GLENDALE MEDICAL CENTRE

SUBJECT ACCESS REQUEST POLICY

Introduction

This policy provides the Practice with a process for the management of requests for personal information (for living individuals) under the Data Protection Act (DPA), the General Data Protection Regulations (GDPR) and (for deceased individuals) the Access to Health Records Act 1990.

It defines a process for achieving legislative requirements and ensuring effective and consistent management of such requests.

The policy ensures that all staff are aware of how a subject access request should be made and to respond quickly.

Under the Data Protection Act, subject to certain conditions, an individual is entitled to be:

- Told whether any personal data is being processed;
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people; and
- Given a copy of the information comprising the data; and given details of the source of the data (where this is available).

The Data Protection Act extends equally to all relevant records relating to living individuals, including records held in the private health sector and health professionals' private practice records.

Personal data held by the Practice may be:-

- Personnel/Staff records relating to a member of staff, present, past or prospective, whether permanent, temporary or volunteer
- Health records consisting of information about the physical or mental health of an identifiable individual made by, or on behalf of, a health professional in connection with the care of that individual.

Access encompasses the following rights:-

- To obtain a copy of the record in permanent form
- To have information provided in an intelligible format (and explained where necessary)

The Data Protection Act also gives subjects who now reside outside the UK the right to apply for access to their former UK health and employment records:

- Employees are legally entitled to request their personal records and may take them outside of the UK at their own discretion.
- Original health records should not be given to people to keep/take outside the UK. A GP or community health professional may be prepared to provide the patient with a summary of treatment; alternatively the patient may make a request for access in the usual way.

Organisations must have procedures in place to ensure that individual's rights of access are met within a timely and appropriate fashion.

Individual's rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

In the response to the Caldicott2 Report, the Department of Health confirmed that service users should have access to information about themselves even if it was obtained through new or non-traditional approaches (for example, virtual consultations) to delivering health and care services.

The BMA Confidentiality and Health Records Toolkit helps identify the key factors to take into consideration when making a decision around confidentiality and disclosure of health records.

Scope

This policy applies to any request by a patient or member of staff for access to their personal information held by the Practice.

This policy applies to all staff (employees, governing body members, contractors) of the Practice.

Who can make an Access Request?

An application for access to personal data may be made to the Practice by any of the following:-

- an individual
- a person authorised by the individual in writing to make the application on an individual's behalf e.g. solicitor, family member, carer
- a person having parental responsibility for the individual where he/she is a child.
- a person appointed by a court to manage the affairs of an individual who is deemed incompetent
- individuals who hold a health and welfare Lasting Power of Attorney
- where the individual has died, the personal representative and any person who may have a claim arising out of the individual's death (the executor of the deceased's will; someone who has been appointed as an Administrator of the Estate by the Courts; someone who has the written consent of either of the above to be given access, someone who is in the process of challenging the deceased's will)

•

Police Requests

The Police may, on occasion, request access to personal data of individuals. Whilst there is an exemption in the Data Protection Act which permits the Practice to disclose information to support the prevention and detection of crime, the Police have no automatic right to access; however they can obtain a Court Order.

Solicitor Requests

A patient can authorise their solicitor or another third party to make a SAR. As long as the solicitor has provided the patient's written consent to authorise access to the records, the SAR process should be followed as usual.

Insurance Requests

Insurance companies however do not have the same privileges to access patient records – the ICO has said that insurance companies using SARs to obtain full medical records is an abuse of the process (the DPA 2018 still says that information must be adequate, relevant and not excessive in relation to the purpose the data is processed).

It is a criminal offence to make a SAR to access information about individuals' convictions and cautions – the law sets out various levels of fines, and a clause in the DPA 2018 will soon be enacted to extend this to cover medical records. If you suspect that a SAR from an insurer is not relevant or excessive then it should be reported to the ICO and the Association of British Insurers

Requests relating to children/young persons

Parental responsibility for a child is defined in the Children's Act 1989 as 'all the rights, duties, powers, responsibilities and authority, which by law a parent of a child has in relation to a child and his property'. Although not defined specifically, responsibilities would include safeguarding and promoting a child's health, development and welfare, including if relevant their employment records. Included in the parental rights which would fulfil the parental responsibilities above are:

- having the child live with the person with responsibility, or having a say in where the child lives;
- if the child is not living with her/him, having a personal relationship and regular contact with the child;
- controlling, guiding and directing the child's upbringing.

Foster parents are not ordinarily awarded parental responsibility for a child. It is more likely that this responsibility rests with the child's social worker and appropriate evidence of identity should be sought in the usual way.

The law regards young people aged 16 or 17 to be adults for the purposes of consent to employment or treatment and the right to confidentiality. Therefore, if a 16 year old wishes HR or a medical practitioner to keep their information confidential then that wish must be respected.

In some certain cases, children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected.

Where a child is considered capable of making decisions, e.g. about his/her employment or medical treatment, the consent of the child must be sought before a person with parental responsibility may be given access. Where, in the view of the appropriate professional, the child is not capable of understanding the nature of the application, the holder of the record is entitled to deny access if it is not felt to be in the patient's best interests.

The identity and consent of the applicant must always be established.

The applicant does not have to give a reason for applying for access.

The Practice is a Data Controller and can only provide information held by the organisation. Data controllers in their own right must be applied to directly, the Practice will not transfer requests from one organisation to another.

Application

Individuals wishing to exercise their right of access should:

- Make a written application to the Practice holding the records, including via email
- Provide such further information as the Practice may require to sufficiently identify the individual

An individual may also raise a request using the form in **Appendix A**, however this is not mandatory.

The Practice as "data controller" is responsible for ascertaining the purpose of the request and the manner in which the information is supplied.

Fees and Response Time

Under GDPR the Practice musts provide information free of charge. However, we can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee must be based on the administrative cost of providing the information only.

The request should be initially passed to the Data Protection Officer who will manage Subject Access Request.

If the request involves creating a medical report or interpreting the information in an existing medical record or report, then this would be a request under the **Access to Medical Reports Act (AMRA)**. Unlike a Subject Access Request, these requests will require new material to be created. **This would mean that a fee is payable in such circumstances.**

Appendix A to this policy prompts the applicant to clarify whether they wish to make this type of request.

The request must be complied with without delay and at least within **one calendar month** of receipt of the request. This period can be extended for a further two months where requests are complex or numerous, however the Practice must inform the individual within one month of receipt of the request and explain why the extension is necessary.

The identity of an individual who provided/recorded information should not be disclosed, nor should the identity of any other person/s referred to in the record(s) of the individual requesting access, unless explicit consent has been given.

The Release Stage

The format of the released information must comply with the requester's wishes. Where no specific format is requested, the Practice should provide the information in the same manner as the original request. For example, requests received via email can be satisfied via email.

The release of a health record is subject to consultation with either:-

- The health professional who is currently, or was most recently, responsible for the clinical care of the data subject in connection with the information which is the subject of the request
- Where there is more than one such health professional, the health professional who is the most suitable to advise on the information which is the subject of the request

Once the records have been collated, redacted where applicable and signed off by the Caldicott Lead, they should be sent to the requester. On no account must the original record be released.

In denying or restricting access, a reason for the decision does not need to be given but the applicant should be directed through the appropriate complaint channels.

Where information is not readily intelligible, an explanation (e.g. of abbreviations or terminology) must be given.

If it is agreed that the subject or their representative may directly inspect the record, a health professional or HR administrator must supervise the access. If supervised by an administrator, this person must not comment or advise on the content of the record and if the applicant raises enquiries, an appointment with a health professional must be offered

Exemptions

Access may be denied or restricted where:

- The record contains information which relates to or identifies a third party that is not a care professional and has not consented to the disclosure. If possible, the individual should be provided with access to that part of the record which does not contain the third party information
- Access to all or part of the record will prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental well-being of the individual or any other person is likely. If possible the individual should be provided with access to that part of the record that does not post the risk of serious harm
- Access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious harm
- If an assessment identifies that to comply with a SAR would involve disproportionate effort under section 8(2)(a) of the Data Protection Act (**Appendix C**).

There is no requirement to disclose to the applicant the fact that certain information may have been withheld.
In addition, Article 23 of the GDPR enables Members States, such as the United Kingdom to introduce further exemptions from the GDPR's transparency obligations and individual rights. The Data Protection Officer can provide further information regarding exemptions applicable at the time of receipt of the subject access request.

Complaints and Appeals

The applicant has the right to appeal against the decision of the Practice to refuse access to their information. This appeal should be made to [*insert name and role*].

If an applicant is unhappy with the outcome of their access request, the following complaints channels should be offered:

- meet with the applicant to resolve the complaint locally
- Advise a patient to make a complaint through the complaint's process
- Advise a member of staff to consult with their trade union representative

If individuals remain unhappy with the Practice response, they have the right to appeal to the Information Commissioner's Office:

https://www.ico.org.uk/Global/contact_us.

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 0303 123 1113

Email: casework@ico.gsi.gov.uk

Roles and Responsibilities

The Caldicott Lead has executive responsibility for Subject Access Requests.

The Data Protection Officer has operational responsibility for Subject Access Requests.

All staff must be aware of how to recognise and manage a subject access request. Training will be provided to staff likely to be in receipt of requests covering:-

- Required format of a subject access request
- Correct identification of the requesting individual
- Location of personal information
- Timescales for compliance
- Provision of information in an intelligible format
- Action to be taken if the information includes third party data or if it has been determined that access will seriously harm an individual (see exemptions)