PATIENT ACCESS TO MEDICAL RECORDS POLICY (INC PROXY ACCESS)

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of Aspiro Healthcare.
This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from our organisation

B. Document Details

Author and Role:	Sarah Bradshaw, Head of Operations
Current Version Number:	V1
Current Document Approved By:	Partnership Board
Date Approved:	13.06.2019

C. Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
V1	01.10.18	Sarah Bradshaw	Partnership Board	

Discrimination

Gender	This policy will be applied equally regardless of the gender of the patient
Race	This policy will be applied equally regardless of the Race of the patient
Disability	This policy will be applied equally regardless of whether or not the patient has a disability or not
Sexual Orientation	This policy will be applied equally regardless of the sexual orientation of the patient
Age	This policy will be applied equally regardless of the age of the patient
Religion/Belief	This policy will be applied equally regardless of the religion/belief of the patient
Human Rights	This policy will not impact on anyone's human rights

Introduction

The law states that NHS organisations must, when requested by an individual, give that person access to their personal health information, and occasionally, certain relevant information pertaining to others. In order to do this, they must have procedures in-place that allow for easy retrieval and assimilation of this information.

There are three main areas of legislation that allow the right of the individual to request such personal information, and they are:

- The Data Protection Act 2018 (formerly DPA 1998) (DPA)
- The General Data Protection Regulation 2016 (GDPR)
- The Access to Health Records Act 1990
- The Medical Reports Act 1988

Where the request for information by an individual falls under the legislation of any of these areas, access must be granted. Patients requesting information about their own personal medical records would usually have their request dealt with under the provisions of the Data Protection Act 2018 and GDPR 2016.

See section 20 for new requirements regarding Cost and Timeframes for responding to requests

The GMS contract and PMS agreement for 2015-2016 require practices to promote and offer their registered patients online access to all coded data in their GP records, referred to as their *Detailed Coded Record*.

The introduction of online patient access to services does not change the right that patients already have to request access to their medical records provided by the provisions of the Data Protection Act (DPA) and GDPR. The DPA principles and confidentiality requirements apply in the same way for online access as they do for paper copies of the record.

1. What Constitutes a Health Record?

A health record could include, and not exhaustively, hand-written clinical notes, letters between clinicians, lab reports, radiographs and imaging, videos, tape-recordings, photographs and monitoring printouts. Records can be held in either manual or computerised forms.

2. What Constitutes the Detailed Coded Record

The minimum specification described by NHS England in the patient online support and resources guide is:

- Demographic data
- Investigation results including numerical values and normal ranges
- Problems/diagnoses
- Procedure codes (medical and surgical) and codes in consultations (symptoms and signs)
- Biological values (e.g. BP and PEFR)
- Immunisations
- Medication
- Allergies and adverse reactions
- Codes showing referrals made or letters received
- Other codes (ethnicity, QOF)

The Detailed Coded Record can also include consultation free text and access to letters, but this is optional. At this stage the practice has decided not to include this level of access.

3. Medical Records Access – Staff Responsibility

Ops Manager and Clinical Leads

For the purposes of reviewing requests, the Ops Manager and a named Clinical Lead will ensure current data protection requirements are followed. The main (but not exhaustive) duties of these roles are explained below:

Ops Manager

- To process and co-ordinate the application.
- Verification of identity (See Section 6)
- Reviewing the medical records for third party information and redacting information where consent has not been given.
- Contacting the patient to explain the process and inform of the outcome.
- The Ops Manager for each surgery will be the named Administrative Lead.
- Each Ops Manager will consult the Clinical Lead or DPO for further advice where needed.

Clinical Lead

- Responsibility for reviewing the medical record and limiting or redacting sensitive and/or harmful information.
- Overall responsibility for decision to allow access.

4. Requests under the Data Protection Legislation

The scope of the Data Protection law includes the right of patients to request information on their own medical records. Requests for information under this legislation must:

- Be made to the surgery (E-mail requests are allowed). Verbal requests can be accepted where the individual is unable to put the request in writing, or chooses not to – however a record of what is requested should be recorded and a letter for approval by the patient sent out (this must be noted on the patient record);

See SECTION 20 For updated access advice

- Be accompanied with appropriate proof of identity (please see Section 6.).

- Where requests are made on behalf of another evidence of correct and adequate consent must be provided (please see Section 6.).

- Where an information request has been previously fulfilled, the practice does not have to honour the same request again unless a reasonable time-period has elapsed. It is up to the administrative/clinical leads to ascertain what constitutes a reasonable time-period.

- Suitably trained and authorised reception staff should ensure the application form has been completed correctly and verify identify via the stipulated methods. The application form must be completed and signed by the patient.

- The Administrative Lead will check whether all the individual's health record information is required or just certain aspects. They will then check the records for third party information and ensure that this is not given to the patient. (Please see Section 7) If it is not possible to remove such information the clinical lead should be consulted.

- The Clinical Lead will review the content of the medical record and ensure that sensitive or harmful data are not made available to the patient.

- The Clinical Lead can refuse the request for the reasons set out in section 8.

- The Clinical Lead will also check the record for quality, clarity of presentation, completeness, and accuracy.

5. Detailed Coded Records Access – Application

Patients will also be given a leaflet on the benefits and risks to Detailed Coded Access to Records.

On completion of an application form the Administrative Lead will review the application form and invite the patient into the practice to complete the following:

- Identity Verification (See Section 6)
- Inform the patient of the benefits and potential risks to detailed coded access to records.
- Advice Leaflet will be given to the patient and application process and timescales will be discussed.

(this is not applicable to DCRA but to requests under DPA)

The Administrative Lead will then check the records for third party information and redact information where appropriate. (Please see Section 7) If it is not possible to remove information the clinical lead should be consulted.

The Clinical Lead will review the content of the medical record and ensure that sensitive or harmful data are not made available to the patient. The clinical lead may redact sensitive or harmful data if they consider it to be in the patients' best interest.

The Clinical Lead can refuse the request for the reasons set out in section 8.

The Clinical Lead will also check the record for quality, clarity of presentation, completeness, and accuracy.

If approved the Administrative Lead will place an alert on the system to notify other members of staff that the patient has Detailed Coded Record access.

The completed application form should be scanned and attached to the patient's record. The administrative lead will contact the patient to inform them of the outcome of the application, explain the next steps and provide any further information.

6. Identity Verification

Before access to health records is granted, the patient's identity must be verified. There are three ways of confirming patient identity:

- Documentation (Forms of Identification)
- Vouching
- Vouching with confirmation of information held in the applicant's records

All applications for access to health records will require formal identification through 2 forms of ID one of which must contain a photo. Acceptable documents include passports, photo driving licences and bank statements, but not bills.

Where a patient may not have suitable photographic identification – Vouching with confirmation of information held in the medical record can be considered by the Administrative Lead. This should take place discreetly and ideally in the context of a planned appointment. It is extremely important that the questions posed do not incidentally disclose confidential information to the applicant before their identity is verified.

Adult proxy access verification - Before the practice provides proxy access to an individual or individuals on behalf of a patient further checks must be taken:

- There must be either the explicit informed consent of the patient, including their preference for the level of access to be given to the proxy, or some other legitimate justification for authorising proxy access without the patient's consent

- The identity of the individual who is asking for proxy access must be verified as outlined above.

- The identity of the person giving consent for proxy access must also be verified as outlined above. This will normally be the patient but may be someone else acting under a power of attorney or as a Court Appointed Deputy.

- When someone is applying for proxy access on the basis of an enduring power of attorney, a lasting power of attorney, or as a Court Appointed Deputy, their status should be verified by making an online check of the registers held by the Office of the Public Guardian.

Child proxy access verification - Before the practice provides parental proxy access to a child's medical records the following checks must be made:

- The identity of the individual(s) requesting access via the method outlined above.

- That the identified person is named on the birth certificate of the child.

- In the case of a child judged to have capacity to consent, there must be the explicit informed consent of the child, including their preference for the level of access to be given to their parent.

7. Third Party Information

Patients' records may contain confidential information that relates to a third person. This may be information from or about another person. It may be entered in the record intentionally or by accident.

It does not include information about or provided by a third party that the patient would normally have access to, such as hospital letters.

All confidential third-party information must be removed or redacted. This will be reviewed and completed by the Administrative Lead. If this is not possible then access to the health records will be refused.

8. Denial or Limitation of Information

Access to any health records can be denied or limited in scope of information. This decision will be made by the Practice Manager for the practice.

Access will be denied or limited where in the reasonable opinion of the clinical lead , access to such information would not be in the patient's best interests because it is likely to cause serious harm to:

- The patient's physical or mental health, or
- The physical or mental health of any other person
- The information includes a reference to any third party who has not consented to its disclosure

A reason for denial of information must be recorded in the medical records and where possible and appropriate an appointment will be made with the patient to explain the decision.

9. Proxy Access to Medical Records

Proxy access is when an individual other than the patient has access to an individual's medical record on their behalf to assist in their care. Proxy access arises in both adults and children and is dealt with differently according to whether the patient has capacity or not.

The patient's proxy should have their own login details to the patient's record. If a patient wants to have more than one proxy, they should all have their own personal login details. In the current version of our electronic records system (EMIS) login details will be shared between the patient and the individual with proxy access.

Proxy access should not be granted where:

- The practice suspects Coercive behavior. (See Section 14)
- There is a risk to the security of the patient's record by the person being considered for proxy access.
- The patient has previously expressed the wish not to grant proxy access to specific individuals should they lose capacity, either permanently or temporarily; this should be recorded in the patient's record.
- The clinical lead assesses that it is not in the best interests of the patient and/or that there are reasons as detailed in Denial or Limitation of Information. (Please see 8)

10. Proxy Access in Adults (including those over 13 years of age) with capacity

Patients over the age 13 (under UK DPA 2018) are assumed to have mental capacity to consent to proxy access. Where a patient with capacity gives their consent, the application should be dealt with on the same basis as the patient.

In terms of online access, it may be possible to give the proxy different levels of access depending on the wishes of the patient and/or the views of the Clinical Lead. For example, some patients may want to allow a family member to have access only to book appointments and order repeat prescriptions without accessing the detailed care record.

11. Proxy Access in Adults (including those over 13 years of age) without capacity

Nursing/ Residential homes will not be granted proxy access for patients under their care.

Proxy Access without the consent of the patient may be granted in the following circumstances:

The patient has been assessed as lacking capacity to make a decision on granting proxy access and has registered the applicant as a lasting power of attorney for health and welfare with the Office of the Public Guardian.

The patient has been assessed as lacking capacity to make a decision on granting proxy access, and the applicant is acting as a Court Appointed Deputy on behalf of the patient

The patient has been assessed as lacking capacity to make a decision on granting proxy access, and in accordance with the Mental Capacity Act 2005 code of practice, the Clinical Lead considers it in the patient's best interests to grant access to the applicant.

When an adult patient has been assessed as lacking capacity and access is to be granted to a proxy acting in their best interests, it is the responsibility of the Clinical Lead to ensure that the level of access enabled or information provided is necessary for the performance of the applicant's duties.

12. Proxy Access in Children under the age of 11

All children under the age of 11 are assumed to lack capacity to consent to proxy access. Those with parental responsibility for the child can apply for proxy access to their children's medical records.

Parents will apply for access through the same process outlined in Sections 4 and 5. Additional identification of Parental / Guardian evidence will be required. (See Section 6)

13. Proxy Access in Children above the age of 11 and under 13 years of age

Access to medical records will need to be assessed on a case by case basis. Some children aged 11 to 13 have the capacity and understanding required for decision-making with regards to access to their medical records and should therefore be consulted and have their confidence respected.

Online proxy access will automatically be turned off when a child reaches the age of 11. Online proxy access to the Detailed Coded Record of children aged 11 to 13 will not normally be approved unless it is in the best interests of the child or is the express wishes of a competent child.

The Clinical Lead will invite the child for a confidential consultation to discuss the request for proxy access whether this is for requests under the Data Protection Law or for online access.

The Clinical Lead should use their professional judgement in deciding whether to grant parental access and/or whether to withhold information.

If the practice suspects coercive behaviour access will be refused and documented in the medical notes. The clinical lead will liaise with Child Safeguarding teams if appropriate

Online proxy access will also be turned off when a child turns 13. Access can be turned back on by following the processes set out above governing access to adults.

14. Coercion

Coercion is the act of governing the actions of another by force or by threat, in order to overwhelm and compel that individual to act against their will.

Online access to records and transactional services provides new opportunities for coercive behaviour.

If the practice suspects coercive behaviour for either an individual or proxy access application, then access will be refused and documented in the medical notes. The clinical lead will liaise with CCG Safeguarding Team if appropriate.

15. Staff Training and Education

All staff at the practice will be required to read the policy and confirm their understanding.

All staff will be encouraged to undertake the E-learning programmes provided by their local training provider. For the Ops Manager and Clinical Leads this will be mandatory.

Presentations of Detailed Coded Access will be given at Organisational Education Meetings.

16. Advertisement

The practice endeavour to continue to improve the patient experience. Detailed Coded Records Access may improve the level of communication between patient and clinician and encourage patients to self-manage their health and wellbeing.

The practice will make patients aware via the following medias:

- Surgery Websites
- Practice Notice Boards
- Display Screens in surgery

17. Former NHS Patients Living Outside the UK

Patients no longer resident in the UK still have the same rights to access their information as those who still reside here and must make their request for information in the same manner.

Original health records should not be given to an individual to take abroad with them, however, the Practice may be prepared to provide a summary of the treatment given whilst resident in the UK.

18. Subject Access Requests- Following Implementation of GDPR (from 25 May 2018)

On 25 May 2018 the current UK Data Protection Act 1998 (DPA 1998) will be fully replaced by the General Data Protection Regulation (2016/679)

As with the DPA 1998, these new regulations give living individuals the right to request access to personal data held on them by the Practice. This is known as a Subject Access Request (SAR), the person who will hold data about is known as the Data Subject, in many cases this will be the patient, but could be a staff member, a contractor or contact.

Requests must not always be writing, this includes, letter, e-mail, however verbal requests should be documented, and a clarification letter sent to the patient for approval. There could also an electronic form for requesters to complete if they prefer. SARs can also be submitted via social media, such as the practice Facebook page or Twitter.

Requesters must be either, the data subject OR have the written permission of the data subject OR have legal responsibility for managing the subject's affairs to access personal information about that person. It is the requester's responsibility to satisfy the Practice of their legal authority to act on behalf of the data subject.

The practice must be satisfied of the identity of the requester before we can provide any personal information.

19. New Requirements for Subject Access

From 25 May 2018 some new requirements were introduced affecting the handling of subject access requests.

These are listed below:

What do we need to provide to a requester?

As well as providing confirmation that their personal is being processed and providing a copy of this personal data that the data subject has asked for; (subject to any exemptions). Individuals will have the right to be provided with additional information which largely corresponds to the information to be provided in a privacy notice:

- Source of the data.
- Recipient, including details international transfers.
- Retention period for the data.
- How to amend inaccurate data.
- How to complain to the Information Commissioner's Office (internal review will usually need to be satisfied first).

20. Timeframe for responding to requests

The ***Statutory*** timeframe has now been reduced to at least one month of receipt of the request, and in any event ***without delay.*** **In Accordance with Article 12 of the GDPR 2016.**

The period of compliance can be extended by a further two months where requests are determined to be 'complex' or 'numerous'.

The fee of £10 - £50 in the previous DPA 1998 has now been removed

It was the case that £10-£50 fee could be charged, but GDPR ***does not*** allow for a fee, so it must be provided **free of charge**. However, some charges can be made in the following circumstances:

- where further copies are requested by the data subject,
- or the request is manifestly unfounded, or excessive (definitions still required by the ICO) a reasonable fee based on the organisations administration costs may be charged.

When can a subject access request be refused?

The Practice can decide to refuse a request where the request is 'manifestly unfounded or excessive', in particular if it is 'repetitive', and the requester must be informed of the reason why, within one month of the receipt of the request. If the practice decides to apply this option advice MUST be sought from the practice Data Protection Officer, Paul Couldrey, PCIG Consulting Limited. (07525 623939).

What format should the response be provided in?

Where a request is received by electronic means, unless otherwise stated by the data subject, the information must be provided in a commonly used electronic format.

What are the penalties for non-compliance with the statutory timeframe?

The penalties are still at the discretion of the ICO. However, for non-compliance the financial penalties are now much greater. Depending on the severity of the infringement, this could be up to £17m approximately.

A new criminal offence has been created

If you receive a Subject Access Request, and records are altered with intent to prevent disclosure, this will be committing a criminal offence, and will be punishable by a fine.

What should you do if you identify that you have received a SAR?

Incoming SARs should be passed on immediately to the Practice Manager, where they will be logged, acknowledged, and processed.

21. Disputes Concerning Content of Records.

Once access to medical records has been granted patients may dispute their accuracy or lack understanding of medical codes.

Patients may notice and point out errors in their record, unexpected third-party references, entries they object to or want deleted. The right of rectification and deletion are now established within the GDPR.

Reception Staff will pass on any queries to the practice manager who will contact the patient.

The Ops Manager will investigate swiftly and thoroughly to identify the source and extent of the problem

The Ops Manager will then decide on the most appropriate action. Where the dispute concerns a medical entry the clinician who made the entry should be consulted and consideration given as to whether it is appropriate to change or delete an entry. Where it is not possible or practical to contact the clinician concerned the clinical lead should be consulted. If it is not possible to amend the records a meeting with the patient should be organised to explain why.

If a patient wishes to apply their GDPR 2016 rights of

- Rectification (Article 16 GDPR)
- Erasure (Article 17 GDPR)
- Restriction of Processing (Article 18 GDPR)
- Data Portability (Article 20 GDPR)

Advice MUST be sought from the Practice Data Protection Officer, Paul Couldrey, PCIG Consulting Limited. (07525 623939).

The final decision surrounding the accuracy of the medical record will be the responsibility of the clinician who made the entry. Where it is not possible or practical to contact the relevant clinician the clinical lead will decide to amend the record if appropriate. If the patient further disputes the accuracy once a decision has been made they will be referred to the complaints procedure and/or the Health Ombudsman.

22. Complaints

The practice has procedures in place to enable complaints about access to health records requests to be addressed.

Please refer to our practice complaints policy.

All complaints about Access to Records should be referred to the practice Data Protection Officer, Paul Couldrey, PCIG Consulting Limited. (07525 623939).

If the issue remains unresolved, the patient should be informed that they have a right to make a complaint through the NHS complaints procedure (further information is available at:

http://www.nhs.uk/NHSEngland/thenhs/records/healthrecords/Pages/what_to_do.aspx

Sometimes the patient may not wish to make a complaint through the NHS Complaints Procedure and instead, take their complaint direct to the Information Commissioner's Office (ICO) if they believe the Practice is not complying with their request in accordance with the Data Protection Act Alternatively, the patient may wish to seek legal independent advice.

23. Application Length

Requests for health records information should be fulfilled within 1 month (unless under exceptional circumstances – the applicant must be informed where a longer period is required - up to 2 months extension can be requested – but must be requested from the patient within the first month). Information given should be in a manner that is intelligible to the individual.

Due to the time required to process requests for Detailed Coded Records Access each practice will process applications within 28 working days from date of application. In some circumstances there may be a delay in access to records. Where a longer period is anticipated the patient will be informed.