CHARTERED SOCIETY OF PHYSIOTHERAPY

14 Bedford Row, London WC1R 4ED
Tel +44 (0)20 7306 6666
Web www.csp.org.uk

Information paper

Record Keeping Guidance

reference PD061 version 4
issuing function Practice and Development
date of issue January 2021

This version follows the original PD061 (paper version, January 2012 - November 2014)
and PD061 version 2 (archived webpages, November 2014 – November 2016).
reference PD061 version 3.1
issuing function Practice and Development
date of issue November 2016 (amended April 2017)

CHARTERED SOCIETY OF PHYSIOTHERAPY

Content

CHARTERED SOCIETY OF PHYSIOTHERAPY

Record Keeping Guidance

Introduction

Physiotherapy staff have a professional and legal obligation to keep an accurate record of their interaction with patients.

Physiotherapy records are legal documents that may be called upon for a range of legal purposes. The purpose of the physiotherapy record is to allow a third party reader to make a judgment based on the content of the record and therefore, the physiotherapy record may be the only robust defence against any claim or error, omission, act or negligence in the course of clinical practice.

Poor record keeping poses a significant clinical safety risk and is the most common reason physiotherapists find themselves being referred to the Health and Care Professions Council (HCPC). It is therefore imperative that members are clear what is expected of them and that staff are supported to maintain their competency in this area. You can read more about the HCPC standards here.

Principles of Good Record Keeping

Format

Physiotherapy staff in all settings are required to maintain records in whatever system or format their employer specifies. A record can be in paper or electronic format, or a mixture of both, and should include all the information relating to the health status and management of the individual patient. Clinic letters or digital records are acceptable provided all elements of the assessment, intervention, judgment and treatment are recorded.

The CSP does not specify what format notes should take, e.g. many physiotherapists choose to use SOAP notes (Subjective/Objective/Assessment-Action/Plan) while others choose a different style. What is important is that they give a clear and accurate account of the physiotherapy intervention and assessment.

Content

A good record will enable an independent reader to understand what conversations took place with a patient, what information was exchanged, the extent of any examination performed, what treatment was provided and what clinical reasoning decisions were made.

- The information must be clear to another health professional /the patient (including the use of short forms)

- Written records should be:

    - legible and written in permanent ink
    - signed at the end of the record (and name printed)
    - paginated, including date of consultation and time when appropriate
    - amendments should be dated, timed and signed and the original entry still clearly visible

- Electronic recording systems should be able to:
    - show who has made the record
    - show revisions or amendments
    - lock the notes

The CSP cannot recommend any one provider of electronic record system over another. However, when procuring a records system it is essential that clinicians consider what they need from such a system (creating meaningful data). If physiotherapy records are to be part of a wider electronic health record procurement; the best results are achieved when clinicians are involved from the procurement phase through development and beyond implementation. See the CSP's pieces on electronic health records, moving to paper light records and person-held records for more information.

More detail around the specific standards expected of physiotherapists when keeping records can be found in section 6 of the CSP's Quality Assurance Standards.

To ensure that records fulfil the key requirements the CSP's Record Keeping and Information Governance Audit Tool may be useful.

SNOMED

SNOMED is the world's most comprehensive terminology for electronic health information, underpinning datasets and electronic health records. Use of SNOMED allows for better data standardisation, data sharing, data analysis and research, as well as supporting patient safety and clinical decision making. You can find out more information in the CSP SNOMED page including the new way of searching for appropriate SNOMED terms. The subsets previously developed by the CSP are still available here.

Use of Abbreviations / Short forms

The language used in health records must be understood by other health professionals and anyone else who is required to read it. This includes the patient themselves.

The CSP acknowledges that its members face significant risks with using short forms in health records. However (alongside the HCPC and other national NHS IT programmes) it also understands that their use is common practice in the profession. We have therefore tried to take a pragmatic approach that supports members to mitigate the risks associated with their use.

- Members should only use short forms if there is an agreed list developed locally that is accessible to anyone entering information into, or viewing, health records
- If records are being transferred elsewhere, the agreed list must be transferred with the record to aid subsequent understanding of the short forms that appear in the record
- Educators within the profession need to highlight both the risks associated with, and good practice relating to, the use of short forms in pre and post registration training for physiotherapists, and in training for support workers

Shared Record

Shared records are increasingly common and perfectly acceptable, as long as physiotherapy staff keep records of their intervention, and where record keeping is delegated to a support worker they do so in the knowledge that the support worker is competent in this. It is becoming more common for a group of different clinicians involved in the delivery of patient care to input into one shared or unified record (in either paper or electronic format). This is perfectly acceptable practice.

The professional and statutory requirement to keep in mind is that the physiotherapist must keep a record of their intervention. The physiotherapist should record the information they obtain into whatever repository their employer requires (for example, this could be within the medical ward notes if it gives the capacity to document physiotherapy treatment and decision making appropriately).

In circumstances where physiotherapy staff are asked to contribute to the main medical record (for example around the basic details of care) but there is no facility to capture decision making and intervention details, then a separate record should be maintained. However, duplication of effort around record keeping should be minimised

Countersigning

Health Care Support Workers (HCSW)

When you delegate or allocate a task to a HCSW you are accountable for the decision and as such must be confident that they have the necessary knowledge, training and competency to carry it out. The HCSW is responsible for carrying out the task to the best of their ability and so they should enter what they do with the patient in the patient record. There is therefore no reason for the registered physiotherapist to countersign the record.

Students

Physiotherapists who are supervising students have a duty to make sure, as far as possible, that records completed by their students are clearly written, accurate and appropriate. (HCPC)

The practice educator, physiotherapist or qualified member of the multidisciplinary team is responsible for the patient and professionally accountable for the actions of the student, who is performing delegated tasks. They must therefore countersign the record.

There are circumstances when a HCSW can counter sign a student's record. In this situation there must be local agreement to this approach; the HCSW must have competence in practice education and supervision, and the student must only be recording the tasks and activities they have undertaken that are in the scope of the supervising HCSW's role.

Physiotherapists undertaking post graduate training and/or returning to work

HCPC registered physiotherapists (whether undertaking postgraduate studies or returning to practice after a career break) do not need to have their entries into the health record countersigned.

Physiotherapists undergoing a formal return-to-work programme who are not yet HCPC registered must have their records countersigned, as they have not yet fulfilled the requirements of autonomous practice associated with HCPC registration.

Accessing Health Records

There are a number of pieces of legislation that cover the use of data and information; some are specific to healthcare. This summary is not detailed or exhaustive, but should provide some guidance when considering GDPR in the context of wider healthcare confidentiality.

The Data Protection Act 2018

This Act describes how individuals, businesses, organisations and Government must handle personal information relating to living people. This new law replaces the Data Protection Act 1998. It covers all information held in paper or electronic form. There is stronger legal protection for certain types of sensitive information, and individuals have new legal rights to find out about their information and how it is used.

There are six fundamental data protection principles:

1. Data processing must be lawful and fair.
2. Data must be only processed for the specific purpose for which it was collected.
3. Data processing must be relevant and not excessive.
4. Data processed must be accurate and kept up to date.
5. Data must only be kept for as long as necessary for the original reason it was collected. There must be periodic review to determine if ongoing retention is necessary.
6. There must be organisational and technical measures in place to assure the security of data collected

National Health Service Act 2006

This permits health service organisations to disclose patient information to relevant authorities to improve patient care or in the public interest where the patient information relates to diagnosis or treatment of neoplasia, managing communicable diseases or for medical research and audit. More information on this can be found here.

Health and Social Care Act 2012

NHS digital has a legal right to collect data and information about people using health and care services in England and in some cases Wales, Scotland and Northern Ireland. This information is needed to plan and run the health service. This Act requires NHS Digital to be the safe haven of health and care information. The NHS Digital website provides detailed information about how it collects and uses data in its work, including details about the National Data Opt-Out programme.

Health and Social Care Act 2015

This Act requires all organisations, and individuals, to share patient information where this enables care for an individual patient. It makes the seventh Caldicott Principle of 'sharing of

information' a legal requirement, not an option. Sharing of information is essential for safe care. Information to support direct patient care must be shared where it is lawful to do so.

This means patients must be told about the proposed sharing of information although specific consent may not always be needed. A patient's objection to sharing information should be considered, but does not always mean that information cannot be shared. Patients must be told if their objection to sharing information means their treatment choices and/or options may be subsequently restricted.

The General Data Protection Regulations (GDPR)

GDPR is one of the set of Regulations that underpin the new Data Protection Act 2018. It introduces significant changes to data privacy to how data can be used. There is a significant focus on demonstrating compliance with the new laws and the penalties for data breaches are significantly increased. You can read more about GDPR and data ethics from a physiotherapy perspective here.

The duty of confidentiality

Privacy for healthcare treatment is assured under the 'duty of confidence'. This does not mean that information cannot be shared with others under any circumstances. When providing direct healthcare, consent to share information with others also providing direct care is implicit, unless there is a reason not to share. No further agreement is needed to share information although in practice is commonly sought.

The 'duty of confidence' has not been changed by GDPR.

Subject Access Requests (SAR)

A SAR is the way in which a person exercises their right under GDPR to find out what information an individual, organisation or business holds about them. Once the SAR is made you should verify the identity of the person making the request if you have any doubts as to who you are dealing with. You then have one month (30 days) to provide the information and it is usually be provided free of charge. You may be able to refuse to comply with a SAR if it is unfounded or 'manifestly excessive'. You must document how you manage SAR requests.

There is no requirement for the person making the SAR to tell you why they are making the SAR. SARs can be used for any purpose for which the person may need their records. This can include for example, deciding whether to make a complaint or a legal claim against a practitioner.

There may be parts of the record that you cannot disclose (see below), but apart from that, you must provide the information the patient asks for within 30 days. People may want copies of their health records for a variety of reasons. If you believe that the person may want to records in order to bring a negligence claim against you, you should also make a PLI notification.

GDPR has several **exemptions** in response to a SAR if;

- it is likely to cause serious physical or mental harm to the patient or another person;
- it is requested by a third party and, the patient had asked that the information be kept confidential and/or has not given their permission for the records to be released
- it is restricted by Order of the courts
- it relates to adoption records, human gametes, embryo's or relates to people born from IVF

You should still disclose the remainder of the records. Circumstances in which information may be withheld on the grounds of serious harm are extremely rare, and this does not justify withholding records because patients may find them upsetting.

You may also not have to disclose information if it relates to a third party who has not given consent for disclosure (where that third party is not a health professional who has cared for the patient) and after taking into account the balance between the duty of confidentiality to the third party and the right of access of the applicant, the data controller concludes it is reasonable to withhold third party information; You may be able to disclose without consent if you feel it is appropriate to do so and wouldn't put the third party at risk,

A patient can authorise a **solicitor** to make a SAR on their behalf. The SAR from the solicitor should be treated in the same way as if it was made directly by the patient. As long as the patient has given written consent for their solicitor to access their records, you must comply with the patient's or their solicitor's request.

In most cases SAR requests must be processed and provided **free of charge**. You can charge a 'reasonable' fee if the request is 'manifestly unfounded' or 'excessive'. For example, if you provide information under a SAR and the person requests the same information again within a short period of time you could charge a fee, or refuse the request.

You must make reasonable allowances for how the data is provided. You can provide the data how you want so long as the person is able to read it. If the data subject has a disability they may require you to provide it in brail or other alternative format. If the data subject does not own a computer they may ask you to provide a hard copy**.**

People requesting records have no entitlement to the original records. You must retain your original records for the required length of time. People must be provided with a copy of their record, in the format that they ask for.

Where an insurance company requires a person's medical records in order to offer or provide insurance policies a SAR cannot be used. Insurance companies must apply under the terms of the Access to Medical Reports Act. The ICO has said that the use of SARs by insurance companies to obtain full medical records is an abuse of SAR rights.

Deceased Individuals

The GDPR and DPA only apply to living people. However, confidentiality remains after death. People who have a legitimate reason to access the health records of those who have died must apply under the Access to Health Records 1990 Act. This will usually be the deceased's Executor or person with Letters of Administration if there was no will. Disclosure must be free of charge.

Control of Records

Physiotherapists and Physiotherapy HCSWs in employment

When a physiotherapist or physiotherapy HCSW is employed, the records they create or contribute to belong to the employer. As the record is owned by the organisation, it controls access and release, not the individual who created the record, so it does not matter if the individual has moved on or not. The organisation or practice employing you must keep the clinical records securely on their premises. You must be given reasonable access to the records you create but must not take records with you when you leave that place of work.

In cases in the NHS where there has been a decision to allow a patient to hold their own health record, the record is still owned by the NHS body providing care to the patient. The record is stored with the patient until such time as that care has ended, at which point the record is returned to the NHS body.

Considerations in Private Practice

Sole Practitioners

Where a person is self-employed and a ‘sole practitioner’ i.e. not contracted to provide services on behalf of another (for example a private practice, a private hospital or even a NHS hospital), it is the self-employed physiotherapist who owns the notes. In this case, the self-employed physiotherapist also has legal responsibility to register with the Information Commissioner and take on the burden of all Data Protection issues including storage, retention, security, processing and destruction of records. Failure to comply with such requirements can result in legal penalty.

Self-employed physios contracted to provide services for/on behalf of a third party

Where a person is self-employed but is contracted to provide services for/on behalf of a third party, for example to a private practice or clinic, private hospital or NHS establishment, the self-employed physiotherapist is in effect working on a consultancy basis. In this situation the Practice contracting with the self-employed physiotherapist is normally considered to 'own' the records, for the following practical reasons:

- In most circumstances the records are generated as a by-product of the 'contract' and in the first instance it would be the company that would be sued if something untoward happened, therefore it should be the company that retains the records. In these circumstances, the self-employed physiotherapist is also exposed to liability, they must be able to access the records to defend themselves. Having access to the records does not mean that they have to own the records.
- If the self-employed physiotherapist is absent from the Practice for some time, the patient is likely to wish to be treated by someone else within the Practice, and in these cases the other physiotherapist must have access to the notes, again making it essential that the Practice own the notes.

The Practice has the legal responsibility to register with the ICO.

Thus, if you run your own physiotherapy business (including medico legal work), or you provide self-employed services to a physiotherapy business where you decide yourself how your patients are treated, you need to register with the ICO.

If you are unsure whether you need to do so, you can take the ICO’S quick self-assessment test to find out.

Storing and Retaining Records

Records form a legal record of treatment and therefore must be retained safely and securely (You must store your records in accordance with the DPA, (i.e., in a lockable cabinet). in accordance with the Data Protection Act 2018. Under GDPR regulations data must only be kept for as long as necessary for the original reason it was collected.

The legal requirement to retain records for a certain period relates to the legal period for bringing civil claims under either Personal Injury law or Contract law as defined by the Limitation Act 1980 and The Limitation (Northern Ireland) Order 1989.

Retention schedules vary according to the type of record but, in general, for those with capacity is usually eight years from the date of last treatment for adult records, and for children eight years after their 18 birthday or until 25 years of age. Other types of records may need to be stored indefinitely.

Each UK country sets out minimum retention periods for NHS health records. The minimum retention periods apply to all formats/mediums which contain components of information relating to the health record. Although the retention periods quoted apply to the health departments in the devolved nations, private practitioners would be advised to apply the same retention periods.

Storage of electronic records

Just as with paper records, electronic records should be kept secure whenever practically possible. This could include password protection when records are static and encryption when sharing sensitive or identifiable information. Under GDPR, data about an EU citizen should remain in the EU unless the provider can demonstrate that they comply with certain regulations. This information is normally on the company's privacy policy. The CSP cannot recommend any provider over another but it is essential that any systems being used by members comply with GDPR regulations. You can read more in the CSP's GDPR and data ethics paper or in the NHSX Records Management Code of Practice .

Dealing with data breaches / data damage

It is the ICO that deal with data breaches, some of which must be reported to them. You will find further information and guidance on their website.