

**Blaenavon Medical Practice
Middle Coed Cae Road
Blaenavon
Torfaen
NP4 9AW**

Tel 01495 796360 Fax 01495 360663

**ACCESS TO HEALTH RECORDS
POLICY
for
GP PRACTICES**

*(under the Data Protection Act (DPA) 1998 and the Access to
Health Records Act 1990)*

ACCESS TO HEALTH RECORDS POLICY

Purpose and Scope

To ensure that good security controls and procedures are maintained for all information created, stored and processed by the Practice, and in particular that compliance with Data Protection legislation is observed.

These procedures apply to all employees, temporary staff, volunteers, contractors and other users accessing any of the Practice information systems, wherever the user or system may be situated.

Data Protection Act Registration and Notification

The Lead Partner will nominate a Data Protection Officer (usually the Security Manager) to handle day-to-day matters relating to the Data Protection Act.

The Data Protection Officer will:

- Review the Practice's Data Protection Act Registration details at least annually and ensure there have been no changes or additional uses and purposes introduced into working practices.
- Monitor any disclosures of personal information, particularly without the consent of the patient, to ensure there is a legitimate basis for the disclosure in line with the notification or relevant exemption.
- Produce a Patient Information leaflet that informs patients how their information is used, who may have access to that information, and details their own rights to see and obtain copies of their records.
- Ensure that personal data is not transferred to any country outside of the EEA, unless adequate levels of protection are in place.
- Ensure the annual notification is renewed annually via the Information Commissioner's Website: www.ico.org.uk
- The Lead Partner must 'sign-off' the Data Protection notification.

The Caldicott Guardian

The role of Caldicott Guardian will usually be the Lead Partner and will be responsible for safeguarding the confidentiality of patient related information and will ensure that all staff are aware that they must be consulted before any such information is shared with a third party.

Data Quality

The Lead Partner must ensure that:

- All data held is accurate and up-to-date, the minimum necessary and relevant to the purpose.
- Audits are undertaken or data quality assurance tools are utilised on a regular basis.

Information Sharing Protocols

All staff must ensure that the Caldicott Guardian is consulted before any patient identifiable information is shared with any third parties. This is to ensure that the transfer is justified and essential, and that only the minimum amount of information is transferred in each case.

The Caldicott Guardian:

Must ensure that where personal information is shared within NHS Wales for the direct benefit of a patient that this complies with the Wales Intra-NHS Sharing Agreement.

In conjunction with the Data Protection Officer the Security Manager:

- Will ensure that patient identifiable information sharing takes place in accordance with the standards set out in the 'Confidentiality: Code of Practice for Health and Social Care in Wales' (WAG August 2005) and the sharing with organisations not part of NHS Wales are documented in an Information Sharing Protocol.
- Will use the Wales Accord for the Sharing of Personal Information (WASPI) as the basis for sharing patient identifiable information with third parties and will ensure the Head of Practice signs the Declaration of Acceptance on behalf of the practice and requires any third party to do the same.
- Will be responsible for the production of an Information Sharing Protocol (PISP) and supporting documentation as detailed in WASPI Guidance.
- Must ensure that ONLY the minimum amount of patient identifiable information necessary for the intended purpose is shared and that the information is securely transferred.
- Must ensure a mechanism is in place to ensure that any decision taken by a patient to restrict disclosure of their personal information is appropriately respected.

The Security Manager must:

Record any information exchange process in the Information Assets Register and update this if the processes change.

Background

The Access to Health Records Act 1990 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 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 DPA 1998. For deceased persons, applications are made under sections of the 1990 Access to Health Records Act which have 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.

The Right of Access

Under section seven of the DPA, patients have the right to apply for access to their health records. Provided that the fee has been paid and a written application is made by one of the individuals referred to below, the Practice is obliged to comply with a request for access subject to certain exceptions (see the procedure in section 2). 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.

Applications

An application for access to health records may be made in any of the circumstances explained below.

The Patient

Blaenavon Medical Practice has a policy of openness with regard to health records and health professionals are encouraged to allow patients to access their health records on an informal basis. This should be recorded in the health record itself. The Department of Health's Code of Practice on Openness in the NHS as referred to in HSG (96) 18 Protection and Use of Patient Information will still apply to informal requests.

Such requests are usually made for a reason. The patient may have concerns about treatment that they have received, how they have been dealt with or may be worried that something they have said has been mis-interpreted. Staff are encouraged to try to understand and allay any underlying concerns that may have contributed to the request being made and offer an opportunity of early resolution.

Parental Responsibility

"Children of 16 years or Over"

If a mentally competent child is 16 years or over then they are entitled to request or refuse access to their records. If any other individual requests access to these the Practice should first check with the patient that he or she is happy for them to be released.

"Children Under 16 Years"

Individuals with parental responsibility for an under 16 year old will have a right to request access to those medical records. A person with parental responsibility is either:

- i the birth mother; or
- ii the birth father (if married to the mother at the time of child's birth or subsequently) or;
- iii an individual given parental responsibility by a court.

(This is not an exhaustive list but contains the most common circumstances).

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.

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. Again medical records should not be disclosed unless the process set out in Section 2 is adhered to.

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. Records should not be disclosed unless the process set out in Section 2 is adhered to.

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.

Access to a Deceased Patient's Medical Records

Where the patient has died, the patient's personal representative or any person who may have a claim arising out of the patient's death may make an application. Access shall not be given (even to the personal representative) to any part of the record which, in the GP's opinion, would disclose information which is not relevant to any claim which may arise out of the patient's death. The effect of this is that those requesting a deceased person's records should be asked to confirm the nature of the claim which they say they may have arising out of the person's death. If the person requesting the records was not the deceased's spouse or parent (where the deceased was unmarried) and if they were not a dependant of the deceased, it is unlikely that they will have a claim arising out of the death. All requests for a deceased patient's medical record are now handled by the PSS, Pontypool. All requests are to be forwarded to them for consideration.

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, Blaenavon Medical Practice would attempt to comply by providing factual information as requested.

Before records are disclosed, the patient or parents 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:

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

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

Chapter 8 Review

All Chapter 8 Review requests for information should be immediately directed to the PCT Child Protection Manager who will co-ordinate the Chapter 8 Review in accordance with national and local Area Child Protection Committee Guidance.

PROCESS

GP Practices receives applications for access to records via a number of different departments.

Medical Insurance Companies
Patient's solicitors
Patients
Patient Carers
Parents of under 16 year old patients

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.

Inspecting and withholding of records

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 medical records the patient's GP must have been consulted and he / she checked the records.

Grounds for refusing disclosure to health records

The GP should refuse to disclose all or part of the health record if the he / she is 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. If however, the appropriate health professional thinks that telling the patient:

- i will effectively amount to divulging that information; or this

ii is likely to cause serious physical or mental harm to the patient or another individual

then the GP could decide not to inform the patient, in which case an explanatory note should be made in the file.

That decision can only be taken by the GP and an explanatory note should be made in the file. Although there is no right of appeal to such a decision, 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 every 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 disclosure 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. ***Confidential information should not be sent by fax and never by email unless via an encrypted service such as 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.

Charges and Timescales

For patients currently undergoing care or whose records were updated within the last 40 days, it is assumed such records are more readily available and a response within 21 days from receipt of the written request is required. In respect of patients whose care is completed and whose records have not been updated in the last 40 days, 40 days is allowed from receipt of the written request.

Where further information is required by the Practice to enable it to identify the record required or validate the request, this must be requested within 14 days of receipt of the application and the timescale for responding begins on receipt of the full information.

To provide copies of electronic patient health records a maximum charge of £10 can be requested to cover photocopying. For manual records or a mixture of electronic and manual there can be a maximum charge of £50. No fee can be charged for allowing a patient to directly inspect their record where no copy is requested. The Practice is not required to provide all the information requested if this would involve disproportionate effort and can refuse to provide copies if no fee is paid. At the same time, however, the GP has discretion not to charge for copies should it choose to do so.

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.

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 1998 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.

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 made by the police

In all cases the GP Practice can release confidential information if the patient has given their 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:

- i to protect the patient or another person's vital interests; or
- ii 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 from Solicitors

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. A spreadsheet is kept noting all requests and dates records were sent.

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).

Amendments to or deletions from records

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 Commissioner at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone number 01625 545700.

**Data Protection Act – Request for Copies of
My Medical Records**

Please make sure you use your formal name in this section			
Mr Mrs Ms Dr	Other	Surname	
First Name			Other Initials
Second Name			
Address			
Post Code			
Date of Birth			
Telephone Number			
Section 1 – Accident/Event			
1.	Please provide me with copies of information about the following accident/event		
Section 2 – Medical Records			
2.	Please provide me with copies of my medical records for the following period		
From:		To:	
Section 3 – Signature			
Signed		Date	
Please send completed form to: (Insert Practice Address or Stamp)			
For Practice Use ONLY			
Action	Signed	Date	
Data Extracted			
Data Checked			
Data Sent to Patient			

Review	Date	For Review
Alterations made to Partners names	August 2011	
Information added about deceased patients records and the involvement of the PSS at Pontypool	August 2011	August 2012
Alterations made to Partners names.	October 2012	October 2013
MP. Practice name changed	November 2014	November 2016
MP – No changes	February 2017	November 2018