# Patient access to online medical records

## 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.[[1]](#footnote-1)

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 soon – this will be announced in 2022 ‘

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.

## Registering for online services

GP online services are free and available to all registered patients. 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 able to make this request through <https://www.amershamvale.co.uk/application-for-online-access>

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 a photographic ID. Completed documentation will be reviewed by the responsible staff member 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

It takes approximately fourteen days to process any online service request.

# Summary Care Records (SCR)

## 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.

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

## 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.

## 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.

# Subject Access Request (SAR) to medical records

## Background

Patients have the right to access their data and any supplementary information held by Amersham Vale Practice.

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 patient wishes to access their data, they should fill in a form via https://www.amershamvale.co.uk/emr-consent-form-sar though it is to be noted that:

*“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.

## 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. Verbal requests should be documented and a clarification letter sent or a telephone call made to the patient for approval.

There is also be an electronic form for patients to complete if they prefer and this can be found <https://www.amershamvale.co.uk/emr-consent-form-sar>

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

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 Amersham Vale Practice 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.[[2]](#footnote-2)

* **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

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

Are not automatically entitled to access the individual’s health records. Amersham Vale Practice 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](https://www.legislation.gov.uk/ukpga/2005/9/contents) 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

Nevertheless, health professionals at Amersham Vale Practice have a power under the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) and [Crime Disorder Act 1998](https://www.legislation.gov.uk/ukpga/1998/37/section/116) 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 Amersham Vale Practice to put their request in writing and in in most cases, the requester will provide the patient’s signed consent to release information held in their health record.

The practice will contact the patient to explain the extent of disclosure sought by the third party. The practice 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.

Amersham Vale Practice will advise insurers that the following fees are applicable:

* GP report for insurance applicants £104.00\*
* GP supplementary report £27\*

\*subject to change without notice

The staff responsible for processing such requests 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 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

## Timeframe for responding to requests

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 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 practice will ask the patient to specify what data they require before responding to the request. The practice is permitted to ‘stop the clock’ in relation to the response time until clarification is received.

## Fees

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. 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'.

## 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](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) 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 section 13 – disputes concerning medical records).

## eMR – Medi2Data

When a request for a SAR has been received using the form on <https://www.amershamvale.co.uk/emr-consent-form-sar> or via any other method of request, as stated above.

We will send your request to a secure, NHS and ICO approved third party called eMR/Medi2Data.

ICO Registration Number: ZA353121

Please see <https://www.medi2data.com/keeping-data-safe/> to read their Information Governance and Data Protection Standards and how they process your data.

eMR/Medi2Data system will automatically find and redact items in your digital record that should not be included.

# Refusal to comply with a request

The practice 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 practice 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 the practice refuse to comply, this must be recorded and the reasons for refusal justifiable.

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.

# 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 Amersham Vale, 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.

# Non-disclosure

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 Practice must redact or block out any exempt information. Depending on the circumstances, it may be that the practice will 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 practice, 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 safeguarding lead or the clinician 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 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.

# Proxy access and third-party requests

## Proxy access to medical records

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
* 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.

## 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.

## 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](https://www.legislation.gov.uk/ukpga/2005/9/contents) 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

## 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[[3]](#footnote-3), from the age of 13 young people can provide their own consent and will be able to register for online services.

.The CQC [GP Mythbuster 8: Gillick competency and Fraser guidelines](https://www.cqc.org.uk/guidance-providers/gps/gp-mythbuster-8-gillick-competency-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 13, 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.

* **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.

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 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.

## 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.

# Identity verification

## 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 a form 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 a responsible person.

It is extremely important that the questions posed do not incidentally disclose confidential information to the applicant before their identity is verified.

## Adult proxy access verification

Before the 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

## 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.

# Deceased patients

## 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.

Unless the patient requested confidentiality while alive, under the terms of this Act, Amersham Vale 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 physical 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 that can be used to request copies of a deceased patient’s record and this can be found on their website.

However, should an applicant approach the practice and where the practice holds an electronic copy of the deceased’s record, we are obliged to respond to the request under the Access to Health Records Act 1990.

## 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[[4]](#footnote-4).

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.

# 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.

# 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.

# Former NHS patients living outside the UK

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

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

# 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.

In the first instance that a patient wishes to raise a dispute about their medical record; the patient must submit it in writing either writing to the practice, marking for attention of the practice manager, or via the contact-us submission form on the website <https://www.amershamvale.co.uk/contact-us-form>

Any queries will be directed to the practice 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 be sought from the organisation’s the Caldicott Guardian or data controller.

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.

# Complaints

Amersham Vale has procedures in place to enable complaints about access to health records requests to be addressed.

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](https://www.nhs.uk/using-the-nhs/about-the-nhs/how-to-complain-to-the-nhs/).

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

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. [↑](#footnote-ref-4)