ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

Please note: This document will continue to be updated as more clarity is given on GDPR's implementation

Introduction

In order to provide the right level of care, we are required to hold personal information about you on our computer systems and in paper records to help us to look after your health needs, and your doctor is responsible for their accuracy and safe-keeping. Please help to keep your record up to date by informing us of any changes to your circumstances.

Confidentiality and Personal Information

Doctors and staff in the practice have access to your medical records to enable them to do their jobs. From time to time information may be shared with others involved in your care if it is necessary. Anyone with access to your record if properly trained in confidentiality issues and is governed by both legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safe guards are in place to prevent accidentals loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other circumstance you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends or spouses unless we have prior written consent, and we do not, leave messages with others.

The Access to Health Records Act 1990 and the Access to Medical Reports Act 1988 gave individuals the right of access, subject to certain exceptions, to health information recorded about themselves, and, in certain circumstances, about others, within manual records.

The Access to Medical Reports Act 1988 covers the rights of individuals to access medical reports prepared about them for employment or insurance purposes.

The Data Protection Act (DPA) 1998 came into force in March 2000 and repealed most of the 1990 Access to Health Records Act. All applications for access to records, whether paper based or electronic, of living persons are now made under the Data Protection Act. The DPA was updated even further in 2018 to meet the General Data Protection Regulation.

Under the GDPA, patients have the right to apply for access to their health records. Provided that a written application is made the practice is obliged to comply with a request for access subject to certain exceptions. However, the practice also has a duty to maintain the

confidentiality of patient information and to satisfy itself that the applicant is entitled to have access before releasing information.

For deceased persons, applications are made under sections of the 1990 Access to Health Records Act, which has been retained. These sections provide the right of access to the health records of deceased individuals for their personal representative and others having a claim under the estate of the deceased.

APPLICATIONS

Children and Young People

England, Wales or Northern Ireland where children under 16 should demonstrate that they have the capacity to make these decisions. Where the child is considered to be capable, then their consent must be sought before access is given to a third party.

The law regards young people aged 16 or 17 to be adults in respect of their rights to confidentiality. Access can be refused by the health professional where they consider that the child does not have capacity to give consent / decline decisions.

Individuals with parental responsibility for an under 18 year old will have a right to request access to those medical records (Scotland under 16). Access may be granted if access is not contrary to the wishes of the competent child. Not all parents have parental responsibility. A person with parental responsibility is either:

- the birth mother, or
- the birth father (if married to the mother at the time of child's birth or subsequently) if both are on the birth certificate, or,
- an individual given parental responsibility by a court.

Parental responsibility is not lost on divorce. If parents have never been married only the mother has automatic parental responsibility, however the father may subsequently "acquire" it.

(This is not an exhaustive list but contains the most common circumstances – see the BMA link in **Resources** below).

If the appropriate health professional considers that a child patient is Gillick competent (i.e. has sufficient maturity and understanding to make decisions about disclosure of their records) then the child should be asked for his or her consent before disclosure is given to someone with parental responsibility.

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

If the child is not Gillick competent and there is more than one person with parental responsibility, each may independently exercise their right of access. Technically, if a child lives with, for example, its mother, and the father applies for access to the child's records, there is no "obligation" to inform the mother. In practical terms, however, this may not be possible and both parents should be made aware of access requests unless there is a good reason not to do so.

In all circumstances good practice dictates that a Gillick competent child should be encouraged to involve parents or other legal guardians in any treatment/disclosure decisions. The data controller may refuse access to the record where the information contained in it could cause serious harm to the patient or another person.

Where consent is identified as the lawful basis for processing personal data when offering an online service directly to a child, only children aged 13 or over are able provide their own consent. (This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).

Patient Representatives

A patient can give written authorisation for a person (for example a solicitor or relative) to make an application on their behalf. The practice may withhold access if it is of the view that the patient authorising the access has not understood the meaning of the authorisation.

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 GP 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.

Children and Family Court Advisory and Support Service (CAFCASS)

Where CAFCASS has been appointed to write a report to advise a judge in relation to child welfare issues, De Beauvoir Surgery would attempt to comply by providing factual information as requested.

Before records are disclosed, the patient or parent(s) consent (as set out above) should be obtained. If this is not possible, and in the absence of a court order, the practice will need to balance its duty of confidentiality against the need for disclosure without consent where this is necessary:

- to protect the vital interests of the patient or others, or
- to prevent or detect any unlawful act where disclosure is in the substantial public interest (e.g. serious crime), and
- because seeking consent would prejudice those purposes.

The relevant health professional should provide factual information and their response should be forwarded to a member of the Child Protection Team, who will approve the report.

Amendments to or Deletions from Records

GDPR gives individuals stronger rights to control their data, including the right to erasure, the right to rectification, the right to object to processing and the right to restrict processing. The practice will deal with each such request on its individual merits.

If a patient feels information recorded on their health record is incorrect then they should firstly make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. If this avenue is unsuccessful then they may pursue a complaint under the NHS Complaints procedure in an attempt to have the information corrected or erased. The patient has a right under the DPA to request that personal information contained within the medical records is rectified, blocked, erased or destroyed if this has been inaccurately recorded.

He or she may apply to the Information Commissioner but they could also apply for rectification through the courts. The GP practice, as the data controller, should take reasonable steps to ensure that the notes are accurate and if the patient believes these to be inaccurate, that this is noted in the records. Each situation will be decided upon the facts and the practice will not be taken to have contravened the DPA if those reasonable steps were taken. In the normal course of events, however, it is most likely that these issues will be resolved amicably.

Further information can be obtained from the Information Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone number 0303 123 1113 or 01625 545745.

ico.org.uk/about-the-ico/who-we-are/directions-head-office/

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

PROCESS
Online Access to Medical Records (England)

Since April 2014, practices have been obliged to give patients the opportunity to view online information equating to their Summary Care Record (SCR) as part of the 2014-2015 GP contract.

From March 31, 2016, it is a contractual obligation to give patients online access to coded information held in their medical records, including medication, allergies, illnesses, immunisations and test results. Patients will need to register online with the practice in order to gain access to this information.

Checks should be carried out to ascertain the patient's identity, see **Appendix A**. The following checks should be undertaken:

- Checking photo ID and proof of address, for example, a passport or driving licence and a bank statement or council tax statement
- If the patient has no ID but is well known to the surgery, a member of staff may be able to confirm their identity.
- If the patient has no ID and is not well known to the surgery, the ability to answer questions about the information in their GP record may confirm that the record is theirs.

GP software will be configured to offer all coded data by default, but GPs will be provided with the tools to withhold coded information where there is reference to a third party.

The practice has the option to offer comprehensive online patient records. There are circumstances where a GP may believe it is not in the best interests of the patient to share all information in the record, for example if it contains information about a third party, or could cause harm to their physical or mental health. GPs should be prepared to provide justification surrounding their reasoning in cases where they decline to share any information.

The practice is only expected to meet the above requirements for patient online access to their record when they have been provided with the GPSoC-approved and funded IT systems. Where systems are not yet available, the practice will publish a statement of intent to provide this facility.

Proxy Access

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

Proxy Access refers to giving a third party access to online services on behalf of a patient. Family members or carers can access a patient's medical records online only in circumstances where the patient has consented to this, **or** if the patient lacks capacity AND the applicant can provide evidence that they have been granted the power to manage the patient's affairs.

Patients will be advised about the risks associated with doing this as part of their access application. Proxy access is the recommended alternative to sharing login details.
A person with parental responsibility who wishes to access some or all of the records of a competent child aged between 11 and 16 should only be allowed to do so if the child or young person consents, and it does not go against the child's best interests. If the records contain information given by the child or young person in confidence you should not normally disclose the information without their consent. For further information about Parental Responsibility, please see the **Children and Young People** section, found above.

A person with parental responsibility for a child aged under 12 normally has automatic rights to access a child's records - although not all parents have parental responsibility. Proxy access for people with parental responsibility to a child's record is a practice-level decision.

Coercion

The availability of online services carries the risks of users being subject to coercion, as patients could be vulnerable to being forced into sharing confidential information from their record against their will. In cases where this is believed to be a possibility, online access to medical records can be denied. This should be discussed privately with the patient before a final decision over whether to deny access is taken.

As part of their request to access their medical records online or allow proxy access to a third party, the person submitting the request should provide a statement confirming that they have not been coerced into doing so.

Online Access to Medical Records (Scotland and Wales)

Both Scotland and Wales have plans to make medical records online in the next five years. In Wales, patients between 11 and 16 who request online access to their medical records will be granted this **if** they are deemed to be Gillick competent.

In Scotland, there is a legal assumption that children over the age of 12 have the capacity to give or withhold consent to release medical records. For further information, please see the **Children and Young People** section, found above.

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

Applications for Access to Medical Records

GP practices receive applications for access to records via a number of different sources, for example:

Patients' solicitors
Patients & relatives
Patient Carers
Parents of patients under 16 years old

Requests should be in writing, with a patient signature. Email requests are valid for the purposes of the DPA, however the practice will need to be satisfied that the request is made by the data subject or their legal representative only. Where a solicitor or other representative is making the request, ensure that you have patient-signed consent and sufficient information to clearly identify the patient.

Notification of requests

Practices should treat all requests as potential claims for negligence. Good working practice would be to keep a central record of all requests in order to ensure that requests are cross-referenced with any complaints or incidents and that the deadlines for response are monitored and adhered to.

Requirement to consult appropriate health professional

It is the GP's responsibility to consider an access request and to disclose the records if the correct procedure has been followed. Before the practice discloses or provides copies of medical records the patient's GP must have been consulted and he / she checked the records and authorised the release, or part-release.

Grounds for refusing disclosure to health records

The GP should refuse to disclose <u>all or part</u> of the health record if he / she are of the view that:

- disclosure would be likely to cause serious harm to the physical or mental health of the patient or any other person;
- the records refer to another individual who can be identified from that information (apart from a health professional). This is unless that other individual's consent is obtained or the records can be anonymised or it is reasonable in all the circumstances to comply with the

request without that individual's consent, taking into account any duty of confidentiality owed to the third party; or if:

- the request is being made for a child's records by someone with parental responsibility or for an incapacitated person's record by someone with power to manage their affairs, and the:

i information was given by the patient in the expectation that it would not be disclosed to the person making the request, or

ii the patient has expressly indicated it should not be disclosed to that person.

Informing of the decision not to disclose

If a decision is taken that the record should not be disclosed, a letter must be sent by recorded delivery to the patient or their representative stating that disclosure would be likely to cause serious harm to the physical or mental health of the patient, or to any other person. The general position is that the practice should inform the patient if records are to be withheld on the above basis. However, the GP could decide not to inform the patient if the appropriate health professional thinks that telling the patient:

- will effectively amount to divulging that information, or;
- this is likely to cause serious physical or mental harm to the patient or another individual

In either of these cases, an explanatory note should be made in the file. GPs should be prepared to provide justification surrounding their reasoning in cases where they decline to share any information.

The decision can only be taken by the GP and an explanatory note should be made in the file. It is the practice's policy to give a patient the opportunity to have their case investigated by invoking the complaints procedure. The patient must be informed in writing that assistance will be offered to them if they wish to do this. In addition, the patient may complain to the Information Commissioner for an independent ruling on whether non-disclosure is proper.

Disclosure of the record

Once the appropriate documentation has been received and sufficient identification has been produced to satisfy the data controller that disclosure may be made, disclosure may be approved, the copy of the health record may be sent to the patient or their representative in a sealed envelope by recorded delivery. The record should be sent to a named individual, marked confidential, for addressee only and the sender's name should be written on the reverse of the envelope. Originals should not be sent. It may be good practice to check with the patient that all of the information requested is needed, before fulfilling the request,

although there is no requirement under the Act to specify the extent of the requested information as part of the application procedure.

Where viewing is requested, a date may be set for the patient to view by supervised appointment. Where parts of the record are not to be released or to be viewed (i.e. they are restricted) an explanation does not have to be given, however the reasons for withholding should be documented. GPs should be prepared to provide justification surrounding their reasoning in cases where they decline to share any information.

An explanation of terminology, abbreviation etc. must be given if requested. It is good practice for viewings to be supervised by a clinician (e.g. a nurse) who can explain items if needed. Where a non-clinician (e.g. receptionist) does this then no explanation must be offered. Explanation requests should be then referred to a clinical staff member.

Confidential information should not be sent by fax and never by email unless via an encrypted service such as from one NHS Mail account to another NHS Mail account.

A note should be made in the file of what has been disclosed to whom and on what grounds. Where information is not readily intelligible an explanation (e.g. of abbreviations or medical terminology) must be given.

Where an access request has been fulfilled, a subsequent identical or similar request does not have to be again fulfilled unless a “reasonable” time interval has elapsed.

Appropriate health professional

The Data Protection (Subject Access Modification) (Health) Order 2000 specifies the appropriate health professional to deal with access matters is:

- the current or most recent responsible professional involved in the clinical care of the patient in connection with the information aspects which are the subject of the request, or;
- where there is more than one such professional, the most suitable is to advise on the information which is the subject of the request.

Safe Haven

Confidential medical records should not be sent by fax unless there is no alternative. If a fax must be sent, it should include the minimum information and names should be removed and telephoned through separately.

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

All staff should be aware that safe haven procedures apply to the sending of confidential information by fax, for whatever reason. That is, the intended recipient must be alerted to the fact that confidential information is being sent. The recipient then makes a return telephone call to confirm safe and complete receipt. A suitable disclaimer, advising any unintentional recipient to contact the sender and to either send back or destroy the document, must accompany all such faxes. A suitable disclaimer is shown below:

***Warning**: The information in this fax is confidential and may be subject to legal professional privilege. It is intended solely for the attention and use of the named addressee(s). If you are not the intended recipient, please notify the sender immediately. Unless you are the intended recipient or his/her representative you are not authorised to, and must not, read, copy distribute, use or retain this message or any part of it.*

Patients living abroad

For former patients living outside of the UK and whom once had treatment for their stay here, under the DPA they still have the same rights to apply for access to their UK health records. Such a request should be dealt with as someone making an access request from within the UK. Original records should not be given to a patient to take outside the UK. The GP may agree to provide a summary, or otherwise the request is subject to a normal access request under these provisions.

Requests made by telephone

No patient information may be disclosed to members of the public by telephone. However, it is sometimes necessary to give patient information to another NHS employee over the telephone. Before doing so, the identity of the person requesting the information must be confirmed. This may best be achieved by telephoning the person's official office and asking to be put through to their extension. Requests from patients must be made in writing.

Requests made by the police

In all cases the practice 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 statute (e.g. Road Traffic Act).

The practice does, however, have a power under the DPA and Crime Disorder Act 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 persons 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 which 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.

Requests for Insurance Purposes

Insurance companies may seek to obtain full medical records through the use of Subject Access Requests (SAR) under the Data Protection Act. After seeking clarification from ICO, the BMA advises that upon receiving a SAR from an insurance company, practices should contact the patient to explain the implications of such a request and the extent of the disclosure. The ICO is also clear that GPs should provide the SAR information to the patient themselves, rather than directly to the insurance company.

The ICO's Subject Access Code of Practice states that 'If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.'

It is however expected that insurance companies will stop requesting SARs and revert to requesting medical reports. Practices are able to apply a fee for completion of these reports, in line with the work associated, and should seek to agree the fee with the requestor in advance of completion.

Requests from Third Parties for Non-Insurance Purposes

Under the Data Protection Act, individuals are entitled to make a SAR via a third party, such as solicitors who are acting in civil litigation cases for patients. These parties should obtain consent from the patient using the form that has been agreed with the BMA and the Law Society:

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

Consent form (England & Wales)
(copy and paste the below URL into your internet browser bar)

https://www.bma.org.uk/-/media/files/pdfs/employment%20advice/ethics/bmalawsocietyconsentformmarch2017.pdf?la=en

The ICO Code of Practice states that 'In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney'.

Court Proceedings

You may be ordered by a court of law to disclose all or part of the health record if it is relevant to a court case (for example by a Guardian ad litem).

Resources

Subject Access Request Policy
Data Protection Policy

APPENDIX A - VERIFYING PATIENTS' IDENTIFICATION

The practice's Access Management Lead –Practice Manager, is responsible for appointing people to roles and identity verification issues.

A patient must be registered with the practice to apply for access to any or all online services.

IDENTIFICATION ISSUE	NAME & POSITION
The following staff may vouch for patients' identities:	
The following listed staff may verify patients' identities dependent on the presentation of documents:	

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

The following listed staff may register patients for online access on the practice system, thereby enabling the booking of appointments, the ordering of repeat prescriptions and access to medical records:	
The following listed staff may take the lead on issues of proxy access and any issues related to third parties wishing to gain the authority to represent patients:	
The following listed staff may provide an initial point of contact for any queries re: identity verification:	

APPLICATION FOR ACCESS TO MEDICAL RECORDS
Data Protection Act 1998 Subject Access Request

Details of the Record to be accessed:

Patient Surname	NHS Number
Forename(s)	Address
Date of Birth	

Details of the Person who wishes to access the records, if different to above:

Surname	
Forename(s)	
Address	
Telephone Number	
Relationship to Patient	

Tick whichever of the following statements apply.

ACCESS TO MEDICAL RECORDS AND DATA PROTECTION

- I am the patient.
- I am the patients parent (Mother /Father
- I have been asked to act by the patient and attach the patient's written authorisation.

- I am acting in Loco Parentis and the patient is under age sixteen, and is incapable of understanding the request / has consented to me making this request.
  (*delete as appropriate).

- I have a claim arising from the patient's death and wish to access information relevant to my claim on the grounds that (please supply your reasons below).

Applicant signature.....Date……..

Details of Application

Patient to complete (please tick as appropriate)

I am applying for access to view my records only	
I am applying for copies of my medical record	
I have instructed someone else to apply on my behalf	
I have attached the appropriate fee	

Notes:

Under the Data Protection Act 1998 you do not have to give a reason for applying for access to your health records.

Under the Access to Health Records Act you will/will not need to give reasons for applying for access to a deceased person's health records.

You may be asked to provide photographic identification.

Optional - Please use this space below to inform us of certain periods and parts of your health record you may require, or provide more information as requested above.

This may include specific dates, consultant name and location, and parts of the records you require e.g. written diagnosis and reports. Note: defining the specific records you need may result in lower fee charges and a quicker response.

I would like a copy of all records	
I would like a copy of records between specific dates only (please give date range) below	
I would like copy records relating to a specific condition / specific incident only (please detail below)	