obtained prior to clinical examination, treatment or investigation. This is separate from consent to data processing.

Consent will not be obtained from a patient whose ability to provide consent is impaired.

Patients have the right to refuse consent for data collection, storage or processing. But this may make it impossible to carry out a physiotherapy evaluation and treatment.

Emergency

In a life-threatening emergency situation where a patient is unable to consent or to appreciate what is required, a physiotherapist may administer emergency treatment in the absence of the expressed consent of the patient. This is known as the **Doctrine of Necessity**. This is a common law doctrine developed through case law. It applies to an emergency situation where the clinician treats a patient in the best interests of the patient.

Consent for processing of personal data, or the withholding of consent must be recorded by the Physiotherapist. Patients, as data subjects, may withdraw consent at any time.

Consent is valid when it is:
1. Given voluntarily;
2. Given by a person with capacity to consent;
3. Informed; and
4. Given by someone entitled to give consent.

Informed consent protects the individual's freedom of choice and respects the individual's autonomy.

Consent for Data Collection

Consent for Data Collection, Processing and Retention
PMC Physiotherapy Clinic

PMC Physiotherapy Clinic collects and processes sensitive, healthcare related personal data on the basis of your explicit consent, and in order to form an opinion about, and to diagnose your presenting condition. Your personal data will not be used for any other purpose

Your data will be processed in a fair manner and retained by PMC Physiotherapy Clinic for a period of 7 years after your last attendance. Your data will be stored securely and protected during this time as set out in our Data Protection Policy which is available to you if you wish to have it.

Your personal data may be shared with the person who referred you for physiotherapy, with your family doctor (GP), with a medical consultant or other specialist practitioners. Other examples of people with whom your data may be shared with, subject to your prior agreement, include your Legal Advisors, employers, Insurers, team/club medical staff and management in order to facilitate your return to normal activities. Your Data will not be shared with any other third party outside of the Clinic without getting you permission to do so.

Your data will not be subjected to automated processing by this clinic.

You have a number of rights in relation to your personal data held at this clinic. These include

a. the right to request from us access to and rectification or erasure of your personal data,
b. the right to restrict processing, object to processing as well as in certain circumstances the right to data portability
c. The right to withdraw your consent for the processing of your data (in certain circumstances) at any time which will not affect the lawfulness of the processing before your consent was withdrawn.
d. The right to lodge a complaint to the Data Commissioners Office if you believe that we have not complied with the requirements of the GDPR or DPA with regard to your personal data.

The Data Controller and the Data Protection Officer is the Practice Principal: Paul Conneely

I agree to my Personal Data being collected and processed by PMC Physiotherapy Clinic.

Patient Name:_____ Date:

Guardian / Parent _____ Date:

Privacy Notice for Employees

Data Collection + Processing

Privacy Notice

How your information will be used

1. As your employer, the Clinic / Company need to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately,

   - during the recruitment process,
   - whilst you are working for us,
   - at the time when your employment ends and after you have left

   This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Clinic / Company and protect our legal position in the event of legal proceedings.
   If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.
2. As a Physiotherapy Clinic pursuing business activities, we may sometimes need to process your data as a result of your employment contract or to pursue our legitimate business interests, for example to promote the Clinic Team members skills on our website. We will never process your data where these interests are overridden by your own interests.
3. Much of the information we hold will have been provided by you, but some may come from other sources, such as referees.
4. The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits and expenses purposes; contact and emergency contact details; records of holiday, sickness and other absence; information needed for equal opportunities monitoring policy; and records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.
5. You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company. You should refer to the Data Protection Policy which is available on request or in paper format from the practice principal.
6. Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our

health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and company sick pay.

7. Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency.
8. Where we are processing data based on your consent, you have the right to withdraw that consent at any time.
   In addition, we monitor computer [and telephone/mobile telephone] use, as detailed in our Computer/telephone/electronic communications/expenses policy, available from the practice principal. We also keep records of your hours of work by way of our clocking on and off system, as detailed in your employment contract.
9. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to payroll provider, auditors, pension or health insurance schemes.
   We may transfer information about you to other group companies for purposes connected with your employment or the management of the company's business.
   In limited and necessary circumstances, your information may be transferred outside of the EU. We have in place safeguards to ensure the security of your data.
10. Your personal data will be stored for a period of 7 years following your employment ending.
11. If in the future we intend to process your personal data for a purpose other than that which it was collected we will provide you with information on that purpose and any other relevant information.
12. Your rights under the General Data Protection Regulation (GDPR) and The Data Protection Act (DPA) with regard to your personal data. You have
    a. the right to request from us access to and rectification or erasure of your personal data,
    b. the right to restrict processing, object to processing as well as in certain circumstances the right to data portability
    c. The right to withdraw consent if you have provided consent for the processing of your data (in certain circumstances) at any time which will not affect the lawfulness of the processing before your consent was withdrawn.
    d. The right to lodge a complaint to the Data Commissioners Office if you believe that we have not complied with the requirements of the GDPR or DPA with regard to your personal data.

Paul Conneely is the Data Controller and processor of data for the purposes of the DPA and GDPR.

If you have any concerns as to how your data is processed you can contact:

Paul Conneely Tel: 01 8253997 Email: info@pmcphysiotherapy.ie
Practice Principal / Data Protection Offer.

Access Request Policy

PMC Physiotherapy will provide access to a full copy of the personal data which it holds on any individual on receipt of a written request for same. An informal request will be sufficient to begin the process of retrieval and copying of the data.

The data will be made available to the patient / data subject on receipt of a written request. The written request must identify the data subject clearly and specify precisely what data of theirs the request applies to. The request in writing permits the clinic to maintain a clear audit of its records.

A copy of the data record will be provided in hard copy and either delivered by

1. Hand

2. Mail to a specific name and addressed person

The transfer of the data record needs to be documented and recorded itself to provide an audit trail.

Electronic copies can only be provided where it has been requested in this format and will be sent to a specified email address that is specific to a named recipient as set out in the original written request for the access / copy of the record. A 'read' or 'opened' or 'delivery' receipt will be requested from the email service provider in order to provide an audit trail.
Alternatively the data subject may provide a media device where the electronic record can be transferred and a written confirmation of receipt will be requested.

All email that includes personal data will be sent to specific named individuals email addresses.

Where a request is made to correct the data record the request to do so must specify exactly which data in the record is incorrect, and if possible indicate what change needs to be made in the record in order to correct it.

Changes to the electronic record within Cliniko – the clinic practice management system – is straightforward enough. The system maintains a log of all actions taken. In this situation it is a simple alteration of factual information.

Where there is a difference of opinion the therapist may need to provide additional information to explain how they have come to a particular opinion or on what basis it has been arrived at. Professional and clinical opinion may be altered in light of new or additional information being provided but it does not necessarily negate the opinion reached up to that point .i.e. the processing that has been completed up to the time the request to alter or change was made.

Changes to a hard copy record / patient notes are made in a written form with an explanation for the action taken. The incorrect data is identified and highlighted but not removed or blanked out completely – the corrected information is added to the record and annotated where the original text occurs in the record. Incorrect or data otherwise to be changed may be highlighted by using a highlighter pen, by enclosing in brackets and / or by drawing a single line through the text The text in question should remain legible but clearly identified as having been altered.

Where a conflict arises between the rights of the data subject and the data controller – PMC Physiotherapy Clinic – Paul Conneely will make contact with the data subject and outline the nature of and implications of the conflict, in order to achieve a mutually agreeable solution. i.e. where the data subject may request deletion of a record but there is a legal requirement for the clinic to retain it.

Once the requested change or deletion of a record has been completed the clinic will provide confirmation of having done so to the data subject.

Sharing Data / Transfer of Data Policy

PMC Physiotherapy Clinic will not normally share your personal data with any other person or organisation. It is the policy of the clinic to seek and receive your permission prior to doing so.

However it is understood that your personal data may be shared with the person who has referred you for assessment and treatment should this be appropriate – a GP, a medical consultant, your legal advisors. It is normal to communicate to them the results of having assessed and treated you and the professional opinions arrived at.
You may, if you wish, restrict this communication by requesting that it be done only on your specific consent to do so.

Your consent will be required to share any information about you with any other third party. Your consent will be sought and recorded in your personal record / patient notes.

A written request will be required wither from you, the data subject, or from the third party themselves setting out clearly whom they wish information about, what information they require, when the require it, the purpose for which they require it and how it should be provided.
Any request from a third party will be checked with you, the data subject, before any information is shared.
A record of the request and the transfer of data will be made in the personal record / Patient record.

All personal data shared will be transferred to a specific individual either directly by hand, by mail to a specified person or by email to a specified personal email address. In the latter case the file may be password protected / encrypted and the password provided separately from the electronic file.

Records will be included in any sale of the practice and should be considered as a transfer of ownership and thus needs to be recorded

This practice will not share retained personal data with third parties for advertising or marketing / promotion purposes. It is not currently intended that any personal data collected or retained will be used directly by this clinic itself for marketing purposes.

Records Retention Policy

It is the policy of this practice to retain the Personal Data it has processed for a period of not less than 7 years from the end of the last contact with a patient.

All retained records containing personal data will be stored safely, securely and in such a way as to preserve its privacy and confidentiality.

Access to personal data will be restricted to those who reasonably require it in order to perform their work within the practice.

Personal Data will not be shared with other persons except in connection with their clinical management and treatment, other than by the expressed consent of the patient / data subject.

Current and noncurrent patient records are stored in the Clinko system.
Archived records older than seven years will been retained in case they were needed in the past. It is the policy of the clinic to gradually begin reviewing these records on maturity of 7 years and where no reason is found to retain them they will be destroyed or anonymised.

Records will be reviewed on an annual basis. Records that are older than 7 years, that have no apparent reason for retaining them longer, will be destroyed.

Records that are held beyond this period where possible will be anonymised. Where a record is retained and cannot be anonymised an explanation will be provided to the data subject and a further consent to retain the record will be sought.

The records relating to patients under the age of 18 years of age must be held for 7 years beyond their 18th birthday.

Destruction of the records will be arranged in such a way as to ensure the safety and confidentiality of the data.

This practice will not share retained personal data with third parties for advertising or marketing / promotion purposes. It is not currently intended that any personal data collected or retained will be used directly for marketing purposes by this clinic.

Data Storage Policy

Hard Copy Data Records

The clinic does not maintain hard copy data records. Hard copy inward referrals, reports and requests are scanned to the patient records on Cliniko and then destroyed.

Electronic / Digital Records

The standard of encryption required to adequately secure data changes with advances in technology. Whole-disk encryption of 256-bit strength should meet the requirement at present and is provided by the current PC.

A strong password would typically be 14 characters long, contain a random selection of letters, numbers and symbols and be impossible to guess Passwords used by this clinic include a combination of numbers, letters and some symbols

The practice PC's are protected by a password

The PC 's are protected by a firewall and the computer is provided with antivirus protection that provides daily updates and up to the minute protection for internet security.

The internet service provides additional paid for security protection at the service provider level – before the emails are downloaded – at source.

The WIFI internet used within the practice is password protected.

Files with sensitive personal data are backed up to the Cliniko cloud based system. They are not stored for any length of time on a personal laptop of the practice principal.

Cliniko, The patient management system on the PC is protected by a password for each individual who needs it, clinical therapist and non-professional / receptionist / secretarial staff.

The Letters Folder is password protected. This folder also contained Physiotherapy Reports and other sensitive data.

The Health and Safety Folder is also password protected. This folder contains data relating to health and safety consulting carried out by the Paul Conneely

Other Data

All desks surfaces should be clear of notes and other sources of personal data at the end of each day.

No sensitive record should remain visible when not in use – it should be replaced in the appropriate storage for its current status – current, non-current or archived.

Patients who provided original of legal or other medical reports or referral letters should have these scanned and the original returned to the patient for safe keeping. Similarly other data records like MRI, video, photos etc should be copied and the originals returned to their owner.

Some sensitive data related to the business is stored on the shelving units within the ring binder folders. This is not personal data but is considered sensitive and must be supervised and kept confidential.

A phased programme of reviewing archived records and destruction of them as appropriate will commence in the summer of 2018. It is hoped to complete this task within 6 months.

The premises are protected by an alarm system when the practice is not in use.

Registration Details

Data Protection Commissioners

Reporting Data Breaches

Once detected all data breaches will be reported directly on the DPC website at the following link which provides detailed information on dealing with breaches.

More information is available at the following webpage data security breach Code of Practice

The Breach will be reported to the following contact options.

1. E-Mail - dpcbreaches@dataprotection.ie
2. Phone - 1890 252231(lo-call); 00 353 (0) 57 8684800
3. Fax- 00 353 (0) 57 8684757

Housekeeping /

Good Operational Practice

All information that may identify an individual is considered personal data. Therefore the concept of good housekeeping practice is inherent in keeping personal information private and confidential.

All phone conversations should be conducted in a manner to maximise privacy of the persons involved. Use of names and phone numbers in public areas in association with other clinical details should be avoided.

Access to Patient Clinical Records is restricted to clinical staff in the normal routine. Reception / support staff will normally only have access to the demographic details in order to do their duties. Currently this is through the Cliniko system.

The Filing cabinet has a fully functioning lock and is kept locked when not under direct supervision.

The premises is protected by an alarm system. This system allows for more than one individual to have the access code – therefore a log of who has accessed the premises, and when, can be generated providing an audit trail of who has accessed the premises especially out of hours

Careful use of PCs will allow personal data to be kept safe and confidential. The PC is provided with appropriate levels of software protection, anti -virus protection, firewall protection etc. In addition the following should be noted

1. All folders containing sensitive information are password protected
2. All sensitive files are password protected
3. Patient personal data is appropriately protected and the system should be able to provide an audit trail of who worked on the system, when and with what files.

Use PC screen with care to protect personal data.

1. Use privacy buttons if available, turn off the screen or minimise the working screens when not actively using the PC.
2. Turn the screen so it cannot be read easily by patients lying on couches.
3. Do not leave personal data visible to other people – position the screen to prevent this, turn the screen away, turn the screen off, shut down the programme, clear notes from the desk area or otherwise ensure the information cannot be accessed by others.

This is particularly important when the room / screen is unsupervised.

All written notes, clinical records and other sources of personal data should be removed from the desks and other areas where they can be accessed if left supervised.

All small non clinical notes should be shredded for security

Files for destruction will be shredded / destroyed in a manner to ensure they cannot be reconstructed or retrieved.

Digital records may require specific programmes to delete the data completely.

It is the policy of the practice where possible to scan all digital media, referral letters, reports etc and return the originals to the patient for safe keeping by them.

Email + Electronic Communication

The ISCP has produced guidance on this matter for the use of email within the society. It is the policy of this practice where possible to comply with the principles of the ISCP guidance for the use of email.

One email address is used by the practice.

If the business expanded so that more email addresses were necessary an individual email address would be assigned to each employee. The practice principal will retain administrative control over each account (passwords etc) – hence can control access to practice emails if staff change / move employment etc.

E-mail is considered neither particularly private nor confidential. It should not be assumed that only one person who is a recipient or addressee is the only person who can see or access the information – they may have others who screens the incoming mail, it is extremely easy to forward e-mail messages to the wrong addressee etc

Sending E-mails

1. Use only your own personal password protected accounts to send and check e-mail.
2. Before sending a message check the addresses, especially large numbers are involved.
3. Identify yourself in each message, include your name and position at the end of a message.
4. Use subject headers or titles that will have meaning for the recipient
5. Copy relevant individuals and indicate in the message who is receiving copies.
6. If you are going to be unavailable on e-mail, leave a message to that effect or make alternative arrangements
7. E-mail messages are part of the formal communication for the practice as a whole and therefore should reflect a professional manner and tone.
8. Aim to respond to emails received when required within a reasonable time frame. Send a response indicating where this is not possible and when a response may be expected.

Content

1. Use the subject field to indicate clearly what the content is about.
2. Avoid writing in CAPITAL LETTERS as this is the electronic version of shouting.
3. Keep humour appropriate – it can often be misinterpreted.
4. Avoid sending unnecessary information – keep e-mails brief and to the point

Attachments

1. Careful consideration should be given before sending attachments, Attachments should always be sent as a common file type e.g. Word, Excel etc.

2. The sender should clearly state on the email what the attachment is and the purpose for sending it, to minimise the spread of viruses.

Sensitive Information

1. E-mails are the electronic equivalent of a postcard. Anyone can read its content along the delivery path. Sensitive information should preferably be sent by post or via a secure transfer system.

2. Be professional - e-mail is easily forwarded.

3. Be aware of copyright and libel issues.

4. It is not the policy of this clinic to send emails that are offensive, threatening, defamatory or illegal.

Receiving E-Mails

1. E-mails should be read by the intended recipient only.
2. E-mail accounts should be accessed on a regular basis at least once per day.

Detecting + Reporting of Breaches

PMC Physiotherapy is a Sole Practitioner Practice – therefore the responsibility for all data protection lies with Paul Conneely, the practice owner and principal.

As the sole employee of the business, and the person responsible for all aspects of Data Protection, he is also responsible for Detection of and reporting of Breaches of Data security.

Under GDPR requirements on detection of a data breach Paul Conneely will report the breach to the DPC within 72 hours, unless the data was anonymised or encrypted.

As the practice handles significant amounts of personally sensitive data it is the policy of this clinic to inform the individual(s) impacted by the breach and to keep them informed of progress of investigations + remedial actions taken.

If a data breach is discovered immediate action will be taken to minimise any further loss of data or unauthorised access to the data.

Disconnect the PC and other devices from the internet. Disconnect the internet modem from the phone line

Determine the extent of the breach and what data is affected / has been compromised and whose data it is.

Determine who has perpetrated the breach and how. Take steps or advice on how to close the breach and prevent further exploitation of this security weakness.

Prepare a report for the DPC and submit it within 72 hours or sooner if possible.

Hard copy data / patient records with personally sensitive data will be checked at least every week.

Files with personally sensitive data are handled in a systematic routine manner so that deviations from the routine will be immediately obvious. Departure from the routine if unexplained will be investigated.

Data and sensitive files are monitored at all times when patients or others are present within the premises. Files or data is not left unsupervised and easily accessible to others who are not authorised to have access to it.

Anyone acting suspiciously or apparently trying to gain access to data is warned that this is unacceptable behaviour. Failure to correct such behaviour or persistence with it will result in their exclusion from the premises and the termination of their care if they are patient. They will be offered the contact details of professional colleagues in the area if they request the same.

Specialist guidance will be sought from the website hosting company about apparent irregularities. The clinic website has information for public consumption but no direct personal data is collected or stored in any database as part of the website.

Security setting on websites and social media platforms will be set at HIGH.

Data Protection Risk Assessment

No	Data Hazard / Risk	Risk Level	Control Measure
1	Website being hacked	Med	Have suitable protection in place by Hosting Service. Provide protection for website databases where present
2	Unauthorised access to PC	High	Use password protection for Starting PC Password protection for all users of clinical software systems Password protection of email programmes Password Protection for sensitive data folders and files.
3	Screen visible by patient / visitors	High	Position screen in reception so they are not in direct line of sight Minimise / close sensitive files when not in use Do not leave screen or PC unsupervised
4	Clinical notes open on desk	High	Do not leave notes open and unsupervised on desk – cover of place within a folder out of sight when not in use Place in secure location when unsupervised

			Do not leave notes in reception unsupervised
5	Filing cabinet not secure – lock broken	High	Replace broken lock Replace filing cabinet Keep locked when not directly supervised or being actively used for filing duties
6	Current patient records in expanding file folder	Medium High	Keep records within the folder until needed and replace without delay. Place within the locked filing cabinet when not supervised and others are unsupervised in the premises doing other work
7	Archived Patient records in attic	Medium	Review records with a view to destruction by shredding and or burning as necessary Aim to complete within 6 months.
8	Contractors working in premises unsupervised	High	Switch PC off Lock current patient records folder into filing cabinet Remove the diary Remove any sensitive data from the desk area and lock it away.
9	Patients entering treatment rooms	Medium	Always ensure doors to treatment is closed to waiting area. Speak in a moderate to low level of voice Close interlinking doors when needed for privacy.

			Provide a sign to warn people not to enter a room when door is closed.
10	Notes with contact details on desk	Low	Have a clean desk whenever possible. Keep notes to a minimum.
11	Phone conversations being overheard	High	Keep phone conversations where sensitive data likely to be discussed to a minimum until alone in clinic At a minimum close treatment room doors to maintain auditory privacy.
12	Robbery / theft / unauthorised entry to the premises	High	Always lock the filing cabinet at night. Lock current patients records into filing cabinet Remove the diary at night.