PENN SURGERY
2a Coalway Road, Penn
Wolverhampton, West Midlands. WV3 7LR
Surgery Telephone: 01902 333408 Website: www.pennsurgery.co.uk

Access to Medical Records Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	21/02/2019	Lisa Hayden	Dr D. Bush	
2	18/09/2020	Lisa Hayden	Dr I. Martin	updated
3	18/11/2020	Lisa Hayden	Dr I. Martin	Updated. New request form
4	22.12.2021	Lisa Hayden	Dr I. Martin	updated
5	14.07.2022	Lisa Hayden	Dr I. Martin	Significant update

1 Introduction

1.1 Policy statement

The law states that 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.

The purpose of this document is to ensure appropriate procedures are in place at Penn Surgery to enable individuals to apply for access to health records (commonly referred to as a medical record), whether online or by requesting a copy, and to enable authorised individuals to apply for access to information held about other people.

Access to medical records can be provided via:

- An online portal linked to the organisation's webpage
- A variety of NHS approved apps
- A verbal subject access request (SAR)
- A written SAR including email and/or through social media

This policy is written in conjunction with the following government legislation:

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data Protection (Subject Access Modification) (Health) Order 2000

Throughout this document, references have been taken directly from the Information Commissioners Office (ICO).

1.2 Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

1.3 KLOE

The Care Quality Commission would expect any primary care organisation to have a policy to support this process and this should be used as evidence of compliance against CQC Key Lines of Enquiry (KLOE)[1].

Specifically, Penn Surgery will need to answer the CQC key questions on “Safe”, “Effective” and “Caring”. The following is the CQC definition of Safe:

“By safe, we mean people are protected from abuse and avoidable harm.*

**Abuse can be physical, sexual, mental or psychological, financial, neglect, institutional or discriminatory abuse.”*

CQC KLOE S3	Do staff have all the information they need to deliver safe care and treatment to people?
CQC KLOE S4	How does the provider ensure the proper and safe use of medicines where the service is responsible?

The following is the CQC definition of Effective:

“By effective, we mean that people’s care, treatment and support achieve good outcomes, promotes a good quality of life and is based on the best available evidence.”

CQC KLOE E1	Are people’s needs assessed and care and treatment delivered in line with current legislation, standards and evidence-based guidance to achieve effective outcomes?

The following is the CQC definition of Caring:

“By caring, we mean that the service involves and treats people with compassion, kindness, dignity and respect.”

CQC KLOE C3	How are people's privacy and dignity respected and promoted?

1.4 Training and support

The organisation will provide guidance and support to help those to whom it applies to understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

2 Scope

2.1 Who it applies to

[1] KLOE

This document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

Furthermore, it applies to clinicians who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS).[2]

2.2 Why and how it applies to them

This document explains how patients can access their medical records or those of another individual either by registering for online services or by making a subject access request (SAR) at Penn Surgery. This is particularly relevant to the administration and reception staff; however, all staff should be aware of the available online services and SARs process and be able to advise patients, relatives and carers of the appropriate process.

Failure to comply with the policy and any associated breaches of patient data or confidentiality could lead to prosecution or imposition of penalties by the Information Commissioners Office (ICO).

3 Definition of terms

3.1 App

An app is computer software, or a programme, most commonly a small, specific one used for mobile devices.

The term app originally referred to any mobile or desktop application but, as more app stores have emerged to sell mobile apps to smartphone and tablet users, the term has evolved to refer to small programmes that can be downloaded and installed all at once[3].

3.2 Coercion

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

3.3 Data

The UK GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data. Personal data that has been pseudo-anonymised, e.g., key-coded, can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual[4].

3.4 Data Protection Act 2018

[2] Network DES Contract specification 2022/23
[3] Techopedia
[4] ICO - Anonymisation: managing data protection risk code of practice

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK General Data Protection Regulation (UK GDPR) [5].

3.5 Employment record

An 'employment record' is defined as any record that consists of information relating to a current or former member of staff and has been made by or on behalf of Penn Surgery in connection with the individual's employment.

3.6 UK General Data Protection Regulation (UK GDPR)

The UK GDPR sets out the key principles, rights and obligations for most processing of personal data in the UK[6].

3.7 Health record

A health record is defined as being any record which consists of information relating to the physical or mental or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual.

The definition can also apply to material held on an x-ray or an MRI scan. This means that when a subject access request is made, the information contained in such material must be supplied to the applicant[7].

3.8 Personal identifiable data (PID)

Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.[8]

The UK GDPR definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

3.9 Prospective access

Future (prospective) records access means access to information and data added to the patient record from a set date onwards. This may be the date that a patient joined the practice or from a date when access has previously been granted.

Patients who have had future (prospective) access set up before the change will continue to be able to view this information[9].

3.10 Proxy access

[5] ICO - About the DPA 2018
[6] NI Business
[7] ICO - Health data
[8] ICO - What is personal data
[9] NHS Digital

Proxy access refers to access to online services by somebody acting on behalf of the patient and usually with the patient's consent, by somebody other than the patient for example the patient's parent or carer[10].

3.11 Responsible clinician

The responsible clinician is the most appropriate health professional to deal with the access request who is the current or more recent responsible professional involved in the clinical care of the patient in connection with the information aspects which are the subject of the request.

Where there is more than one such professional, the most suitable should advise.

3.12 Sensitive personal data

The UK GDPR refers to sensitive personal data as "special categories of personal data".

The special categories specifically include revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of genetic data, biometric data (where processed to uniquely identify an individual), data concerning health or data covering an individual's sex life or sexual orientation.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

4 Right to access

Penn Surgery ensures that all patients are aware of their right to access their data and has privacy notices displayed in the following locations:

- Waiting room
- Organisation website
- Organisation information leaflet

To comply with the UK GDPR, all organisation privacy notices are written in a language that is understandable to all patients and meet the criteria detailed in Articles 12, 13 and 14 of the UK GDPR.

The privacy notices are:

- Privacy notice – Practice
- Privacy notice – Children
- COVID-19 privacy notice

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

[10] RCGP - Proxy access guidance for general practice

5 Patient access to online medical records

5.1 Background

Patient Online was designed to support GP organisations offering and promoting an online service to their patient population. The service is referred to as 'GP online services' and is offered to patients in addition to telephone and face-to-face interactions at GP organisations.[11]

All patients should have online access to their full record, including the ability to add their own information, as the default position from April 2020, with new registrants of an organisation having full online access to the digital record for their prospective information '*from summer 2022'*, starting from the date of their registration for online services.

The NHS Digital document titled Access to patient records through the NHS App states the following:

The *"Go-live date is now to be expected summer 2022, and GPs will be informed with 2 months' notice and provided with resources to support preparations".*

The organisation will need to be mindful that this level of access will be the default for all patients within the clinical system.[12] It is therefore imperative that organisations know how to manage their workflows ensuring sensitive information is redacted as it is entered onto the clinical system or, in rare circumstances, know when it may be inappropriate to give a patient access to their record.

Patients will see new information once it is entered or filed onto their record in the clinical system[13].

In addition to the detailed coded record (DCR), access to a full patient record includes free text consultation notes and documents i.e., hospital discharge letters, referral letters etc.

5.2 Registering for online services

At Penn Surgery staff are to remind patients that GP online services are free and available to all registered patients. NHS England has published a number of guides and leaflets that provide further detailed information about how patients can access their health record online.

Patients who wish to register for online services to book or cancel appointments, order repeat prescriptions, view their medical records and clinical correspondence online are to complete the registration form at Annex A.

Additionally, those applicants wishing to apply for access to information held about other people must complete the appropriate sections on the registration form also at Annex A and the application should be processed in line with the requirements outlined in the proxy access and third-party requests section.

[11] NHSE About Patient Online

[12] NHSE - Prospective records access practice guide v1.2

[13] NHS Digital - Access to patient records through the NHS App

For those patients unable to visit their own GP organisation, NHS Digital provides access to sign up for online services here where there is a requirement to provide appropriate identification using a mobile phone as part of the process.

Prospective access to full records is subject to the same safeguarding information requirements as applied to DCR access.[14] Requests for access can be refused and further detail is provided in the refusal to comply with a request and coercion sections.

Unlike registration, ID verification is required to ensure that online access is granted only to the patient or their authorised representative(s). All patients will be requested to provide two forms of ID verification in line with the NHS Good Practice Guidance on Identity Verification[15], and the organisation accepts appropriate forms of ID outlined in the identity verification section.

Completed documentation will be reviewed by the responsible clinician for processing including the review of the online records for third party references and any information that may cause harm or distress to the patient/applicant which may need to be hidden from online access using confidentiality policies (see Third party information and Non-disclosure sections).

At Penn Surgery requesters should be advised that it takes approximately 7 days to process any online service request.

5.3 Post-registration

Once a patient has registered at the organisation and the request has been processed, they are to be issued with a letter/ or email that includes their unique username, password and instructions on how to access the online services.

Only the completed registration form should be scanned into the individual's healthcare record. At Penn Surgery patients access online services using the following:

- Patient access
- NHS app

5.4 Guidance documentation

Further detailed guidance in relation to registering patients for online services can be found here.

6 Summary Care Records (SCR)

6.1 About

Summary Care Records (SCR) are an electronic record of important patient information created from GP medical records. They can be seen and used by authorised staff in other areas of the health and care system involved in the patient's direct care.

[14] BMA - Online Access to Digital GP Records 2019/20

[15] Patient Online Services in Primary Care Good Practice Guidance on Identity Verification

Access to SCR information means that care in other settings is safer, reducing the risk of prescribing errors. It also helps to avoid delays to urgent care. At a minimum, the SCR holds important information about:

- Current medication
- Allergies and details of any previous bad reactions to medicines
- The name, address, date of birth and NHS number of the patient

Further reading can be sought from NHS Digital Summary Care Records.

6.2 Additional information

Additional Information in the SCR, such as details of long-term conditions, significant medical history or specific communications needs, is now included by default for patients with an SCR unless they have previously told the NHS that they do not want this information to be shared.

Should a patient not wish to have any additional information shared, they can complete the SCR patient consent preference form.

Further reading can be sought from NHS Digital Additional information on the SCR and a patient information for additional or enhanced summary care records can be found in this poster.

6.3 COVID-19 and SCR

To help the NHS to respond to the coronavirus (COVID-19) pandemic, there is currently a temporary change to the SCR that includes COVID-19 specific codes in relation to the suspected, confirmed, shielded patient list and other COVID-19 related information. This information is also retained in the additional information.

Further reading can be sought from NHS Digital's document titled Summary Care Records - Information for Patients dated 24 March 22.

7 Subject Access Request (SAR) to medical records

7.1 Background

In accordance with Article 15 of the UK GDPR, individuals have the right to access their data and any supplementary information held by Penn Surgery.

The reason for granting access to data subjects is to enable them to verify the lawfulness of the processing of data held about them. In addition, data subjects can authorise third party access, e.g., for solicitors and insurers, under the UK GDPR.

When a data subject (individual) wishes to access their data, they are to be encouraged to use the subject access request (SAR) form which can be found at Annex B. All staff must note that the ICO state:

"An individual can make a SAR verbally or in writing, including on social media. A request is valid if it is clear that the individual is asking for their own personal data".

Any requests not using the SAR form must be processed.

This policy outlines the procedure to gain access to health records at Penn Surgery:

- Third party requests
- Requests from solicitors
- Requests from insurers (governed by the Access to Medical Reports Act 1988)

Further detailed information is available in the UK GDPR Policy.

7.2 Overview

SARs are predominantly used for access to, and the provision of, copies of medical records. This type of request need not always be in writing (e.g., letter, e-mail). However, applicants should be offered the use of a SAR application form which allows for explicit indication of the required information (see Annex B). Verbal requests should be documented and a clarification letter sent or a telephone call made to the patient for approval.[16]

There should also be an electronic form for requesters to complete if they prefer. SARs can be submitted via social media such as an organisation's Facebook page or Twitter.

Requesters must be:

- 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 this organisation of their legal authority to act on behalf of the data subject. The organisation must be satisfied of the identity of the requester before they can provide any personal information (see Identity verification section).

Requests may be received from the following:

- **Competent patients**

  May apply for access to their own records or authorise third party access to their records.

- **Children and young people**

  May also apply in the same manner as other competent patients and Penn Surgery will not automatically presume a child or young person has capacity under the age of 16. However, those aged 13 or over are expected to have the capacity to consent to medical information being disclosed.[17]

  Note BMA guidance states the age is 12, although it is 13 with UK GDPR and also that age in the CQC GP Mythbuster 8: Gillick competency and Fraser guidelines.

[16] How to access your health records

[17] Access to health records

- **Parents**

  May apply to access their child's health record so long as it is not in contradiction of the wishes of the competent child. The child must not be older than 12yrs old. Access to Medications & appointments may be granted. Proxy form must be completed.

- **Individuals with a responsibility for adults who lack capacity**

  Are not automatically entitled to access the individual's health records. Penn Surgery will ensure that the patient's capacity is judged in relation to the particular decisions being made.

  Any consideration to nominate an authorised individual to make proxy decisions for an individual who lacks capacity will comply with the Mental Capacity Act 2005 in England and Wales and the Adults with Incapacity Act Scotland.

- **Next of kin**

  Have no rights of access to health records.

- **Police**

  In all cases, the organisation can release confidential information if the patient has given his/her consent (preferably in writing) and understands the consequences of making that decision. There is, however, no legal obligation to disclose information to the police unless there is a court order or this is required under statutes (e.g., Road Traffic Act 2006).

  Nevertheless, health professionals at Penn Surgery have a power under the Data Protection Act 2018 and Crime Disorder Act 1998 to release confidential health records without consent for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders. The release of the information must be necessary for the administration of justice and is only lawful if this is necessary:

    - To protect the patient or another person's vital interests, or

    - For the purposes of the prevention or detection of any unlawful act where seeking consent would prejudice those purposes and disclosure is in the substantial public interest (e.g., where the seriousness of the crime means there is a pressing social need for disclosure)

  Only information that is strictly relevant to a specific police investigation should be considered for release and only then if the police investigation would be seriously prejudiced or delayed without it. The police should be asked to provide written reasons why this information is relevant and essential for them to conclude their investigations.

- **Court representatives**

  A person appointed by the court to manage the affairs of a patient who is incapable of managing his or her own affairs may make an application. Access may be denied where the responsible clinician is of the opinion that the patient underwent relevant

examinations or investigations in the expectation that the information would not be disclosed to the applicant.

- **Patient representatives/solicitors**

  A patient can give written authorisation for a person (for example a solicitor or relative) to make an application on their behalf for copies of their medical records.

  This organisation may withhold access if it is of the view that the patient authorising the access has not understood the meaning of the authorisation. It is important to stress to the patient that under a SARs request all health records are provided, unless a specific time period is stated, and patients should be mindful of giving access to this level of health data.

  Solicitors who are acting in civil litigation cases for patients should obtain consent from the patient using the form that has been agreed with the BMA and the Law Society. If a consent form from the patient is not received with the application form then no information must be provided until this has been received.

- **Requests for insurance medical reports**

  SARs are not appropriate should an insurance company require health data to assess a claim. The correct process for this at Penn Surgery is for the insurer to use the Access to Medical Reports Act 1988 (AMRA) when requesting a GP report.

  In most cases, the requester will provide the patient's signed consent to release information held in their health record. The BMA have issued guidance on requests for medical information from insurers.

  Therefore, this organisation will contact the patient to explain the extent of disclosure sought by the third party. The organisation can then provide the patient with the medical record as opposed to the insurer. The patient is then given the opportunity to review their record and decide whether they are content to share the information with the insurance company.

  Penn Surgery] will advise insurers that the following fees are applicable:[18]

    - GP report for insurance applicants £104.00
    - GP supplementary report £50.00

It is the responsibility of the data controller to verify all requests from data subjects using reasonable measures.

The use of the organisation's SAR form supports the data controller in verifying the request. In addition, the data controller is permitted to ask for evidence to identify the data subject, usually by using photographic identification, i.e., driving licence or passport.

Further reading can be sought from BMA - Access to health records document that was updated to reflect the changes to reflect GDPR and DPA18.

[18] BMA Guidance Fees when providing insurance reports and certificates 12 August 2021

7.3 Processing a SAR request

Upon receipt of a SAR, Penn Surgery will record the SAR within the health record of the individual to whom it relates, as well as annotating the Data Subject Access Request (SAR) Register.

Furthermore, once processed, an entry onto the health record should be made, including the date of postage or the date the record was collected by the patient or authorised individual in addition to updating the SAR Register.

Under the Data Protection (Subject Access Modification) (Health) Order 2000, Penn Surgery will ensure that an appropriate healthcare professional (responsible clinician) manages all access matters. At Penn Surgery, there are a number of such professionals and, wherever possible, the individual most recently involved in the care of the patient will review and deal with the request. If for some reason they are unable to manage the request, an appropriate professional will assume responsibility and manage the access request.

Furthermore, to maintain UK GDPR compliance, the data controller at Penn Surgery will ensure that data is processed in accordance with Article 5 of the UK GDPR and will be able to demonstrate compliance with the regulation (see the organisation's UK GDPR policy for detailed information).

Data processors at Penn Surgery will ensure that the processing of personal data is lawful and at least one of the following applies:

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or another natural person

Individuals will have to verify their ID[19] at Penn Surgery and it is the responsibility of the data controller to verify all requests from data subjects using reasonable measures (see Identity verification section).

The process upon receipt of a SAR form is clearly illustrated at Annex C which is an aide-memoire/flow diagram for staff. A poster explaining how to access health records for use in waiting room areas can be found at Annex D.

7.4 Timeframe for responding to requests

[19] NHS England Patient Online Services in Primary Care Good Practice on Identity Verification

In accordance with the UK GDPR, patients are entitled to receive a response within the maximum given time frame of one calendar month from the date of submission of the SAR.

In order to ensure full compliance regarding SARs, this organisation will adhere to the guidance provided in the UK GDPR. In the case of complex or multiple requests, the data controller may extend the response time by a period of two months. In such instances, the applicant must be informed in the first month and the reasons for the extension given.

Should the request involve a large amount of information, the data controller will ask the data subject to specify what data they require before responding to the request. Data controllers are permitted to 'stop the clock' in relation to the response time until clarification is received.

Further reading can be found in the BMA document titled: Access to health records.

7.5 Fees

BMA advises that under the UK GDPR, Penn Surgery SARs are generally free of charge. Only if the SAR is considered to be 'manifestly unfounded' or 'excessive' can a 'reasonable' fee be charged although the circumstances when a fee can be charged are rare and should be on a case-by-case basis.

The ICO has advised that a request could be deemed as 'excessive' if an individual was to receive information via a SAR and then request a copy of the same information within a short period of time ie: within 12 months. In this scenario, the organisation could charge a reasonable fee or refuse the request.

Postage costs for SARs should not be charged for unless they are 'unfounded or excessive'.

Further reading can be found in the BMA document titled: Access to health records.

7.6 Method of response to requests

The decision on what format to provide the requested information in should take into consideration the circumstances of the request and whether the individual can access the data in the format provided.

Should an individual submit a SAR electronically, Penn Surgery will reply in the same format (unless the data subject states otherwise).

Where the patient/applicant requests their information to be emailed to them, it is strongly recommended that the organisation explains to the patient/applicant the risks (for example, unauthorised interception of the data) of receiving the data via unencrypted means to a non-NHS email address. The organisation should document the patient's agreement (expressed in writing or via email) to receive their data via unencrypted means in the medical record. If the patient/applicant agrees, a USB stick or a CD can be used as alternative electronic formats.
For those requests that are not made electronically, a paper copy can be provided unless the patient has explicitly requested a different format.

7.7 Amendments to medical records

Records should not be amended because of a request for access. Indeed, it is a criminal offence under the Data Protection Act 2018 to amend or delete records in response to a SAR. If amendments are made between the time that the request for access was received and the time at which the records were supplied, these must only be amendments that would have been made whether or not the request for access was made. When dealing with a SAR, the most up to date information should be provided.

Information that is clinically relevant must not be deleted from medical records (for electronic records, information can be removed from display, but the audit trail will always keep the record complete). Amendments to records can be made provided the amendments are made in a way that indicates why the alteration was made so that it is clear that records have not been tampered with for any underhand reason. Patients may also seek correction of information they believe is inaccurate (see Disputes concerning content of records section).

7.8 iGPR

When a request is received via iGPR, it should be processed in accordance with the organisation's iGPR protocol. iGPR will automatically find and redact items in a record that should not be included.

Additionally, to ensure all relevant attachments are included in the report (including any hard copies that are not within the patient's electronic healthcare record), the report should not be processed on iGPR until it is certain that the entire record has been scanned into the patient's record on EMIS. Once this has been confirmed, the request can be processed but the secretary/ admin processing the request must then assign the report to the responsible clinician who will review the report and confirm accuracy before agreeing the report can be sent using iGPR.

Further information, including training videos and infographics for iGPR, can be sought here.

7.9 Additional Privacy Information notice

Once the relevant information has been processed and is ready for issue to the patient, it is a requirement, in accordance with Article 15 of (UK GDPR), to provide an Additional Privacy Information notice (APIn), the template for which can be found at Annex E.

7.10 Organisation disclaimer

The template at Annex F is to be used when issuing patients with copies of their medical records. This outlines the fact that the patient is responsible for the security and confidentiality of their records once they leave the organisation and that the organisation will not accept any responsibility for copies of medical records once they leave the premises.

8 Refusal to comply with a request

Penn Surgery will only refuse to comply with a SAR where exemption applies or when the request is manifestly unfounded or manifestly excessive. In such situations, the data controller will inform the individual of:

- The reasons why the SAR was refused
- Their right to submit a complaint to the ICO
- Their ability to seek enforcement of this right through the courts

Each request must be given careful consideration and should Penn Surgery refuse to comply, this must be recorded and the reasons for refusal justifiable.
Being the data controller, Penn Surgery has the right to refuse any online access or SAR, although any such refusal will be within the allotted timescale and reasons for the refusal will be given.[20]

A letter template for refusal can be found at Annex G.

There are occasions when a GP may firmly believe that it is not appropriate to share all the information contained in the individual's record, particularly if there is potential for such information to cause harm or distress to individuals or when the record contains information relating to a third party. This information can be redacted from the patient's view but must not be deleted from the record (see non-disclosure section). If system functionality to redact information is not available, the record should not be shared with the patient.

Further reading can be sought from the GMC document titled When you can disclose personal information.

9 Coercion

The risks for coercion of patients with online access should always be borne in mind. Patients may be forced into sharing information from their record, including log-in details, medical history, repeat prescription orders, appointment booking details and other private, personal information. By gaining access to a person's record, an abuser may gain further control or escalate harm.

Organisations need to consider whether the organisation's policy on safeguarding should be updated to cover patient online services. Registering patients for online services requires awareness of the potential impact of coercion.

Coercion can happen to children, adults in an abusive relationship and elderly or otherwise vulnerable adults. Access to a patient's health record can be particularly attractive to an abusive partner, carer or parent.

At Penn Surgery all staff involved in registering patients for online services are aware of the potential impact of coercion and the signs to look out for in order to help patients who might be subject to coercion.

The Gov.uk webpage titled Domestic abuse: how to get help can support organisations who suspect that a patient is at risk of coercive control.

10 Non-disclosure

[20] ico.org.uk

The UK GDPR provides for a number of exemptions in respect of information falling within the scope of a SAR. In summary, information can generally 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
- 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 considering 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
- 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, in Scotland, 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 data controller reasonably concludes that confidentiality should prevail or it is restricted by order of the courts
- 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
- In the case of children's records, disclosure is prohibited by law, e.g., adoption records

The data controller must redact or block out any exempt information. Depending on the circumstances, it may be that the data controller should take steps to explain to the applicant how the relevant exemption has been applied. However, such steps should not be taken if, and insofar as they would in effect cut across the protections afforded by the exemptions. Indeed, 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 is 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 data controller, advice about serious harm must be taken by the data controller from the responsible clinician. If the data controller is not the responsible clinician, then the appropriate responsible clinician needs to be consulted 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 that are the subject of the request. If there is more than one, it should be the person most suitable to advise. If there is none, advice should be sought from another health professional who 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, the BMA recommends that the responsible clinician discusses the matter anonymously with an experienced colleague, their Data Protection Officer, the Caldicott Guardian or a defence body[21].

[21] BMA

11 Proxy access and third-party requests

11.1 Proxy access to medical records

A joint document from NHS E and RCGP titled What is Proxy Access? advises that this is when an individual other than the patient requests access to a patient'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.

Proxy access should not be granted where:

- The organisation suspects coercive behaviour (See Coercion section)
- 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 responsible clinician 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

Patients have the right to grant a carer, relative, responsible adult or partner access to their online services or copy of medical records. The patient can however limit which online services they want the nominated individual to access. Patients are to be advised that they should not share their own log-in details with anyone.

The nominated individual will be issued with separate log-in details to access the online services for their partner, relative or person they are caring for. To obtain proxy access, a person must be registered for online access at the organisation where the patient they are acting for is registered.

11.2 Proxy access in adults (including those over 13 years) 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.

See note in Section 11.4 in regard to age and competencies.

11.3 Proxy access in adults (including those over 13 Years) without capacity

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

- The patient has been assessed as lacking capacity to decide 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 decide 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 responsible clinician 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 responsible clinician to ensure that the level of access enabled, or information provided is necessary for the performance of the applicant's duties

11.4 Children and young people's access

It is difficult to say at what age the child will become competent to make autonomous decisions regarding their healthcare as between the ages of 11 and 16 this varies from person to person.

In accordance with Article 8 of the UK GDPR[22], from the age of 13 young people can provide their own consent and will be able to register for online services.

Note, this age is deemed to be 12 in the BMA document: Access to health records dated June 2020 although this should always be assessed by the clinician as to whether they are deemed competent.

The CQC GP Mythbuster 8: Gillick competency and Fraser guidelines details this further and states that *"there is no lower age limit for Gillick competence or Fraser guidelines to be applied. That said, it would rarely be appropriate or safe for a child less than 13 years of age to consent to treatment without a parent's involvement."*

- **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 above. Additional identification of parental/guardian evidence will be required.

  When the child reaches the age of 11, access to the parent/guardian will automatically cease. Subsequent proxy access will need to be authorised by the patient (subject to a competency test). In addition, parental proxy access may be reinstated if, after discussion with the parent(s) requesting access, the child's GP believes that proxy access would be in the child's best interest.[3]

- **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.

  The responsible clinician will invite the child for a confidential consultation to discuss the request for proxy access under the Data Protection Law.

[22] Article 8 UK GDPR

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

If the organisation suspects coercive behaviour, access will be refused and documented in the medical notes.

The nominated individual is to complete the online services registration form at Annex A or SARs application form at Annex B. Should the organisation opt not to grant the person access to an individual's record, the responsible clinician will contact the patient and advise them of the reasons why this decision has been reached.

The organisation may refuse or withdraw formal proxy access at any time if they judge that it is in the patient's best interests to do so. Formal proxy access may be restricted to less access than the patient has, e.g., appointments and repeat prescriptions only.

Patients who choose to share their account credentials with family, friends and carers (including a care home) must be advised of the risks associated with doing this. Formal proxy access is the recommended alternative in all circumstances.

- **Proxy access without consent**

The organisation may authorise proxy access without the patient's consent when:

  - The patient does not have capacity to make a decision on giving proxy access
  - The applicant has a lasting power of attorney (welfare)
  - The applicant is acting as a Court Appointed Deputy on behalf of the patient
  - The GP considers it to be in the patient's best interests

The person authorising access has responsibility to ensure that the level of access enabled is appropriate for the performance of the applicant's duties.

Further information on competency for children and young people can be sought in the organisation's Consent Policy.

11.5 Parents gaining access to a child's medical record

This organisation will allow parents access to their child's medical records if the child or young person consents, or lacks capacity, and it does not go against the child's best interests. However, if the records contain information given by the child or young person in confidence then this information should not normally be disclosed without their consent.

It should be noted that divorce or separation does not affect parental responsibility and therefore both parents will continue to have reasonable access to their children's health records unless legally advised not to do so.

Further reading on this subject can be sought in the GMC document titled Accessing medical records by children, young people and parents. Likewise, there are sections on both separated parents and parental responsibility within the Safeguarding Policy.

12 Identity verification

12.1 Requirement

Before access to health records is granted, the patient's identity and requestor's identity in cases of proxy access requests, 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 SARs will require formal identification through two 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 data controller or responsible clinician. 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.

12.2 Adult proxy access verification

Before the organisation 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 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

12.3 Child proxy access verification

Before the organisation 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.

12.4 How to set up a proxy access

Refer to the NHS Digital's Linked profiles and proxy access as this details each process on EMIS to allow parents, family members and carers to access health services on behalf of other people.

13 Deceased patients

13.1 Access to deceased persons medical records

The UK GDPR does not apply to data concerning deceased persons. However, the ethical obligation to respect a patient's confidentiality extends beyond death. There are a number of considerations to be taken into account prior to disclosing the health record of a deceased patient.

Such considerations are detailed in the Access to Health Records Act 1990. Unless the patient requested confidentiality while alive, under the terms of this Act Penn Surgery will only grant access to either:

- A personal representative (executor of the deceased person's estate); or
- Someone who has a claim resulting from the death

Under section 5(4) of the Access to Health Records Act 1990, no information that is not directly relevant to a claim should be disclosed to either the personal representative or any other person who may have a claim arising out of the patient's death.

The medical records of the deceased will be passed to Primary Care Support England (PCSE) for storage. PCSE will retain the GP records of deceased patients for 10 years after which time they will be destroyed. PCSE has provided an application form that can be used to request copies of a deceased patient's record.

However, should an applicant approach the organisation and where the organisation still holds an electronic copy of the deceased's record, the organisation is obliged to respond to the request under the Access to Health Records Act 1990.

Further detailed information is available within the Access to Deceased Patients Records Policy and Medical Protection Society article titled Disclosures after death dated 10 June 2020.

13.2 Chargeable fees for deceased patients

Legislative changes to the Data Protection Act 2018 have also amended the Access to Health Records Act 1990 which now states access to the records of deceased patients and any copies must be provided free of charge.[23]

However, where health information is to be disclosed for the deceased in the absence of a statutory basis, e.g., when a solicitor or insurance company requests a medical report or information to confirm death or an interpretation of what is in the records, this is classed as private work over and above what is already available in the record.

[23] BMA guidance - Access to health records - Nov 19

Any fees charged should be reasonable and proportionate to cover the cost of satisfying a request.

13.3 Chargeable fees for a Subject Access Request (SAR)

Should a SAR request be initiated from a solicitor and they are asking for a report to be written or the request is asking for an interpretation of information within the record this request goes beyond a SAR and therefore a fee can be charged. The organisation may ask the nature of the request from the solicitor to confirm if this should be charged for or not[24].

If the solicitor 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.

Fees are further detailed at Section 7.5.

14 Employee requests

Employees and ex-employees of the organisation have a right to request a copy of their personal data including employment record, occupational health records, complaints files, significant event files and any other relevant correspondence. Not all personal data that an organisation holds about an individual needs to be provided, as certain exemptions exist.

For example, legally privileged documents do not need to be disclosed or where personal data is processed for the purposes of management forecasting or management planning in relation to business planning.

It is also worth bearing in mind that whilst the ICO advises that employers should be prepared to take reasonable efforts to find and retrieve the requested information,they will not be required to act unreasonably or disproportionately regarding the importance of providing subject access[25].

The requestor does not need to provide a reason for making a SAR however they must state who they are and provide appropriate ID. The requestor should specify a date range, subject matter and the people who they believe have sent or received information about them.
An employer cannot refuse to supply information if documents provide third party references. These should simply be redacted on the copy provided to the requestor. Article 15(1) UK GDPR says that an employer must provide the information requested together with some additional information.

The additional information includes:

- The purpose for which the employer is processing the data
- Categories of the personal data being processed
- Who receives or has received the personal data from the employer
- How long the employer keeps personal data or the criteria used in deciding how long to keep the information

[24] BMA Guidance – Access to health records - June 21
[25] ICO - How do we find and retrieve the relevant information

- Information about where the employer got the personal information from if that information was not collected directly from the employee

- If the employer does cross-border data transfers, information about how data security is safeguarded

- Whether the employer uses automated decision-making and profiling. If so, the auto-decision logic used and what this means for the employee.

The procedure for employees or ex-employees undertaking a SARs request follows the same process as detailed in the section Procedure for Access.

Article 15(3) UK GDPR says that on receipt of a SAR, the employer must give the requestor a copy of their personal information without charge but can charge a reasonable fee for additional requests. If the request is made by e-mail then the employer must provide the information in a commonly used electronic format unless the requestor requires the information in a different format[26].

15 Denial or limitation of information

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

- The person'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.

16 Third party information

Patient and organisational 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 highlighted by the appropriate responsible clinician or data controller. If this is not possible then access to the information will be refused.

17 Former NHS patients living outside the UK

[26] Employeerescue.co.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, Penn Surgery may be prepared to provide a summary of the treatment given whilst resident in the UK.

18 Disputes concerning content of records

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

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

Any queries will be directed to the data controller who will contact the patient. They will investigate swiftly and thoroughly to identify the source and extent of the problem.

The responsible clinician and Caldicott Guardian/data controller 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 Caldicott Guardian or data controller should be consulted. If it is not possible to amend the records, a meeting with the patient or their proxy should be organised to explain why.

If a patient wishes to apply their UK GDPR rights of:

- Rectification (Article 16 UK GDPR)
- Erasure (Article 17 UK GDPR)
- Restriction of processing (Article 18 UK GDPR)
- Data portability (Article 20 UK GDPR)
- Right to object (Article 21 UK GDPR)

advice MUST be sought from the organisation's Data Protection Officer, Paul Couldrey Tel: 0115 838 6770 or 07477 052036

Where it is not appropriate to amend a medical record, an entry may be made declaring that the patient disagrees with the entry. If the patient further disputes the accuracy once a decision has been made, they will be referred to the complaint's procedure and/or the Health Ombudsmen.

MDU has written an article for GPOnline that further explains how to handle patients requests to change their medical records.

19 Complaints

Penn Surgery has procedures in place to enable complaints about access to health records requests to be addressed. Please refer to the organisation's Complaints procedure.

All complaints about access to records and SARs should be referred to the Practice Manager. If the issue remains unresolved, the patient should be informed that they have a right to make a complaint through the NHS complaints procedure in accordance with the NHS England document titled How to complain to the NHS.
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 organisation is not complying with their request in accordance with the Data Protection Act 2018.

Alternatively, the patient may wish to seek legal independent advice.

20 Care Quality Commission (CQC)

20.1 Access to medical records during an inspection

The CQC has powers under the Health and Social Care Act 2008 to access medical records to exercise their role and the Code of practice on accessing confidential and personal information describes its powers that permits accessing medical records.

During any inspection, the CQC inspecting team will look at a patient's medical records when it is both necessary, and intruding on that patient's privacy is justified, proportionate and will protect the privacy and dignity of patients. This is to assess the quality of care provided by the practice and not to assess the individual clinician.

Further guidance is given within GP Mythbuster 12: Accessing medical records during inspections where it is advised that confidentiality will be maintained of any patient's clinical record and that the inspecting team will always follow its code of practice.

20.2 Why the CQC looks at medical records

The CQC inspecting team will assess the quality of care against the key lines of enquiry (KLOEs) and corroborate their findings through any evidence that they may see within any medical record.

They look at this evidence alongside:

- Other evidence gathered on the inspection
- Information we have from our ongoing relationship management with the provider
- Information from the CQC Intelligence Model
- Information gathered before the inspection

As previously detailed, reviews are not designed to assess any individual clinician's ability although should any concerns be identified about an individual clinician then the inspector is duty bound to refer the clinician to their appropriate governing body such as GMC, NMC or HCPC.

20.3 Examples of what may be reviewed

The inspecting team will ensure that several areas are being appropriately considered by the clinical staff within this organisation. All searches have been agreed by the RCGP and the

BMA as they represent a reasonable approach to assessing some important features of safe and effective healthcare delivery.
CQC will scrutinise the following categories within the clinical system:

- Monitoring of patients being prescribed Disease Modifying Antirheumatic Drugs (DMARDs)
- High risk drug monitoring
- MHRA/CAS/drug safety update alerts
- Contraindications and combination drug alerts
- Potential missed diagnosis
- Medicines usage
- Do not attempt cardiopulmonary resuscitation (DNACPR) or ReSPECT forms
- Different types of appointments