**Access to Health Records Policy & Disclosure of Personal Data Procedure**

**Version No: 1**

The purpose of the Access to Health Records Policy is to ensure there is a systematic approach to the management and the process of access that is understood by all staff.

| | |
|---|---|
| **Document type** | Access to Health Records Policy & Disclosure of Personal Data Procedure |
| **Date approved** | 2nd February 2018 |
| **Date implemented** | 2nd February 2018 |
| **Next review date** | **July 2021** or sooner should legislative change require. |
| **Policy author** | StHK IG Team |
| **Applies to** | All Staff |

# Table of Contents

## SCOPE

The Practice is committed to providing an effective Access to Health Record Service which deals appropriately with requests for access to information.

This policy was developed in conjunction with the guidance outlined in the Access to Health Records Act 1990, Data Protection Act 2018 and advice from the Information Commissioner's Office following the General Data Protection Regulation (GDPR) which came into force on 25th May 2018.

## INTRODUCTION

This policy has been produced to ensure the Practice meets its obligations regarding requests for access to health records. It defines the different types of requests for access to a health record a Practice may receive and how to respond to such requests. The policy is divided into the following areas.

- Subject access request (SAR)
- Request for access made on behalf of others
- Requests from the police
- Requests from insurers
- Deceased patients

Staff should treat this policy as guidance based on best practice for managing access to health records requests.

***The unauthorised passing on of patient personal information by staff is a serious matter and will result in disciplinary action as it is a criminal offence.***

Staff must not allow personal details of patients to be passed on or sold for fund-raising or commercial marketing purposes.

## STATEMENT OF INTENT

This policy is intended to:

- Set out a clear process for dealing with requests for access to health records for living and deceased patients.
- Ensure the Practice complies with the requirements for access to health records, the Data Protection Act 2018, and the General Data Protection Regulation therefore avoiding the potential cost penalties associated with non-compliance;
- To ensure all staff at the Practice realise an individual has a right under GDPR/DPA2018 to be provided with access to their own PCD which the Practice holds about them.

- Ensure that staff are clear about the process for managing access requests, including their responsibilities in relation to this;

- Ensure staff adhere to the principles of being open in line with the Practice's Being Open policy in matters relating to health records whilst at the same time ensuring there are robust measures in place to ensure patient confidentiality;

- A step by step procedure for all Practice staff to follow.

**Legislation relevant to this policy;**

- The Data Protection Act 2018
- The General Data Protection Regulation
- The Access to Health Record Act 1990
- The Access to Medical Report Act 1988
- The Freedom of Information Act 2000
- The NHS Confidentiality Code of Practice 2003
- Common Law Duty of Confidentiality
- Mental Capacity Act 2005

## DEFINITIONS

An **Access to Health records request** is any request for personally identifiable data and can be made by the data subject or other party.

An **application** means an application in writing or verbally

A **Health record** is defined as information relating to the physical and / or mental health of an individual who can be identified from that Information and which has been made by, or on behalf of a Healthcare Professional, in connection with the care of that individual. . The information is most commonly recorded in electronic form, however some records are in a manual form or a mixture of both. 'Information' covers expressions of opinion about individuals as well as facts.

Health records may include notes made during consultations, correspondence between health professionals such as referral and discharge letters, results of tests and their interpretation, X-ray films, videotapes, audiotapes, photographs, and tissue samples taken for diagnostic purposes. They may also include reports written for third parties such as insurance companies.

The **holder** of the record is the Practice by which, or on whose behalf, the record is held.

The **patient** is the individual in connection with whose care the record has been made.

**Personal Data** means any information relating to an identified or identifiable individual.

The **Healthcare Professional** can be one or more of the following registered professions:

- Medical practitioner
- Dentist
- Optician
- Pharmaceutical chemist
- Nurse
- Midwife
- Health visitor
- Osteopath
- Chiropractor
- Podiatrist
- Dietician
- Occupational therapist
- Orthoptist
- Physiotherapist
- Clinical psychologist
- Child psychotherapist
- Speech therapist
- An art or music therapist employed by the Health Service
- Any other registered member of a Profession Supplementary to the Medicines Act 1960
- A scientist employed by the Health Service as a head of department

A **subject access request** is a request from a person asking an organisation to provide them with information relating to that person which is held or processed by the organisation.

## DUTIES, ACCOUNTABILITIES AND RESPONSIBILITIES

This policy applies to all those working within the Practice, in whatever capacity. A failure to follow the requirements of the policy may result in investigation and management action being taken, in line with the Practice's disciplinary policy and procedure.

The Information Governance Lead/Practice Manager must make their staff aware of the Access to Health Records Policy at the earliest possible opportunity.

## Senior Managers

Managers must give their full backing to all the guidelines and procedures as set out and agreed. They must ensure that their staff are aware and adhere to the policy requirements**.**

The Practice Manager has responsibility for ensuring all subject access requests relating to complaints are actioned. Is also responsible for requests by employees or ex-employees for copies of their personal employment files (this includes medical and non-medical staff).

## The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that the Practice processes satisfy the highest practical standards for handling patient information and provide advice and support to Practice staff as required. The Caldicott Guardian is responsible for ensuring that patient identifiable information is shared appropriately and in a secure manner. The Caldicott Guardian will liaise where there are reported incidents of person identifiable data loss or identified threats and vulnerabilities in Practice information systems to mitigate the risk

## Data Protection Officer (DPO)

The role of the DPO under GDPR includes:

- Inform and advise the organisation and its employees of their data protection obligations under the GDPR.
- Monitor the organisation's compliance with the GDPR and internal data protection policies and procedures. This will include monitoring the assignment of responsibilities, awareness training, and training of staff involved in processing operations and related audits.
- Advise on the necessity of data protection impact assessments (DPIAs), the manner of their implementation and outcomes.
- Serve as the contact point to the data protection authorities for all data protection issues, including data breach reporting.

The DPO will be independent and an expert in data protection. The DPO will be the Practice's point of contact with the Information Commissioner's Office.

## Practice Staff

It is the responsibility of all staff to co-operate in a timely manner regarding the investigation of access requests. In cases of non-compliance outstanding reports from staff will be pursued on request by the Practice Manager.

In terms of **record keeping**, health records must be clear, accurate, factual, legible and should be contemporaneous. They must include all relevant clinical findings, the decisions made, information given to patients, and drugs or treatment prescribed. Personal views about the patient's behaviour or temperament should not be included unless they have a

potential bearing on treatment or it is necessary for the protection of staff or other patients. Health records should not be altered or tampered with, other than to remove or correct inaccurate or misleading information. Any such amendments must be made in a way that makes it clear what has been altered, who made the alteration and when it took place.

Doctors and other clinical staff should ensure that their manner of keeping records facilitates access by patients if requested. It may be helpful to order, flag or highlight records so that when access is given, any information which should not be disclosed, (such as those which identify third parties) is readily identifiable. If patients express views about future disclosure to third parties, this should be documented in the records. Doctors may wish to initiate discussion about future disclosure with some patients if it seems foreseeable that controversial or sensitive data may be the issue of a future dilemma, for example after the patient's death.

## POLICY

Practice staff will read and adhere to this policy and procedure in order to effectively and efficiently comply with all requests for access to health records which the Practice receives. Individuals have the right to ask for a copy of the information an organisation holds about them; this right is known as a Subject Access Request (SAR)

The Practice recognises that staff may find the process of personal access requests stressful and acknowledges that it is important that staff are appropriately supported. Any member of staff who has concerns or wishes to receive support or guidance in respect of their involvement in the access process should contact their Line Manager or senior Clinical Staff who will be available to provide or arrange support as appropriate.
There are certain formalities, which must be observed when applying to see records under the Act. It may seem a rather complicated process but it is of vital importance to make sure that the records are released only to the right person, because the confidentiality of records calls for the greatest safeguards.

- Any member of staff receiving a formal request for access, either verbally or in writing must advise the Practice Business Manager
- If access to records is granted, proof of identity will be required in order to avoid any possible breach of confidentiality. This can be a passport, driving licence, utility bill or birth certificate.
- In order to ensure that we meet the terms of the Act, the administration will be co-ordinated by a named individual.
- If arrangements are made for patient's medical notes to be viewed, the viewing would normally be in the presence of a member of the Admin team available on the day.

## SUBJECT ACCESS REQUEST

A Subject Access Request (SAR) is a request by the data subject/patient or a request by a third party who has been authorised by the patient, for access to their health record under the GDPR/DPA 2018.

A Subject Access Request (SAR) can be made;

- Verbally
- Electronically
- In writing

All SAR received must be recorded on a SAR register (see appendix 1)including the date the application was received, the date all information requested was received e.g. ID, fee if appropriate, consent etc. The identity of the requester must be verified before providing access.

The requestor may be invited by a member of the team to use the Practices SAR form (see appendix 2). Reasonable adjustments may be considered and/or made for disabled people, for example, responding in an appropriate format such as in Braille or large print. However the data subject does not have to complete this form they can put their request in another format as highlighted above.

### Timescale for Disclosure

The Act imposes very specific duties upon us, which have to be carried out within a very tight timescale.

The information is to be supplied within 1 month from the date of the request for access or 1 month from the date you have sufficient information to enable you to satisfy yourself as to the identity of the person making the request and to locate the information requested.

For complex or numerous requests to access the same records the Practice can extend the timescale by a further 2 months. Applicants will be informed immediately.

### Who may apply for access?

The following can request for access;

- Patients with capacity
- Children and young people under 18
- Solicitors

#### Data Subject (patients) with capacity

The Practice understands it is not necessary for a data subject /patient to provide a reason as to why they wish to access their health record. Subject to the exemptions listed in paragraph 7.7. Data subjects with capacity have a legal right to request access to their PCD via a SAR under GDPR/DPA 2018. A data subject may also authorise a third party such as solicitor to request access on their behalf.

**Children and young people age 13 and above**

The Practice understands a child aged 16 and over is presumed to be competent, they are entitled to request access to information held about them. Children who are aged 13 or over, are generally expected to have the competence to give or withhold their consent to the release of information from their health record. However, children aged between 13 and 16 must demonstrate that they have sufficient understanding of what is proposed(termed as being Gillick Competent) in order to be entitled to make or consent to a SAR. Where a child aged 13 and above is considered capable of making decisions (termed as being Gillick Competent) about access to his or her medical record, the consent of the child must be sought before a parent or third party can be given access via a SAR.

Upon assessment from an appropriate health professional at the Practice and where the Practice believes a child lacks competency to understand the nature of his or her SAR application, the Practice is entitled to refuse to comply to the SAR. Where a child is deemed not to have capacity to consent to the access to their own health record; an applicant with parental responsibility of the data subject can request access following;

- The applicant is the child's natural mother (and there is no resident or other Court Order to the contrary). We have to take the applicants / solicitors written word for this at face value. This is often referred to as *acting in loco parentis* and is where the patient is under age 16 and is incapable of understanding the request.
- The applicant is the child's natural father or was married to the child's natural mother at the time of conception or birth of the child. NB the father does not necessarily still have to be married to the child's natural mother. He could be legally separated or divorced from her. Also, this whole point only applies providing that there is no residence or other Court Order to the contrary. We can accept Solicitors written confirmation of this. Marriage / Divorce papers are not necessary.
- The applicant is the child's natural father but was not married to the child's natural mother at the time of conception or birth of the child, but there is an agreement between both parents, which has been passed by a Court of Law, expressly giving the natural father parental responsibility. Documentation will exist if this is the case, and a photocopy of it should be obtained. Since December 2003, if the mother agrees, an unmarried father has parental rights if the child was registered together and the father's name is on the Birth Certificate.
- The applicant has parental responsibility by way of a Residence Order. This could be the child's natural father, a grandparent or other relative. Documentation will exist if this is the case, and a photocopy of it should be obtained. NB a Residence Order is not time limited – up to their sixteenth birthday unless discharged.

- If the applicant does not satisfy any of the above criteria, then access to the records will be denied, unless the applicant can provide the written authority of someone who has got parental responsibility.

**Requests from solicitors**

A data subject/patient can authorise a solicitor to act on their behalf to make a SAR. Necessary steps will be taken to verify this is a valid request and the data subject's written consent has been obtained. It is the solicitor's responsibility to provide the patient's written consent. There must be complete transparency; the data subject must be fully aware to what they are consenting to. The consent captured must be freely given, informed and specific including the nature and extent of the information to be disclosed under the SAR, past medical history and who might have access to it as part of the legal proceedings.

In the event of where a patient refuses to allow a solicitor access to their health record, the solicitor may apply for a court order requiring disclosure of the information. (See appendix 2 for a third party Consent form)

**Lasting power of attorney and an incapacitated patient's records**

A Lasting Power of Attorney (LPA) authorises another person appointed by the patient to make decisions about their property and finances and/or health and welfare, which could include decisions about healthcare. However, it does not give an automatic right to see a patient's notes. The reason for this is that patients may have issues recorded in their notes that they may not wish others to see (even LPAs)-for example unknown relationships, sexuality and so on and/or sensitive health issues such as termination of pregnancy, HIV status, sexually transmitted diseases and so on. Patient confidentiality is paramount here.

Therefore always check the following before releasing a patient's records if they are incapacitated and have an LPA:

- The person applying for access must apply formally as per the policy for a SAR
- *and* The LPA must explicitly give permission for healthcare decisions for the named patient
- *and* It must be registered and there must be proof of registration with the Office of the Public guardian
- *and* the consultant in charge must check the notes and establish whether if it is thought to be in the patient's best interests and if any information should be withheld.
- Contact the Practice Business Manager if further advice is needed as this is a patient confidentiality issue.

## Processing a Subject Access Request

SARs can be made electronically, in writing or verbally**;**

The Orchard Surgery understand the requirement to comply with the DPA 2018/GDPR and the Practice will take all necessary step to respond to data subject access request within/no later than 1 calendar month after verifying the identity of the requestor and obtaining consent from the data subject where applicable. An extension of 2 months may apply where a request is complex or excessive; The Practice will take necessary steps to inform the data subject or requestor without delay.

## Administrative Fees

A fee cannot be charged for processing and responding to a subject access request from a data subject including a request made by third party on behalf of the data subject e.g. solicitors.

Initial access must be provided free of charge.

For further requests for the same information, a 'reasonable fee' can be charged if the request for PCD is 'manifestly unfounded' or 'excessive'.

For the avoidance of doubt the ICO have confirmed;

*"A SAR for the whole medical record would never be considered excessive for the purposes of imposing a charge. As to what constitutes 'excessive', the legislation is clear that this would be by way of repeated/vexatious requests and* ***NOT*** *dictated by the size of the record."*

Charging a fee for access to health records is likely to be rare; if a fee is charged it must be justified and the reason recorded.

This is not to be confused with a request for a medical report under the Access to Medical Records Act 1990 (See section 9) where the request for the report is chargeable.

## Maintaining confidentiality

The Practice will take necessary steps to protect and maintain the confidentiality of the data subject at all times whilst handling, processing and responding to a SAR and information about third party persons contained on a data subject record will be redacted before disclosure.

## What supplementary information must be provided with a SAR?

The GDPR requires the following additional information must be provided when providing copies of health records;

- The purpose for processing data
- The categories of personal data

- The organisations with which the data has been shared
- The existence of rights to have inaccurate data rectified
- Right to complain to the ICO

A copy or the link to the Practices Privacy notice which contains all this information will be provided with each SAR.

## Can access be refused?

If a request is 'manifestly unfounded or excessive', for example, because it is repetitive, access can be refused (or a fee can be charged, see above paragraph 5.3). There is little explanation from the legislation as to when a request might be considered as 'manifestly unfounded or excessive'. However, the threshold must be set fairly high and that accordingly requests should be refused on this basis only where the facts are particularly extreme.

Where access has been refused on this basis, the patient must in any event be given an explanation as to why access has been refused and they must also be informed that they have the right to complain to the ICO.

## When should information not be disclosed?

Information can be treated as exempt from disclosure and should not be disclosed, if:

- it is likely to cause serious physical or mental harm to the patient or another person; or
- 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 Practice concludes it is reasonable to withhold third party information; or
- it is requested by a third party and, the patient had asked that the information be kept confidential, or the records are subject to legal professional privilege, or the records are subject to confidentiality as between client and professional legal advisor. This may arise in the case of an independent medical report written for the purpose of litigation. In such cases, the information will be exempt if after considering the third party's right to access and the patient's right to confidentiality, the Practice reasonably concludes that confidentiality should prevail; or
- it is restricted by order of the courts; or
- it relates to the keeping or using of gametes or embryos or pertains to an individual being born as a result of in vitro fertilisation; or

- in the case of children's records, disclosure is prohibited by law, e.g. adoption records.

The Practice will redact, or block out any exempt information. Depending on the circumstances, the response will include an explanation to the requestor around how it has applied the relevant exemption. However, such steps should/ will not be taken if, and insofar as, they would in effect cut across the protections afforded by the exemptions. In some cases even confirming the fact that a particular exemption has been applied may itself be unduly revelatory (e.g. because it reveals the fact that the information sought is held where this revelation is itself unduly invasive of relevant third party data privacy rights). There is still an obligation to disclose the remainder of the records. While the responsibility for the decision, as to whether or not to disclose information, rests with the Practice, advice about serious harm will be taken by the Practice from the appropriate health professional before the records are disclosed. This is usually the health professional currently or most recently responsible for the clinical care of the patient in respect of the matters which are the subject of the request. If there is more than one, it should be the person most suitable to give advice. If there is none, advice should be sought from another health professional that has suitable qualifications and experience.

Circumstances in which information may be withheld on the grounds of serious harm are extremely rare, and this exemption does not justify withholding comments in the records because patients may find them upsetting. Where there is any doubt as to whether disclosure would cause serious harm, an appropriate health professional will discuss the matter anonymously with an experienced colleague such as the Data Protection Officer, or the Caldicott Guardian.

## REQUESTS FOR ACCESS MADE ON BEHALF OF OTHERS.

The GDPR/DPA 2018 does not provide subject access rights to third parties when they are acting on behalf of an induvial who is lacking competence or capacity. However they may still be able to access information as outlined below.

### Parents

Parents with parental responsibility may apply for access to confidential information of children aged 13 and above if the request is not contrary to the child's best interest or a competent child's wishes. Under the Data Protection Act a competent child may consent to processing from the age of 13, providing they are Gillick competent.

### Individuals with a responsibility for adults who lack capacity

Requests from individuals with a responsibility for the data subject/patient may not automatically be entitled to access the data subject's health record. Necessary steps will be taken to assess a

data subjects mental capacity based on the request made on behalf of a data subject and in line with the Mental Capacity Act 2005

## REQUESTS FROM THE POLICE

The Practice can release confidential information if the data subject/patient has provided consent and understands the consequences of making that decision. The police do not have an automatic right to access PCD of a data subject unless there is a court order or this is required under statute (e.g. Road Traffic Act). If the police do not have a court order or warrant they may ask for a patient's health record to be disclosed voluntarily under the DPA 2018 Exemptions in Schedule 2 Part 1(2).

If the Practice receives a police request the following procedure must be followed (see attachment) and the request must only be authorised by the Practice Business Manager. Only disclose PCD if you have;

1. Obtained Consent from the data subject/patient or
2. There is an overriding public interest.

An overriding public interest is a disclosure that is essential to prevent a serious threat to public health, national security, the life of an individual or a third party, or to prevent or detect a serious crime. This includes crimes such as murder, rape, kidnapping and abuse.

## REQUESTS FROM INSURANCE COMPANIES

If a request is asking for a report to be written or it is asking for an interpretation of information within the record this is not a Subject Access Request. These requests fall under the Access to Medical Reports Act (AMRA)1990.

In these circumstances, the Practice will clarify the nature of the request from the third party. If the third party confirms that they are seeking a copy of the medical record then this should be treated as a SAR and complied with in the usual way.

What third parties cannot do is seek a SAR for information under the AMRA. The position of the ICO is that the use of SARs to obtain medical information for life assurance purposes is an abuse of subject access rights and the processing of full medical records by insurance companies risks breaching the GDPR. It is a criminal offence (clause 181 DPA18) for a third party to trick or encourage a patient to use SARs to obtain medical information for life assurance purposes.

This does not mean, however, that the Practice can refuse to respond to a SAR from an insurer outright. When a SAR from an insurance company is received, the Practice will contact the patient to explain the extent of the disclosure that has been sought. If requested, the patient themselves can be provided with their medical record rather than providing them directly to the insurance company. It is then the patient's choice as to whether, having reviewed the record, they choose to share it with the insurance company.

The AMRA deals with reports or requests for information relating to employment and insurance purposes – accident claims, mortgages, etc. If you receive a request for information that requires you to create a document, this is not a subject access request and is chargeable.

There is a clear distinction between the use of SARs by a solicitor, who can be seen as an agent of the patient and who is acting on the patient's behalf, and the use of SARs by insurance companies. Insurance companies should use the provisions of the Access to Medical Reports Act 1988 to seek reports.

## REQUESTS TO ACCESS A DECEASED PATIENT RECORD

GDPR/ DPA2018 does not apply to data concerning a deceased patient. Request for PCD for deceased patients can only be made under the Access to Health Record Act (AHRA) 1990. When a request is made to access PCD of a deceased patient, the Practice will take necessary steps to seek the reason for such a request; as the duty of confidentiality needs to be balanced with other consideration such as when a request is made in the interest of justice and of people close to the deceased. The Practice will continue to exercise its ethical obligation to respect a patient's confidentiality beyond their death.

### Who legally can apply for access?

- The patient's personal representative (the executor or administrator of the deceased person's estate)
- Any other person who may have a claim arising out of their death has a right of access to information in their records, which is directly relevant to a claim.
- While there is no legal entitlement other than the limited circumstances covered under the AHRA legislation, health professionals have always had discretion to disclose information to a deceased person's relatives or others when there is a clear justification.

The medical record needs to be checked to ensure the patient's wishes are respected after death and all third party information which may cause distress, serious mental and physical harm to anyone is redacted.

A copy of the record should be supplied to the requester within 40 days if the request is for PCD concerns information which was recorded more than 40 days before the date of the request.

If the PCD requested was recorded in the 40-day period before the date of application then access must be given within 21 days.

## Can a Fee be charged?

A fee can be charged for supplying a copy of the requested information. However the fee must not exceed the cost of making the copy any postal charges must reflect the true cost. (As per BMA guidance)

Health professionals may charge a professional fee to cover the costs of giving access to the records of deceased patients that is not covered by legislation.

Refer to the AHRA 1990 for more in depth information for access to a deceased record.

## DISCLOSURE REQUIRED BY STATUTE

- Under the Mental Capacity Act 2005, Independent Mental Capacity Advocates (IMCAs) have rights of access to health/clinical records relating to the patient they are presenting. The Practice is required to give access to relevant records requested by an IMCA under S.35 (6) (b) of the Act. The rights of the IMCA include the right to examine and take copies of any records.

- The Mental Health Act (2007) gives Independent Mental Health Advocates (IMHA) the right to access information relating to some individuals who are subject to the Mental Health Act.

- The Medical Act 1983 gives the General Medical Council ("GMC") powers under S.35A for taking action when questions arise about fitness to practise. As part of a fitness to practice investigation, the GMC may request access to medical records. The Practice must comply with this request and have 14 days to process and provide copies of the information held.

- The Criminal Appeal Act 1995 gives the criminal Cases Review Commission the right to access clinical records requested. Consent from the service user is not required in the circumstances.

- The Coroner and Justice Act 2009 gives Coroners the power to request for any documents including health records. As part of the investigation into a deceased death, the coroner might request for health records and the Practice will be obliged to disclose these to the coroner.

## RETENTION

The practice will log and retain all SARs and access to a deceased patient's record in a register. All records will be kept in line with the Record Management Code of Practice 2016.

When records are destroyed by health professionals they must ensure the method of destruction is effective and does not compromise confidentiality.

Appendix 3 of the Records Management Code of Practice for Health & Social Care 2016 defines the retention schedules for all health records which the Practice adheres to.

## POLICY EXCLUSIONS

- Duplicate records provided to other health care providers;
- Duplicate individual letters provided directly to patients by consultants/medical secretaries ;
- Medical reports that are completed by consultants for the benefit of the courts, insurance companies and the Police are outside the scope of this Policy as they do not constitute health records;
- Access data that is anonymised or pseudonymised which cannot identify the individual;
- The provision of original records for court purposes, however the Practice will take a paper copy of these records prior to release;
- Adopted children with new names are outside the scope of this policy. There is one national register of old and new names of adopted children held by the Department of Health whom these adopters will need to apply.
- Freedom of Information Request under the Freedom of Information Request Act 2000

## COMPLAINTS CONCERNING ACCESS TO HEALTH RECORDS

If the applicant feels that they have not been fairly treated and that the holder of the record has not complied with the DPA 2018, then they should first complain in writing to Practice Business Manager, The Orchard Surgery, Bromborough Village Road, Bromborough, Wirral, CH62 7EU. If they are still unhappy after this, the patient has the right to apply to Court if necessary. The Court can order that the applicant be given access to the records if it is satisfied that the complaint is justified.

## REFERENCES


| Author | Year | Title | Edition | Place of Publication |
|---|---|---|---|---|
| Her Majesty's Stationery Office (HMSO) | 2018 | Data Protection Act | 2nd | London UK |
| Official Journal of the European Union | 2016 | General Data Protection Regulations | 1st | European Union |
| HMSO | 2000 | Freedom of Information Act | | London UK |
| British Medical Association (BMA) | July 2018 | Access to Health Records | | London UK |