Data Security and Protection Advisory Team

LITTLEDOWN SURGERY

SUBJECT ACCESS POLICY

1. Introduction

1.1 Article 15 of the General Data Protection Regulation (GDPR) provides living individuals with the right to obtain confirmation that we are processing their personal data, a copy of their personal data from us, as well as other supplementary information. This right of access is commonly referred to as subject access.

1.2 The supplementary information that data subjects have a right to receive includes the following:

- the purposes of the processing;
- categories of personal data processed;
- the recipients or categories of recipients of the information;
- the retention period for storing the personal data or, where this is not possible, the criteria for determining how long the information will be stored;
- the right to request rectification, erasure or restriction or to object to processing;
- the right to complain to the Information Commissioner's Office (ICO) or another supervisory authority;
- the sources of the data if it wasn't obtained directly from the individual;
- the existence of, and reasoning behind any automated decision-making (including profiling); and
- the safeguards provided if the information is transferred to a third country or international organisation.

1.3 This information is included within the Practice's Privacy Notice, available on the Practice website, and as a print-out provided to data subjects.

1.4 An individual is only entitled to their own personal information, and not to information about other people (unless they have the authority to act on behalf of someone else).

2. Subject Access Requests

2.1 An individual can make a subject access request (SAR) to anyone in the Practice, either verbally or in writing (including by email and social media). All staff are expected to recognise a request for access to information.

2.2 The request does not have to include the phrase 'subject access request' or mention the Data Protection Act or the GDPR, it just needs to be clear that the individual is

asking us for their own personal data. Individuals do not need to tell us their reason for making the request, or what they intend to do with the information.

2.3 Occasionally a request may mistakenly state that it is a Freedom of Information request. If the request relates to the requester's personal data, staff must treat it as a SAR.

2.4 Where necessary, staff may wish to check with the requester that we have understood their request to avoid later disputes about how the request has been interpreted.

2.5 The practice has a subject access form (see Appendix One) to enable requests to be made efficiently however, it is not compulsory to use the form in order to obtain access to records.

2.6 Any request for access to personal information should be forwarded to the Practice Manager

2.7 Any request for access to staff records from an employee must be made to the Practice Manager

2.8 SARs will be recorded on a database to monitor compliance with requests and the statutory timescales.

Who can make a request?

2.9 A request can be made by:

- an individual (for access to their own personal data);
- a third party authorised in writing to make an application on an individual's behalf i.e. a solicitor, or someone else that the individual feels comfortable allowing to act for them e.g. a relative, carer or friend;
- a person appointed by the Court when an individual does not have capacity to manage their own affairs.

2.10 Where the request is made by a third party, we must be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this such as written authority to make the request, lasting power of attorney, Disclosure Order from the Family Proceedings Court or a Court of Protection Order.

2.11 An individual does not have the right to access information we hold about someone else unless they are an authorised representative, have parental responsibility, or are acting on behalf of a deceased person.

2.12 When the individual is a child, it is the child who has a right of access to information held about them even though, in the case of young children, these rights are likely to be exercised by those with parental authority. Care should be taken for requests made by parents for a child between the age of 13-16, as the child's rights should be upheld first. When a child reaches the age of 16 onwards, competence to decide who can access their data should be assumed.

Individuals living abroad

2.13 Individuals who now live outside of the UK still have the right to apply for access to their former UK health records. Such a request should be dealt with in the same way as someone making a SAR from within the UK.

2.14 Original records should not be given to individuals to keep or take outside of the UK. However, they are entitled to request a copy which they may take with them.

Response time

2.15 The practice must comply with a SAR without undue delay and at the latest within one month of receipt of the request or within one month of receipt of any information requested to confirm the requester's identity.

2.16 The time limit should be calculated from the day we receive the request, or other requested information (whether it is a working day or not) until the corresponding calendar date in the next month i.e. if we receive a request (or other requested ID) on the 2 January, we have until the 2 February to respond to the request.

2.17 If the following month is shorter and there is no corresponding calendar date, the date for the response is the last day of the following month.

2.18 If the corresponding date falls on a weekend or a bank holiday, we have until the next working day to respond.

2.19 The response time can be extended by a further two months if necessary where the request is complex (e.g. we have technical difficulties in retrieving the information, or we are clarifying potential issues around disclosure of information about a child to a legal guardian), or we have received a number of requests from the individual (e.g. if the individual has made a SAR, a request for erasure and a request for data portability all at the same time).

2.20 If we decide that it is necessary to extend the time limit by two months, we must let the individual know as soon as possible and within one month of receiving their request, explaining why. This will be done by the Practice Manager.

Charging of fees

2.21 Generally, we cannot charge a fee to comply with a SAR, the information should be provided free of charge to the data subject.

2.22 However, if further copies of the same information are requested, a 'reasonable fee' can be charged based on the administrative costs of providing further copies. These costs should be explained to the individual.

2.23 We can also charge a 'reasonable fee' if the request is manifestly unfounded or excessive (refer to ICO Guidance on Right of Access for further information).

2.24 Administrative costs should be based on charges for photocopying and printing of the records, and postage. We cannot charge for the time taken to deal with the request.

Identification checks

2.25 In order to confirm the identity of the person making the SAR (or the person the request is made on behalf of), we can ask for identification before responding to the request. We should only ask for enough information to determine whether the requester (or the person the request is made on behalf of) is the person that the data is about. We must be reasonable about what we ask for and should not request more information if the identity of the requester is obvious to us.

2.26 If the requester is applying for records on behalf of an individual, they must also include the individual's written authorisation for access to their records.

2.27 The level of checks we deem appropriate may depend on the possible harm and distress that inappropriate disclosure of the information could cause to the individual concerned.

2.28 We should request ID documents promptly. The timescale for responding to the SAR does not begin until we have received the requested ID documentation.

Refusing to comply with the request

2.29 There are limited circumstances in which we may determine that all or some of the information cannot be provided to an individual who has made a SAR.

2.30 These circumstances include:

- in the opinion of the relevant clinical professional, the information to be disclosed would likely cause serious harm to the physical or mental health or condition of the applicant or any other person, and they do not already know that information (see Section 3 serious harm redactions);

- where the record relates to, or has been provided by, an identifiable third party, unless the third party has consented to disclosure (see Section 3 third party redactions);
- where the granting of access to a patient's representative would disclose information provided by the individual, in the expectation that it would not be disclosed to the person making the request;
- the individual has expressly indicated that such information should not be disclosed to another individual;
- where disclosure is restricted by order of the courts;
- when disclosure may hamper the prevention or detection of serious crime;
- where there are child protection concerns or where releasing information may put a child or young person at risk, or where disclosure is prohibited by law e.g. adoption records;
- where the record relates to the keeping or using of gametes or embryos or is about an individual being born as a result of in vitro fertilisation;
- where requests are manifestly unfounded or excessive, in particular because they are repetitive. In these instances, the Practice can refuse to deal with the request or charge a 'reasonable fee' to deal with the request.

2.31 Where the Practice refuses to respond to a manifestly unfounded or excessive request, an explanation must be provided to the patient/representative, informing them of their right to complain to the ICO or another supervisory authority and their right to seek a judicial remedy without undue delay and at the latest within one month.

3. Processing of Subject Access Requests

3.1 Data subjects have the right to request access to their information in a specific format. Unless otherwise specified, requests should be responded to in the same format that they were made.

3.2 Where a request for information is made electronically (e.g. by email or via social media), we should provide the information in a commonly used electronic format unless the requester makes a reasonable request for us to provide it in another commonly used format (electronic or otherwise). We will not provide personal information via social media channels.

3.3 If the request is submitted by other means (e.g. by letter or verbally), we can provide the information in any commonly used format (electronic or otherwise), unless the requester makes a reasonable request for the information to be provided in another commonly used format.

3.4 Where we are using email to send copies of records to a patient, we should explain the risks of using this method to the patient i.e. unauthorised interception of the data, and we should document the patient's agreement to receive thee data in this way.

3.5 It is our responsibility to provide the information to the individual or their appointed representative – an individual should not have to take action to receive the information (e.g. by collecting it from the Practice), but we can request that they collect information if they are willing to do so.

3.6 Where the patient requests a specific format which cannot be complied with, or where a request is made in paper but the information is only available electronically, the patient should be contacted and the format for the response agreed within the one-month timeframe.

Online access

3.7 The GDPR encourages controllers to provide individuals with remote access to their personal data via a secure system.

3.8 Although a patient with SystmOne online access can view their health record, there is no facility to download the record, and therefore this does not satisfy the requirement to provide a copy. However, when we receive a subject access request from a patient, we should contact them to ask whether online access to view the record meets their requirements. If this is the case, then it will not be necessary to provide a full copy.

Collating the records

3.10 Once a request has been received, the health record or electronic information should be located and copied.

What should be included?

3.14 Hospital letters such as a referral letter, a discharge summary or a clinic outcome letter following a visit to the hospital are sent directly to the GP for inclusion in the patient record and, as such, they form part of the record and should be disclosed – there is no need to redact them.

3.15 Information entered into a patient record by staff at other units such as Health Visitors or School Nurses at Dorset Healthcare, is shared with GP Practices to enable clinical staff to see the full picture when assessing a patient. However, Dorset Healthcare (or the relevant unit) remains the organisation responsible for releasing these entries when a subject access request is made. This information can be excluded in SystmOne from a subject access request by ticking the option to 'exclude consultations owned by other Units'.

Safeguarding information held within a record

3.16 If the safeguarding information held in the record is about the patient themselves, and the patient is aware of what has been documented in the record then it would be reasonable to expect the information to be disclosed as part of the subject access request. However, we do need to be mindful of family circumstances and should consider whether coercion is taking place, particularly where there are known cases of domestic abuse. If staff are unsure about releasing the information then we should err on the side of caution and check with the patient's GP, Caldicott Guardian or the Data Protection Officer before making the decision to disclose.

3.17 If the patient has mental health issues, then again check with the patient's GP, Caldicott Guardian or the Data Protection Officer before disclosing any information. We should always consider whether the information we are intending to disclose is relevant and proportionate.

3.18 It is particularly important to review the notes before release, to ensure that there is not any information about another person such as a family member mentioned in notes that may need redacting, such as historic PPN, MARAC or MASH reports which mention multiple parties. It is now recommended that we copy any relevant information from such reports, including the dates and type of report, into the patient's record and dispose of the report itself. This means that only relevant health information about the patient themselves is entered into the patient's record. If the full report is required by the Practice or a third party, it should be obtained directly from the Data Controller of the report. We can mark such entries into the patients record as 'safeguarding relevant' and 'hide from online view' which will remove the consultation from the patient's online access and highlight any safeguarding consultations when processing a SAR.

Call recordings

3.19 Under GDPR Article 15, data subjects have a right to access their personal data including recordings of telephone calls, where these are made. Recordings made as part of the patient's care form part of the medical record. Relevant information from the recording can be transferred into the record through transcription or

summarisation, but where it is not possible to transfer clinical information from the recording to the medical record, the recording must be considered as part of the medical record and retained accordingly. Where this is the case, we would need to release a copy of the recording if requested in response to a subject access request.

3.20 Patient/receptionist calls won't generally form part of the medical record. However, if a patient specifically makes a request for a copy of the recording and we still hold this recording, then we should disclose this to the patient. Further information on call recordings can be found in our Telephone Call Recording and Retention Guidance which can be found in the DSP section on the GP Sharepoint site.

Checking the records

3.21 The copied records should be checked by an appropriate health professional prior to release. There is a restriction in the GDPR that restricts health data from being disclosed in response to a SAR if you are not a health professional, unless:

- an opinion has been obtained within the last six months from the appropriate health professional that the serious harm test for health data is not met, and
- we are satisfied that the health data has already been seen by, or is known by, the individual it is about.

3.22 The Data Protection Act 2018 defines a 'health professional' as a registered medical practitioner, or a registered nurse or midwife.

3.23 The record should be reviewed to determine whether any of the information contained in the record is exempt from disclosure.

When should we redact?

3.24 The bar for redacting information for the data subject is set very high. The GDPR sets out two instances when we should redact information:

- where granting access would disclose information relating to, or provided by a third party who could be identified from that information and who has not provided consent for the release of the information;
- where granting access would disclose information likely to cause serious harm to the physical or mental health of the patient or another individual, where the data subject does not already know the information.

3.25 As we use a redaction tool (iGPR), it is important that the GP reviews the redaction suggestions to ensure that we do not over redact.

Third party redactions

3.26 We should not normally redact information in a health record that identifies a health professional such as a doctor, consultant or nurse, carrying out their duties.

3.27 If the health record contains personal data relating to someone other than the requester, such as a family member, we should take into account the information we are disclosing and whether the other individual has consented to the disclosure of their data, and whether it is reasonable to disclose without consent. For example, if the record states that during a consultation '*Mr Smith's wife commented that…*', this would be acceptable to disclose because Mr Smith knows that he brought his wife along to the consultation and he is aware of what she said at the consultation. However, if the record has a separate entry stating that '*Mr Smith's mother telephoned to provide information about the family history of…*' then that should be redacted as it is information about a relative, provided by a relative and we can assume that the data subject may not be aware of this. Again, in practice, there should not be a lot of third party redactions.

3.28 If the third party has given their consent for disclosure, or if we are satisfied that it is reasonable to disclose it without consent, we should provide the information in the same way as any other information we provide in response to a SAR.

3.29 If we have not got the consent of the third party and we are not satisfied that it is reasonable to disclose the third party information, then we should withhold it and only disclose as much of the requested information as we can without disclosing the third party's identity.

Serious harm redactions

3.30 In most circumstances, even where information which is perceived to be of high sensitivity (e.g. abortions, sexual health etc.), it should not be redacted as the data subject knows that they have has an abortion/STD etc. This means that, in practice, there should not be a great deal of information likely to cause significant harm.

3.31 To determine whether right of access would be likely to cause serious harm to the physical or mental health of the patient, the health professional most recently responsible for the diagnosis, care or treatment of the individual should carry out the 'serious harm test'.

3.32 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.

3.33 Where there is any doubt as to whether disclosure would cause serious harm, advice can be provided by the Data Protection Officer, the Caldicott Guardian, or a defence body.

4. Requests from third parties

4.1 A third party can make a SAR on behalf of an individual, provided that the third party is entitled to act on the individual's behalf. We need to be satisfied that the third party making the request is entitled to act on behalf of the individual - it is the third party's responsibility to provide evidence of this. This might be a written authority to make the request or a power of attorney.

4.2 If there is no evidence that a third party is authorised to act on behalf of an individual, we are not required to respond to the SAR. However, if we are able to contact the individual, we should respond to them directly to confirm whether or not they wish to make a SAR.

4.3 In most cases, provided we are satisfied that the third party has the appropriate authority, we can respond directly to that third party. However, if we think an individual may not understand what information would be disclosed, and in particular we are concerned about disclosing excessive information, we will contact the individual first to make them aware of our concerns. If the individual agrees, we may send the response directly to them rather than to the third party.

4.4 There are cases where an individual does not have the mental capacity to manage their own affairs. In these cases, a representative with a Health and Welfare Power of Attorney has the appropriate authority to make a SAR on their behalf.

Solicitor

4.5 A solicitor can make a subject access request on behalf of a client, and it is the solicitor's responsibility to provide evidence that they are entitled to make a subject access request on their client's behalf. Solicitors have their lawful basis in the form of consent and are the liable party under the Data Protection Act 2018 to obtain fully informed consent.

4.6 If we have a genuine concern that a solicitor has requested excessive information, we should contact the patient first to make them aware of our concerns (each case needs to be judged on its own merits). If the patient agrees, we may send the response directly to the patient rather than to the solicitor. The patient may then choose to share the information with the solicitor after reviewing it. If we cannot contact the patient, we should provide the requested information to the solicitor, as long as we are satisfied that they are authorised to act on the patient's behalf.

4.7 We cannot demand that the patient collects their records on behalf of third party requests. The ICO has stated that "ultimately, data controllers are responsible for providing a SAR response to the individual or their appointed representative and a

person should not have to take action to receive the information, such as by collecting it from the controller's premises, unless they agree to do so".

Excessive information

4.8 Very often, we will receive a SAR from a solicitor who would like the patient's full record, for example, the solicitor may ask us to provide 50 years of records for a car accident that occurred two years ago, which may seem to be disproportionate. However, there is a legal principle, applicable in civil cases where the defendant has caused the claimant harm, known as the 'thin skull' rule. This means that a defendant will be liable for the full extent of the damage caused, even for outcomes which are not reasonably foreseeable, when the loss suffered by the claimant is at least partly due to a pre-existing vulnerability, be it physical, psychological or financial. If a defendant has injured someone who consequently requires medical treatment, they are likely to be liable for the consequences of that treatment, even if it is unforeseeable. Solicitors therefore request the full medical records to check for any particular vulnerabilities of their client (the claimant), when loss and injury are suffered as a result of another person's actions (the defendant), in order to prove that the defendant is liable for the full extent of the injuries suffered. This means that the full records will need to be provided.

4.9 If we are unsure as to whether the solicitor requires the full record, we can always check with the solicitor, or ensure that the patient understands that they have consented to their full record being shared. Ultimately, the solicitor is likely to require the full records in order to assess their client's vulnerabilities as well as the extent of the injuries they sustained. Solicitors are also bound by a professional code of secrecy and are under contract with their client.

Insurance company

4.10 The right of subject access gives individuals the right to obtain a copy of their own personal data. It should not be used by insurance companies as part of their business processes; the ICO has stated that "a SAR is not appropriate in situations where the third party's interests are not aligned with the individual's, for example an insurance company needing to access health data to assess a claim".

4.11 Insurance companies should request medical reports under the provisions of the Access to Medical Reports Act 1988. In such circumstances, with an individual's consent, an insurer can apply to the patient's GP who may produce a tailored medical report, providing only the information the insurer needs. Practices are able to apply a fee for completion of these reports and should agree the fee with the insurance company in advance. The GP must be satisfied that the patient has given valid consent to the release of the information (electronic consent is acceptable).

This Act applies only to medical reports written by a medical practitioner who has been involved in some way in the diagnosis or treatment of the individual patient

Consent

4.12 We should be satisfied that the patient has given valid consent to the disclosure of the information before any medical report can be provided. If consent is obtained electronically, there must be an audit trail of the consent process available to both the patient and the GP.

Opportunity to see the report

4.13 The insurer must inform the patient when a report has been requested, and check whether they wish to see the report. If the patient does wish to see the report, the insurer must inform the GP and the patient has 21 days to arrange to see the report. The GP must not send the report before the 21 days have elapsed. It is good practice to date stamp the request when received, to ensure compliance with this timeframe.

4.14 If the patient does not initially request access but then changes their mind and makes a subsequent request before the report is sent, the doctor must not send the report until the patient has made arrangements to see it, or 21 days have elapsed since the patient's request was made.

4.15 Doctors must not comply with requests from the patient to leave out relevant information from reports. If a patient is unwilling to give permission for certain relevant information to be included, the doctor should indicate to the insurer that he/she cannot write a report (without revealing any of the information that the patient did not want revealed).

4.16 A copy of the report must be kept for six months and patients have the right to request access to the report during this period.

4.17 It is a criminal offence to force an individual to make a SAR. If a SAR from an insurance company is received, in the first instance we should go back to the insurance company and ask them to request a medical report instead. Alternatively, the BMA suggests that we can also contact the patient to explain the implications of the insurance company making a SAR, and the extent of the disclosure. In these instances, GPs should provide the SAR information to the patient themselves, rather than directly to the insurance company.

Armed Forces

4.18 When a patient applies to join the Armed Forces, we may receive a SAR from them to access the medical records of the patient, as part of the Forces application

process. GDPR provides the data subject with the right to request access to their record by a third party. We must ensure we have received valid consent with the request, and if this is the case we can send the medical records directly to the Forces by a secure method.

4.19 The reason for requesting access to the medical records of an applicant is to enable an informed decision to be made as to the suitability of the patient for the Forces. The Navy/Army/Air Force Medical Officer needs to see the full patient record in order to make this assessment. The patient knows their own medical history and has consented to disclosure of this to the Forces.

4.20 There should be very few redactions within the disclosed record, as the reasons for redaction remain the same – only if it is information about a third party, or if it is information which may cause significant harm to the individual, and they don't already know the information e.g. safeguarding.

4.21 Where safeguarding information is contained within the medical record such as PPNs, MARAC reports, Child Protection reports etc. we will need to share proportional information that will allow the Forces to ensure that the individual meets their criteria for joining. If the Child Protection information relates to an event when the patient was a baby, then this may not be relevant or proportionate. However, if there is a history of criminal behaviour as a young person, then it would be in the public interest to disclose this information.

4.22 If we have concerns that the patient may not be aware that their full record will be disclosed to the Forces, we can always contact them to advise that we are intending to share this information (usually if they have had a social worker or a looked after children's nurse then they are quite aware of their issues).

4.23 Sometimes the Forces will offer a fee for release of the records. Where this is the case, we may charge for postage but not for collating the SAR itself.

4.24 The Forces may also ask for copies of full medical records for a new recruit. Where this is the case, we should transfer the full record as we would do if the patient were moving practices, which of course is effectively the case as they will be under the care of the relevant Forces Medical Officer.

Parents on behalf of children

4.25 Although a child may be too young to understand the implications of the right of access, it is still their right under the GDPR. However, in the case of young children, this right is likely to be exercised by those with parental responsibility, on their behalf.

4.26 Before responding to a SAR for information held about a child, we should consider in the first instance whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights (i.e. is Gillick competent if 13 years or older), then we should usually liaise directly to the child, providing that this will not place them in a difficult or uncomfortable situation with their parents. We may need to prepare to deny access to parents on behalf of a competent child.

4.27 We may, however, allow the parent or guardian with parental responsibility to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

Parental Responsibility

4.28 SARs can be exercised by anyone who has parental responsibility and our policy for checking an individual's parental responsibility should be equal and inclusive. If we expect all fathers to demonstrate parental responsibility, then we should also ask mothers to do so. Always consider the child's welfare - it is likely to be in their interest that all individuals with parental responsibility are aware of any conditions or illnesses and involved in their child's healthcare. We should not need to check for any removal or restriction of parental responsibility, the parent or guardian who is the main carer for the child will let we know about any Court Orders preventing access or removing parental responsibility.

4.29 Both biological parents will have parental responsibility if they are registered on a child's birth certificate and the child was born after 1 December 2003 (England and Wales). This means they are both entitled to independently make a subject access request and there is no obligation to inform the other parent that a SAR has been made. However, we should be careful not to release the contact details of one parent when responding to a SAR made by another parent, particularly where there is animosity between the parents, or the other parent is estranged but still has parental responsibility. This is particularly important when releasing safeguarding information.

4.30 If the child has been formally adopted, the adoptive parents hold parental responsibility as they have become the child's legal parents.

4.31 More than two people can have parental responsibility for the same child. Step-parents can apply to the court to obtain a parental responsibility order, which has to be agreed by both living parents with parental responsibility. If a step-parent has adopted a child, it puts him/her in the same position as a birth parent.

4.32 All women who carried the child automatically acquire parental responsibility as the mother. All spouses and civil partners of the mother also automatically acquire

parental responsibility. Unmarried biological fathers can automatically acquire parental responsibility by either being named on the child's birth certificate, by subsequently marrying the mother, by entering into a Parental Responsibility Agreement with the mother, or under a Parental Responsibility Order granted by the Courts.

4.33 Same-sex female partners who were civil partners at the time of the birth will both have parental responsibility. Both should be named on the birth certificate and there will be no legal father registered for the child. Same-sex male parents will need to formally adopt their child to gain parental responsibility and remove parental responsibility from the birth mother.

4.34 Occasionally, people other than the parents gain parental responsibility for a child, such as a legal Guardian or on the order of a Court e.g. a local authority can acquire parental responsibility (shared with the parents) while the child is the subject of a care or supervision order. If we are unsure as to whether the person requesting access to a child's medical record has parental responsibility, we should obtain legal advice.

4.35 Biological mothers, and fathers who are married to the mother, can only lose parental responsibility if their child is adopted. Their parental responsibility could also be restricted with a Prohibited Steps Order or Specific Issue Order made by the Courts. The parent or guardian who is the main carer for the child will advise us of such Orders, we should not need to go looking for them. An unmarried biological father will also lose their parental responsibility if their child is adopted.

4.36 It is possible for the Courts to terminate parental responsibility of an unmarried father or step parents where they have acquired parental responsibility by either being named on the birth certificate (unmarried fathers only), or with a Parental Responsibility Agreement or Parental Responsibility Order. Such cases are extremely rare, and the Courts will only discharge parental responsibility if it is in the best interests of the child. The parent or guardian who is the main carer for the child will advise us of this information.

4.37 We are entitled to refuse access to a parent or an individual with parental responsibility if the information held in the child's record is likely to cause serious harm to the child or another person.

5. Other disclosures

5.1 There will be other occasions when we receive requests for access to patient records from other agencies. These can include:

- the Coroner;
- the Courts;
- Social Services and other agencies;
- CCG;
- Parliamentary and Health Service Ombudsman;
- Department of Work and Pensions;
- Police;
- Mental Health Tribunals;
- Prisons.

Coroner's Office

5.2 Information may be disclosed to the Coroner. Although Data Protection legislation only applies to living individuals, the Common Law Duty of Confidentiality still applies to deceased individuals. If the information is in the form of original records, a form must be signed to transfer responsibility for confidentiality whilst in the possession of the Coroner's office. This form will also act as a receipt for the Practice that the original records are with the Coroner. Copies of the records must be retained by the Practice.

Courts

5.3 A court may order disclosure of personal information. A Court Order should be obeyed unless there is a robust justification to challenge it. Disclosure Orders from the court are processed under Article 6(1)(c) of the GDPR, and not under the lawful basis of consent. Therefore, Practices do not need to check the consent of the data subject.

5.4 Information does not need to be redacted for the courts as they are performing their judicial function under civil procedure rule 31.5, and in order to make an appropriate judgement on the case before them, they require all of the information. Data subjects should not need to put their own SAR into a practice in order to provide the Courts with un-redacted copies of their records.

Social Services and other Agencies

5.5 There will be occasions where the Practice receives requests for access to a patient's medical record from other agencies. This may include the General Medical Council, Social Services and other NHS organisations or statutory bodies such as the National Health Service Litigation Authority (NHSLA) and the Care Quality Commission. All of these requests should be considered on a case by case basis.

CCG

5.6 The Safeguarding team within the CCG may request access to patient records for a number of reasons:

- scoping or completion of domestic homicide reviews;
- safeguarding adult reviews;
- rapid reviews for children;
- serious case reviews;
- learning disability mortality reviews;
- fabrication and induced illness reviews.

5.7 There are statutory requirements to carry out these reviews and we can provide access to the records for nominated members of the CCG safeguarding team.

5.8 Other requests from the Safeguarding team relating to access to patient records (e.g. audit of patient safeguarding records) may be passed to the Practice for completion, with anonymised results to be sent back to the CCG.

5.9 The Continuing Healthcare team may also require access to patient records to enable assessments of eligibility for CHC or FNC funding. The patient (or their representative) has requested and consented to their information being accessed (including medical records) to enable the CCG to complete the funding assessment.

Note: There is a requirement within CHC to move their legal basis from a consent based model to public task. This will require some work between the CCG and Practices to ensure that data is processed lawfully.

Parliamentary and Health Service Ombudsman

5.10 Requests from the Parliamentary and Health Service Ombudsman must be complied with. The Ombudsman operates under the lawful basis of official authority and public interest, and therefore consent from the patient is not necessary (the patient will already have provided the PHSO with their consent to investigate their complaint).

Department of Work and Pensions

5.11 The Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the assessment or collection of a tax or duty. Any request by the Department of Work and Pensions for access to personal information about a patient must be accompanied by the relevant form. The individual should be asked for their consent to disclose the information, unless this would prejudice the enquiry or court case.

Police

5.12 When a request for access to patient information is made by the police, we must consider whether we have a legal duty to disclose, or a sufficiently important reason to disclose and a legal basis to do so.

Legal Duty to Disclose to the Police

5.13 Sometimes a disclosure is required under a specific piece of legislation and is therefore mandatory. The police should provide us with a disclosure form from the Chief Superintendent of the requesting police force which should state the specific information that is requested and the Act that they are making the application under, for example:

- Prevention of Terrorism Act (1989) and Terrorism Act (2000). We MUST inform the police if we have information (including personal information) that may assist them in preventing an act of terrorism, or help in apprehending or prosecuting a terrorist.
- The Road Traffic Act (1988). We have a statutory duty to inform the police, when asked, of any information that might identify any driver who is alleged to have committed an offence under the Act. We are not required to disclose clinical or other confidential information.
- The Female Genital Mutilation Act (2003). We have a statutory duty to report to the police where it appears that a girl under the age of 18 has been subject to genital mutilation.

5.14 The police may also present a written Court Order to acquire information about a patient. We do not need to obtain consent from the patient and we should not redact any of the record. If the Court Order is unclear or appears to be asking for too much information, we may be able to query this with the Court. Further information on call recordings can be found in the Disclosures to the Police Guidance which can be found in the DSP section on the GP Sharepoint site.

Voluntary Disclosures to the Police

5.15 The Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the prevention, detection or investigation of crime and/or the prosecution or apprehension of offenders. The Crime and Disorder Act 1998 also allows the disclosure of information to the police, local authority, probation service, or health authority for the purposes of preventing crime and disorder.

5.16 Any request by the police for access to personal information about an individual must be accompanied by the relevant disclosure form which should state the legal basis that the police are relying on. The form should also provide a clear description of the specific information that is requested.

5.17 Health professionals can then disclose patient information voluntarily to the police but there is no obligation to do so. If the request for information includes confidential medical information, the common law duty of confidentiality must be

respected. In such cases health professionals may only disclose information where the patient has given consent, or there is an overriding public interest.

5.18 A disclosure in the public interest is a disclosure that is essential to prevent a serious threat to public health, national security, the life of the individual or a third party, or to prevent or detect serious crime (such as murder, manslaughter, rape, treason, kidnapping and abuse of children or other vulnerable people). Serious harm to the security of the state or to public order and serious fraud will also fall into this category.

5.19 We should seek guidance from our Caldicott Guardian, Data Protection Officer or defence body if there is any doubt as to whether disclosure is in the public interest

5.20 Theft, minor fraud or damage to property, where loss or damage is less substantial, would generally not be considered to meet the public interest requirements.

5.21 When disclosing information to the police, we should only disclose the minimum and relevant information to satisfy the request.

Mental Health Tribunals

5.22 Requests for access to records may be received in preparation for mental health review tribunals. These requests should be dealt with urgently.

Prisons

5.23 We may receive requests for access to a patient's record from the prison service. All healthcare professionals in prisons are NHS staff and they should have an NHS email account. We must only liaise with healthcare staff and not patients or patient's relatives in order to maintain the safety of our staff, the healthcare professionals within the prison service and all of the offenders within the prison.

6. Deceased patients

6.1 The definition of personal data only relates to living individuals; the GDPR does not apply to data concerning deceased patients and therefore a SAR cannot be used to obtain information about a deceased individual. However, a third party may be able to access this information under the Access to Health Records Act 1990. Under this legislation, when an individual has died, their personal representative, executor, administrator or anyone having a claim resulting from the death has the right to apply for access to the deceased's information. This is subject to the recorded wishes of the deceased person.

6.2 The personal representative is the only person who has an unqualified right of access to a deceased patient's information and need give no reason for applying for access.

Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from an individual's death.

6.3 There may be circumstances where individuals who do not have a statutory right of access request access to a deceased patient's record. The duty of confidentiality continues beyond death and therefore when such requests are received, they must be considered on a case by case basis.

Deducted Patients

6.4 After a patient's death, GP health records are deducted from the Practice and a paper copy of the record should be sent to Primary Care Support England (PCSE). Applications for access to the deceased patient's record should be made to PCSE.

6.5 PCSE, as the holder of the deceased's record, is required to take advice before making a decision about disclosure. This is because PCSE is not the Data Controller of the record, as Data Protection legislation does not apply to the records of deceased patients. Staff at PCSE are not qualified to make a confidentiality decision which is why they return to the last registered practice for assistance. This is usually from the patient's last GP or, if several health professionals have contributed to the care of the patient, the health professional who was responsible for the patient's care during the period to which the application refers. If no appropriate health professional who has cared for the patient is available, a suitably qualified and experienced health professional must provide advice.

Fees

6.6 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.

Timeframe

6.7 The timeframe for responding to requests for information under the Access to Health Records Act 1990 is 40 calendar days.

6.8 Where the application concerns access to records or parts of records that were made in the 40-day period immediately preceding the date of application, access must be given within 21 days. Where the access concerns information all of which was recorded more than 40 days before the date of application, access must be given within 40 days.

Redactions

6.9 As with the medical records for living patients, information in the medical record of a deceased person should not be disclosed if:

- it identifies a third party without that person's consent unless that person is a health professional who has cared for the patient; or
- in the opinion of the relevant health professional, it is likely to cause serious harm to a third party's physical or mental health.

6.10 Additionally, information should not be disclosed if:

- the patient gave it in the past on the understanding that it would not be disclosed. No information at all can be revealed if the patient requested non-disclosure.

7. Other Data Subject Rights

7.1 Occasionally, after making a subject access request and receiving the information, a patient may wish to exercise another of their rights. As well as the right of access, patients also have the following rights under GDPR:

- the right to rectification (GDPR Article 16);
- the right to be forgotten (GDPR Article 17);
- the right to restrict processing (GDPR Article 18);
- the right to data portability (GDPR Article 20);
- the right to object (GDPR Article 21)
- the right to appropriate decision making (Article 22).

The right of rectification

7.2 Where the patient feels that information is incorrect, they have the right to ask for it to be corrected. This right applies to information of fact and not opinion. Incorrect demographic information will be immediately corrected. If the information is of a clinical nature, this will need to be reviewed and investigated by the Practice. The investigation will end with one of the following outcomes:

1. The Practice deems the information to be correct at the time of recording and it will not be amended. A statement from the patient may be placed within the record to show that they disagree with the information held. The patient has the right to appeal to the Information Commissioner.

2. The Practice agrees that the information is incorrect. However, it is not legally possible to modify or remove information within the record as it represents 'historical information' which may have influenced subsequent events or decisions made. Instead, a note will be place in the file, which alerts the reader of the inaccuracy and the correct facts.

The right to be forgotten

7.3 The right to be forgotten is a limited right with regards to healthcare information. There is a legal obligation to keep information in accordance with the Health Records Act 1958, in order to maintain patient safety and continuity of care. Additionally, the Records Management Code of Practice for Health and Social Care 2016 must be followed, and information cannot be destroyed before the retention period has ended. Where a patient requests the right to be forgotten, a note should be added to their record to indicate that they would like their information to be disposed of as soon as legally possible.

The right to restrict processing

7.4 The right to restrict processing can only be used in the following circumstances:

- the patient challenges the accuracy of the data;
- the processing is unlawful and the patient opposes the erasure of the personal data and asks for the restriction of its use instead;
- the Practice no longer needs the personal data for the purposes of processing, but the patient requires the data to establish, exercise or defend a legal claim. Practices should seek legal advice in these circumstances;
- the patient objects to the processing of their data whilst the Practice verifies whether the legitimate grounds of the Practice to continue processing overrides those of the patient.

7.5 The right to restrict processing of healthcare data for direct care should not be taken lightly and only in extreme circumstances. The patient should be given the opportunity to meet with a relevant clinician who can properly explain the limited services and treatments that will be available with restricted processing.

7.6 Patients are allowed to restrict the processing of data for secondary use purposes and should be provided with information on the National Data Opt-Out available via NHS Digital.

The right of data portability

7.7 This right only applies where the original processing is based on consent or the fulfilment of a contract that the patient is party to, and if the processing is carried out by automated means. However, in the spirit of the Regulations, subject access requests should be provided in a useful electronic format where possible.

The right to object

7.8 Patients can object to the processing of their personal data if it is for direct marketing purposes. They can also object if the processing is for a task carried out in the public interest or in the legitimate interests of the Practice, or if processing is for research or statistical purposes. If a patient raises an objection, the Practice has to demonstrate their legitimate grounds for the processing, which override the interests, rights and freedoms of the patient, or demonstrate that the processing is for the establishment, exercise or defence of legal claims. Until the justification can be provided, processing should be suspended.

7.9 This right is aligned with the right to restrict processing, and the patient should be provided with information on the National Data Opt-Out in order to opt-out of data processing for research or statistical purposes.

The right to appropriate decision making

7.10 Patients have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

References:

- ICO Guide to the GDPR;
- BMA Access to Health Records Guidance July 2019;
- BMA Access to Medical Reports October 2019;
- BMA Subject Access Requests for Insurance Purposes Updated October 2019;
- IGA Disclosure of Personal Information to the Police

Document Owner: **Emma Prince, Practice Manager**

Review period: Two yearly

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.2	September 2020	Emma Prince	Berni Rogers	Policy written by CCG DPO

APPENDIX ONE

LITTLEDOWN SURGERY

APPLICATION FOR ACCESS TO MEDICAL RECORDS

Article 15 GDPR 2016 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	

Declaration: I declare that the information given by me is correct to the best of my knowledge and that I am entitled to apply for access to the health records referred to above under the terms of Article 15 GDPR 2016.

Tick whichever of the following statements apply.

- I am the patient.
- I have been asked to act by the patient and attach the patient's written authorisation.
- I am the parent, or 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 am the deceased patient's Personal Representative and attach confirmation of my appointment.
- 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).

YOUR SIGNATURE……..DATE……..

Details of my Application (please tick as appropriate)

Patient to complete

I am applying for access to view my records only	
I am applying for a copy of my medical record	
I have instructed someone else to apply on my behalf	

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.

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)	