BMA

Access to health records

Updated to reflect the General Data Protection Regulation and Data Protection Act 2018

Guidance for health professionals in the United Kingdom May 2018

British Medical Association
bma.org.uk

Contents

1. Introduction **2**

2. Defining a health record **2**

3. Advice on record-keeping **2**

4. Subject access requests **3**

4.1 Who may apply for access? 3

4.1.1 Patients with capacity 3

4.1.2 Children and young people under 18 3

4.1.3 Next of kin 3

4.1.4 Solicitors 3

4.2 When should access be given? 4

4.3 What information should be provided to satisfy a subject access request? 4

4.4 Who must give access? 5

4.5 Can access be refused? 5

4.6 In what format should access be provided? 5

4.7 Must data controllers permit patients to inspect original records if they do not request copies of the data? 5

4.8 Can a fee be charged? 6

4.9 When should information not be disclosed? 6

4.10 Should medical terms be explained? 7

4.11 Can records be amended or can information be deleted from records? **7**

5. Requests for access made on behalf of others **7**

5.1 Parents 7

5.2 Individuals on behalf of adults who lack capacity 8

6. Requests from the police **8**

7. Requests from insurers **9**

8. Deceased patients **9**

8.1 Are there any rights of access to a deceased patient's records? 9

8.2 Who can apply for access? 9

8.3 Who must give access? 10

8.4 Can a fee be charged? 10

8.5 What information should not be disclosed? 10

8.6 Are relatives entitled to information about the deceased's last illness? 11

9. Records retention **11**

1. Introduction

The General Data Protection Regulation (GDPR) is an EU Regulation which became law in the UK on 25 May 2018. The GDPR should be read alongside the UK Data Protection Act 2018 (DPA 2018). The GDPR and the DPA 2018 replace the Data Protection Act 1998.

This guidance sets out a range of circumstances in which health professionals may receive, and respond to, requests for access to health records. It reflects the common enquiries received by the BMA. The guidance is divided into the following areas.

- Defining a health record (part 2)
- Advice on record-keeping (part 3)
- Subject access requests (part 4)
- Requests for access made on behalf of others (part 5)
- Requests from the police (part 6)
- Requests from insurers (part 7)
- Deceased patients (part 8)
- Records retention (part 9)

2. Defining a health record

A health record exists to provide an account of a patient's contact with the healthcare system. Health records consist of information relating to the physical or mental health or condition of an individual made by a health professional in connection with the care of that individual.

The information is most commonly recorded in electronic form, however, some records are in a manual form or a mixture of both. 'Information' covers expressions of opinion about individuals as well as facts. Health records may include notes made during consultations, correspondence between health professionals such as referral and discharge letters, results of tests and their interpretation, X-ray films, videotapes, audiotapes, photographs, and tissue samples taken for diagnostic purposes. They may also include reports written for third parties such as insurance companies.

3. Advice on record-keeping

Health records must be clear, accurate, factual, legible and should be contemporaneous. They must include all relevant clinical findings, the decisions made, information given to patients, and drugs or treatment prescribed. Personal views about the patient's behaviour or temperament should not be included unless they have a potential bearing on treatment or it is necessary for the protection of staff or other patients. Health records should not be altered or tampered with, other than to remove or correct inaccurate or misleading information. Any such amendments must be made in a way that makes it clear what has been altered, who made the alteration and when it took place.

Doctors should ensure that their manner of keeping records facilitates access by patients if requested. It may be helpful to order, flag or highlight records so that when access is given, any information which should not be disclosed, (such as those which identify third parties) is readily identifiable.

If patients express views about future disclosure to third parties, this should be documented in the records. Doctors may wish to initiate discussion about future disclosure with some patients if it seems foreseeable that controversial or sensitive data may be the issue of a future dilemma, for example after the patient's death.

4. Subject Access Requests

A request by a patient, or a request by a third party who has been authorised by the patient, for access under the GDPR (and DPA 2018) is called a subject access request (SAR). Rights of access are not confined to health records held by NHS bodies. They apply equally to the private health sector and to health professionals' private practice records. Subject to the conditions explained in this guidance, individuals have a right to apply for access to health records irrespective of when they were compiled.

Where joint data controller arrangements are in place for multi-contributory records, there must be a clearly documented agreement on how data controller responsibilities will be satisfied, including the handling of subject access requests.

4.1 Who may apply for access?

4.1.1 Patients with capacity

Subject to the exemptions listed in paragraph 4.9 (below) patients with capacity have a right to access their own health records via a SAR. Patients may also authorise a third party such as a solicitor to do so on their behalf. Competent young people may also seek access to their own records. It is not necessary for patients to give reasons as to why they wish to access their records.

4.1.2 Children and young people under 18

Where a child is competent, they are entitled to make or consent to a SAR to access their record.

Children aged over 16 years are presumed to be competent. Children under 16 in England, Wales and Northern Ireland must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to an SAR. However, children who are aged 12 or over are generally expected to have the competence to give or withhold their consent to the release of information from their health records. In Scotland, anyone aged 12 or over is legally presumed to have such competence. When assessing a child's competence, it is important to explain the issues in a way that is suitable for their age.

Where, in the view of the appropriate health professional, a child lacks competency to understand the nature of his or her SAR application, the holder of the record is entitled to refuse to comply with the SAR.

Where a child is considered capable of making decisions about access to his or her medical record, the consent of the child must be sought before a parent or other third party can be given access via a SAR (see paragraph 4.1.3 below).

4.1.3 Next of kin

Despite the widespread use of the phrase 'next of kin', this is not defined, nor does it have formal legal status. A next of kin cannot give or withhold their consent to the sharing of information on a patient's behalf. As next of kin they have no rights of access to medical records. For parental rights of access, see the information above.

4.1.4 Solicitors

A patient can authorise a solicitor acting on their behalf to make a SAR. Health professionals releasing information to solicitors acting for their patients should ensure that they have the patient's written consent. Solicitors must provide the patient's written consent. The consent must cover the nature and extent of the information to be disclosed under the SAR (for example, past medical history), and who might have access to it as part of the legal proceedings. Where there is any doubt, health professionals should confirm with the patient before disclosing the information. Should the patient refuse, the solicitor may apply for a court order requiring disclosure of the information.

A standard consent form has been issued by the BMA and the Law Society of England and Wales (attached). While it is not compulsory for solicitors to use the form, it is hoped it will improve the process of seeking consent. (The form is suitable for use in England and Wales).

A common enquiry to the BMA is whether a patient's original medical records can be sent to a solicitor. While the GDPR entitles the applicant (or their solicitor) to be supplied with a copy of the health record it does not entitle them to be supplied with the original record. The BMA strongly recommends that health professional do not send original notes and records to solicitors (or any other external parties) because of the potential detriment to patient care should the records be lost.

4.2 When should access be given?

SARs can be made electronically, in writing or verbally.

Before access is provided the identity of the person making the request must be verified using 'reasonable means'.

Once the request has been received and verified, the individual must be provided with a copy of their data without undue delay, and at the latest within 28 days from the date of the request.[1] Sometimes, additional information is needed before copies can be supplied. In such cases, the 28-day time limit will begin as soon as the additional information has been received.

The 28-day time-limit can be extended for two months for complex or numerous requests where the data controller needs more time to collate and supply the data. Individuals should be informed about this within 28 days and provided with an explanation of why the extension is necessary.

There is nothing in the GDPR or DPA that prevents health professionals from informally showing patients (or proxies) their records as long as no other provisions of the GDPR or DPA are breached.

4.3 What information should be provided to satisfy a subject access request?

Individuals are entitled to receive all the personal data a controller holds about them (subject to the limited exemptions covered in paragraph 4.9). It is reasonable, however, for a health professional to discuss with a patient whether they require all the information held or whether limited or tailored content would satisfy the request. For example, a patient might submit a SAR for their full medical record but on discussion it might be revealed that the patient only requires their blood type and would be satisfied to receive this limited content. Should a patient ask for the full information this should be supplied.

Data controllers should also be aware that the time-limit for compliance with SARs (see paragraph 4.2) begins when the initial request is received and verified. The time-limit is not suspended by a discussion with the patient in relation to the content of the SAR.

The GDPR requires that certain supplementary information must be provided when individuals submit a SAR. When providing copies of health records, individuals must be provided with the following additional information:

- **The purposes for processing data**
  Organisations, such as GP practices, which provide healthcare services to patients can state that the purpose for which data is processed is for the delivery of healthcare to individual patients. In addition, the data is also processed for other non-direct healthcare purposes such as medical research, public health or health planning purposes when the law allows.
- **The categories of personal data**
  The category of personal data can be stated as healthcare data.

1 The GDPR refers to a 'one month' deadline. The BMA advises that organisation should apply a universal 28 day month approach.

- **The organisations with which the data has been shared**
  Healthcare bodies can state that health records are shared with the appropriate organisations which are involved in the provision of healthcare and treatment to the individual. Healthcare bodies must also tell individuals which other organisations will receive their confidential health information, for example, NHS Digital or the Scottish Primary Care Information Resource (SPIRE) or research bodies such as the Secure Anonymised Linkage Databank (SAIL). (This information should already be available to patients in practice privacy notices.)[2]
- **The existence of rights to have inaccurate data corrected and any rights of objection**
  For example, a national 'opt-out' model.
- **Any automated decision taking including the significance and envisaged consequences for the data subject**.
  For example, risk stratification.
- **The right to make a complaint to the Information Commissioner's Office (ICO)**.

4.4 Who must give access?

Responsibility for providing access to records lies with the 'data controller'. The data controller will usually be an organisation. Organisations should have a policy for handling subject access requests which makes it clear which member(s) of staff are responsible for managing these requests.

4.5 Can access be refused?

If a request is 'manifestly unfounded or excessive', for example, because it is repetitive, access can be refused (or a fee can be charged, see below). There is little further explanation as to when a request might be considered as 'manifestly unfounded or excessive'. However, it would be prudent to assume that the threshold set here is fairly high and that accordingly requests should be refused on this basis only where the facts are particularly extreme.

Where access has been refused on this basis, the patient must in any event be given an explanation as to why access has been refused and they must also be informed that they have the right to complain to the ICO.

4.6 In what format should access be provided?

If the request is made electronically access should normally be given in electronic format. Where patients request the medical record to be emailed to them it is strongly recommended that the practice explains to the patient the risks (for example, unauthorised interception of the data) of receiving their data via unencrypted means to a non-NHS email address. The practice should document the patient's agreement (expressed in writing or via email) to receive their data via unencrypted means in the medical record. If the patient agrees a USB stick or a CD can be used as alternative electronic formats if these are supplied by the patient.

For requests which are not made electronically a paper copy should be provided unless the patient has requested a different format.

4.7 Must data controllers permit patients to inspect original records if they do not request copies of the data?

The GDPR does not expressly require a data controller to permit a patient access to their data by inspecting original records where no copy is requested. However, depending on the circumstances a data controller may take the view that it should in any event permit inspection of the original records. Patients sometimes become distressed when reading their records. It is therefore advisable for a member of staff to be present with them to provide support, as well as to explain any clinical terms (see paragraph 4.10). It is also important for staff to be present to ensure that records are not altered.

2 For more information on privacy notices and other data controller responsibilities see BMA guidance 'GPs as data controllers' available at: bma.org.uk/ethics. The BMA has also produced a range of template privacy notices for GP practices.

4.8 Can a fee be charged?

Initial access must be provided free of charge (including postage costs) unless the request is 'manifestly unfounded' or 'excessive' – in which case a 'reasonable' fee can be charged. These circumstances are likely to be rare and should be assessed on a case by case basis.

The ICO has advised us that a request may be deemed 'manifestly unfounded' if the requestor makes it clear they are only requesting the information to cause disruption to the organisation or if the requestor makes completely unsubstantiated accusations against the controller. If however, the requestor has some form of genuine intention in obtaining their information, it is unlikely the request could be deemed as manifestly unfounded.

A request could be deemed as 'excessive' if an individual was to receive information via a subject access request (SAR), and then request a copy of the same information within a short period of time. In this scenario, the organisation could charge a reasonable fee based on the administrative costs of providing further copies or refuse the request.

4.9 When should information not be disclosed?

The GDPR read together with the forthcoming Data Protection Act 2018 provides for a number of exemptions in respect of information falling within the scope of a SAR. In summary, information can generally be treated as exempt from disclosure and should not be disclosed, if:

- it is likely to cause serious physical or mental harm to the patient or another person; or
- it relates to a third party who has not given consent for disclosure (where that third party is not a health professional who has cared for the patient) and after taking into account the balance between the duty of confidentiality to the third party and the right of access of the applicant, the data controller concludes it is reasonable to withhold third party information; or
- it is requested by a third party and, the patient had asked that the information be kept confidential, or the records are subject to legal professional privilege or, in Scotland, the records are subject to confidentiality as between client and professional legal advisor. This may arise in the case of an independent medical report written for the purpose of litigation. In such cases, the information will be exempt if after considering the third party's right to access and the patient's right to confidentiality, the data controller reasonably concludes that confidentiality should prevail; or
- it is restricted by order of the courts; or
- it relates to the keeping or using of gametes or embryos or pertains to an individual being born as a result of in vitro fertilisation; or
- in the case of children's records, disclosure is prohibited by law, e.g. adoption records.

The data controller must redact, or block out any exempt information. Depending on the circumstances, it may be that the data controller should take steps to explain to the applicant how it has applied the relevant exemption. However, such steps should not be taken if, and insofar as, they would in effect cut across the protections afforded by the exemptions. Indeed, in some cases even confirming the fact that a particular exemption has been applied may itself be unduly revelatory (e.g. because it reveals the fact that the information sought is held where this revelation is itself unduly invasive of relevant third party data privacy rights). There is still an obligation to disclose the remainder of the records.

While the responsibility for the decision, as to whether or not to disclose information, rests with the data controller, advice about serious harm must be taken by the data controller from the appropriate health professional. If the data controller is not the appropriate health professional, then the appropriate health professional needs to be consulted before the records are disclosed. This is usually the health professional currently or most recently responsible for the clinical care of the patient in respect of the matters which are the subject of the request. If there is more than one, it should be the person most suitable to advise. If there is none, advice should be sought from another health professional who has suitable qualifications and experience.

Circumstances in which information may be withheld on the grounds of serious harm are extremely rare, and this exemption does not justify withholding comments in the records because patients may find them upsetting. Where there is any doubt as to whether disclosure would cause serious harm, the BMA recommends that the appropriate health professional discusses the matter anonymously with an experienced colleague, their Data Protection Officer, the Caldicott Guardian, or a defence body.

4.10 Should medical terms be explained?

Copies of medical records which are supplied under subject access rights must be accompanied by an explanation of any terms that might be unintelligible to the patient or the person requesting access to the records. Even in cases where permanent copies cannot be supplied, an explanation of such terms must be given.

4.11 Can records be amended or can information be deleted from records?

No. Records should not be amended because of a request for access. Indeed, it is a criminal offence under the forthcoming Data Protection Act 2018 to amend or delete records in response to a SAR. If amendments are made between the time that the request for access was received and the time at which the records were supplied, these must only be amendments that would have been made whether or not the request for access was made. When dealing with a SAR the most up-to-date information should be provided.

Information which is clinically relevant must not be deleted from medical records. (For electronic records, information can be removed from display but the audit trail will always keep the record complete.) Amendments to records can be made provided the amendments are made in a way which indicates why the alteration was made so that it is clear that records have not been tampered with for any underhand reason. Patients may also seek correction of information they believe is inaccurate. The health professional is not obliged to accept the patient's opinion, but must ensure that the notes indicate the patient's view. Health professionals are advised to provide the patient with a copy of the correction or appended note.

Patients also have the right to apply to the ICO or a court to have inaccurate records amended or destroyed.

5. Requests for access made on behalf of others

The GDPR and forthcoming Data Protection Act 2018 do not provide subject access rights to third parties when they are acting on behalf of an individual who is lacking competence or capacity. Subject access rights lie only with the individual who is the subject of the record. However, those acting on their behalf may still be able to access information as set out below.

5.1 Parents

Parents may have access to their children's records if this is not contrary to a child's best interests or a competent child's wishes. For children under 18 or, in Scotland under 16, any person with parental responsibility may apply for access to the records.

Not all parents have parental responsibility. In relation to children born after 1 December 2003 (England and Wales), 15 April 2002 (Northern Ireland) and 4 May 2006 (Scotland), both biological parents have parental responsibility if they are registered on a child's birth certificate. In relation to children born before these dates, a child's biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or at some time thereafter. If the parents have never been married, only the mother automatically has parental responsibility, but the father may acquire that status by order or agreement. Neither parent loses parental responsibility on divorce. Where more than one person has parental responsibility, each may independently exercise rights of access.

A common enquiry to the BMA concerns a child who lives with his or her mother and whose father applies for access to the child's records. In such circumstances there is no obligation to inform the child's mother that access has been sought.

Where a child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility.

In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court. A local authority acquires parental responsibility (shared with the parents) while the child is the subject of a care or supervision order. If there is doubt about whether the person seeking access has parental responsibility, legal advice should be sought.

The holder of the record is entitled to refuse access to a parent, or an individual with parental responsibility where the information contained in the child's records is likely to cause serious harm to the child, or another person (see paragraph 4.9).

5.2 Individuals on behalf of adults who lack capacity

Patients with a mental disorder or some degree of cognitive impairment should not automatically be regarded as lacking capacity to give or withhold consent to disclosure of confidential information. Most people suffering from a mental impairment can make valid decisions about some matters that affect them.

An individual's mental capacity must be judged in relation to the particular decision being made. If a patient has capacity, requests for access by relatives or third parties require his or her consent.

When patients lack mental capacity, health professionals are likely to need to share information with any individual authorised to make proxy decisions such as an individual acting under the authority of a lasting power of attorney.

Both the Mental Capacity Act in England and Wales and the Adults with Incapacity (Scotland) Act contain powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults. The Court of Protection in England and Wales, and the Sheriff's Court in Scotland, can also appoint deputies to do so. This may entail giving access to relevant parts of the incapacitated person's medical record, unless health professionals can demonstrate that it would not be in the patient's best interests. These individuals can also be asked to consent to requests for access to records from third parties.

Where there are no nominated individuals, requests for access to information relating to incapacitated adults should be granted if it is in the best interests of the patient. In all cases, only information relevant to the purposes for which it is requested should be provided.

6. Requests from the police

A common enquiry to the BMA is the rights of access to health records by the police. If the police do not have a court order or warrant they may ask for a patient's health records to be disclosed voluntarily under Schedule 2, Paragraph 2 of the DPA 2018. However, while health professionals have the power to disclose the records to the police, there is no obligation to do so. In such cases health professionals may only disclose information where the patient has given consent, or there is an overriding public interest. For doctors, the threshold for disclosures in the public interest is that set out by the GMC and which reflects the requirements of the common law duty of confidentiality[3].

In this context 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. This includes crimes 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. In contrast, theft, minor fraud or damage to property, where loss or damage is less substantial, would generally not justify the breach of confidence necessary to make the disclosure.

Health professionals should be aware that they risk criticism if they fail to take action to avoid serious harm being caused to others. Guidance should be sought from the Caldicott guardian, or defence body where there is any doubt as to whether disclosure should take place in the public interest.

3 GMC (2017) Confidentiality: good practice in handling patient information paras 63 – 70.

7. Requests from insurers

SARs from insurance companies to GP practices for the disclosure of full medical records is the subject of separate advice available on the BMA website.[4] The position of the ICO is that the use of SARs to obtain medical information for life assurance purposes is an abuse of subject access rights and the processing of full medical records by insurance companies risks breaching the GDPR.

This does not mean, however, that GP data controllers can refuse to respond to a SAR from an insurer outright. When a SAR from an insurance company is received, the GP should contact the patient to explain the extent of the disclosure that has been sought. GPs can then, if requested, provide the patient themselves with their medical record rather than providing them directly to the insurance company. It is then the patient's choice as to whether, having reviewed the record, they choose to share it with the insurance company.

There is a clear distinction between the use of SARs by a solicitor, who can be seen as an agent of the patient and who is acting on the patient's behalf, and the use of SARs by insurance companies.

Insurance companies should use the provisions of the Access to Medical Reports Act 1988 to seek a GP report.

8. Deceased patients

The GDPR does not apply to data concerning deceased persons. However, the ethical obligation to respect a patient's confidentiality extends beyond death. Moreover, The Information Tribunal in England and Wales has also held that a duty of confidence attaches to the medical records of the deceased under section 41 of the Freedom of Information Act. The Freedom of Information Act in Scotland contains an exemption to the disclosure of medical records of deceased patients. However, this duty of confidentiality needs to be balanced with other considerations, such as the interests of justice and of people close to the deceased person. Health professionals should therefore counsel their patients about the possibility of disclosure after death and solicit views about disclosure where it is obvious that there may be some sensitivity. Such discussions should be recorded in the records.

8.1 Are there any rights of access to a deceased patient's records?

Statutory rights of access are set out in the Access to Health Records Act 1990 and the corresponding legislation in Northern Ireland, the Access to Health Records (Northern Ireland) Order 1993. The Access to Health Records Act 1990 covers manual health records made since 1 November 1991. In Northern Ireland the Access to Health Records (Northern Ireland) Order 1993, covers manual records from 30 May 1994. Access must also be given to information recorded before these dates if this is necessary to make any later part of the records intelligible.

8.2 Who can apply for access?

Unless the patient requested confidentiality while alive, their personal representative and any other person who may have a claim arising out of their death has a right of access to information in their records, which is directly relevant to a claim.

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

4 bma.org.uk/advice/employment/gp-practices/service-provision/medical-information-requests-from-insurers

8.3 Who must give access?

After a patient's death, GP health records may be held by Primary Care Support England, local health boards or, in Northern Ireland, the Business Services Organisation. Hospital records may have been retained at the hospital the patient attended or they may have been sent to a local archive for storage. Applications for access can be made to the records manager of these bodies, or applicants may approach the deceased's GP practice. Should applicants approach the GP practice and, where the practice still holds an electronic copy of the deceased's record, the practice is obliged to respond to the request under the Access to Health Records Act 1990 (or corresponding legislation in Northern Ireland).

The bodies holding the deceased's record (other than the deceased's GP) are required to take advice before making a decision about disclosure. 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.

Once the person holding the records is satisfied that the person requesting the information is entitled to it, access must then be given within specified time limits. Access can be given either by allowing the applicant to inspect the records or extract, or by supplying a copy if this is requested.

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. If the records are held by a health service body access cannot be given before advice has been obtained. The courts may enforce compliance with the legislation if access is not given within the required time limits. The court may also require that the records be made available for its own inspection in order to come to a decision.

There is no statutory right of access to records of deceased patients which fall outside of the time period covered by the legislation. If access to these records is being granted, the BMA advises that doctors should apply the safeguards and restrictions of the legislation to prevent harm or breach of confidence.

8.4 Can a fee be charged?

Legislative changes to the Data Protection Act 2018 has 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.

8.5 What information should not be disclosed?

Information 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; or
- the patient gave it in the past on the understanding that it would be kept confidential. No information at all can be revealed if the patient requested non-disclosure.

8.6 Are relatives entitled to information about the deceased's last illness?

While there is no legal entitlement other than the limited circumstances covered under the Access to Health Records legislation, health professionals have always had discretion to disclose information to a deceased person's relatives or others when there is a clear justification. A common example is when the family requests details of the terminal illness because of an anxiety that the patient might have been misdiagnosed or there might have been negligence. Disclosure in such cases is likely to be what the deceased person would have wanted and may also be in the interests of justice. Refusal to disclose in the absence of some evidence that this was the deceased patient's known wish exacerbates suspicion and can result in unnecessary litigation. In other cases, the balance of benefit to be gained by the disclosure to the family, for example of a hereditary or infectious condition, may outweigh the obligation of confidentiality to the deceased.

9. Records retention

The health departments give detailed advice about the minimum retention periods applicable to NHS records. The recommendations apply to both electronic and manual records, and the BMA advises private practitioners to follow the same rules.

Hospital records should be kept for a minimum of eight years following the end of treatment, and GP records for 10 years, although certain types of records, such as children's records, obstetric records, and mental health records are kept for longer.

When health professionals are responsible for destroying health records, they must ensure that the method of destruction is effective, and does not compromise confidentiality. Incineration, pulping, and shredding are appropriate methods of destroying manual records. Electronic data should be destroyed using appropriate data destruction software.

BMA/The Law Society consent form

Consent form (Releasing health records under the General Data Protection Regulation and the Data Protection Act 2018)

Your health records

Your health records typically contain information from almost all consultations and contacts you have had with health professionals in the practice and information sent to the practice about you from others, such as hospital letters.

The information they contain usually includes:

- why you saw a health professional;
- details of clinical findings and diagnoses, investigations, tests and scans;
- any options or recommendations for care and treatment the health professional discussed with you;
- the decisions made about your care and treatment, including evidence that you agreed; and
- details of actions health professionals have taken and the outcomes.

Why your records are needed and what may happen to them

If you are making, or considering making, a legal claim for compensation related to an injury to your health, your solicitor will likely need to see copies of all your GP records. They will also need any hospital records made in connection with the incident and others that may be relevant. This is to enable the solicitor to understand the incident and your injury and give you legal advice on the merits and value of your claim.

If you decide to go ahead with your claim, your solicitor may advise that it is sensible (or that it may be necessary) to give copies of your records to:

- the expert whom your solicitor or agent instructs to produce a medical report as evidence for the case;
- the insurance company for the person or body you are making a claim against;
- the person or the body you are making a claim against and/or their solicitors;
- any insurance company or other organisation paying or providing an indemnity for your legal costs; and
- any other person (such as a barrister) or body (such as the court) officially involved with the claim.

Once you start your claim, the court can order you to give copies of your health records to the solicitor of the person you are making a claim against so he or she can see if any of the information in your records can be used to defend his or her client. The solicitor of the person or body you are making the claim against will likely show your records to their client in the normal course of advising them and may show them to others too (such as a barrister or medical expert). If the person you are making the claim against does not have a legal representative the court can order you to give copies to them directly.

You do not have to give permission for your health records to be obtained and disclosed in your case but if you don't, it is unlikely that your claim will be able to proceed if the medical records are crucial evidence in your claim. The court may not let you go ahead with your claim and your solicitor may be unable to continue to represent you.

If there is very sensitive information in the records that is not connected to the claim you should tell your solicitor. They will then consider whether this information may be relevant and needs to be disclosed in the case. Your solicitor can advise you on this and if appropriate may advise you to discuss the matter with your medical practitioner.

Important

By signing this form, you are agreeing to the health professional, hospital and others named on this form releasing copies of your health records to your solicitor or agent. During the process your records may be seen by people who are not health professionals, but they will keep the information confidential.

Part a – your details and those of your health professionals and your solicitors or agents

Your full name (and any other names by which you have been known):	
Your address:	
Date of birth:	
NHS number (if known):	
Hospital number (if known):	
Date of incident:	
Solicitor's or agent's name and address:	
GP's name and address (and phone number if known):	
Ambulance Service used (if any):	
Name (and address if known) of the hospital(s) you attended in relation to this incident:	
If you have seen any other person or organisation about your injuries (for example, a physiotherapist) or have had any investigations (for example, X-rays) please provide details:	

Part b – your declaration and signature

I have read this form and fully understand the contents of it.

To health professionals
I understand that filling in and signing this form gives you permission to give copies of all my health records including complete GP records, and any hospital records relating to this incident, to my solicitor or agent whose details are given below.

Please give my solicitor or agent copies of my health records, in line with the Data Protection Act 2018, within 30 days.

Your signature: Date: / /

Part c – your solicitor's or agent's declaration and signature

Before you ask your client to fill in and sign this form you should ask your client to read the notes above. You should explain that signing this form will permit release of his or her complete health records and how the information in them may be used. You should explain that this form only applies to the release of the medical record to you and that separate consent will be obtained for any onward disclosures which are required.

If your client is not capable of giving his or her permission in this form, it may be possible for someone to give consent and sign it on their behalf, for example:
– your client's litigation friend;
– someone who has enduring/lasting power of attorney to act for your client; or
– your client's deputy appointed by the Court of Protection.

You must only use health records for specific purposes that your client has agreed to in advance.

Under the General Data Protection Regulation and Data Protection Act 2018 you have responsibilities relating to sensitive information. The entire health record should not be revealed without the client's permission and you should not keep health records for any longer than is necessary for agreed-to purposes. You should return copies of health records to the client at the end of the claim if they want them. If they do not want them, you will be responsible for confidentially destroying them.

To health professionals
I have told my client the implications of giving me access to his or her health records. I confirm that I need the full records in this case.

Solicitor's or agent's signature: | | Date: | / / |

Notes for the medical records controller

This form shows your patient's permission for you to give copies of his or her complete record, and any hospital and other records relating to this incident, to his or her solicitor or agent.

You must give the solicitor or agent copies of these health records unless any of the exemptions set out in Schedules 3 and 4 of the Data Protection Act 2018 apply. The main exemptions are that you must not release information that:

– is likely to cause serious physical or mental harm to the patient or another person; or
– relates to someone who would normally need to give their permission (where that person is not a health professional who has cared for the patient).

Your patient's permission for you to release information is valid only if that patient understands the consequences of his or her records being released, and how the information will be used. The solicitor or agent named on this form must explain these issues to the patient. If you have any doubt about whether this has happened, you should contact the solicitor or agent, or your patient.

This form does not contain a comprehensive statement of solicitors' or health professionals' obligations under the relevant data protection legislation. If you are in any doubt about your legal obligations, seek advice.

The BMA publishes detailed guidance for doctors on giving access to health records. You can view that guidance by visiting: **www.bma.org.uk/ethics**

This form is published by the Law Society and British Medical Association. (3rd edition, October 2018)

BMA

The Law Society

British Medical Association
BMA House, Tavistock Square,
London WC1H 9JP
bma.org.uk

© British Medical Association, 2018

BMA 20180215