BMA

Focus on Subject Access Requests for insurance purposes

Updated September 2024

British Medical Association
bma.org.uk

Focus on Subject Access Requests for insurance purposes

Introduction

The BMA often receives enquiries from member about some insurance companies who are seeking to obtain full medical records through the use of Subject Access Requests (SARs) under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Due to the BMA's concern that this practice was potentially a breach of the DPA (now UK GDPR), as disclosure of the full medical record would amount to a disclosure of information which was not relevant for the purpose, on behalf of our members we raised this matter with the Information Commissioner's Office (ICO).

The ICO is the UK's independent authority set up to uphold information rights in the public interest, including data privacy for individuals. It is the duty of the Information Commissioner to promote the following of good practice by data controllers. We have now received a view from the ICO on the use of SARs for insurance purposes.

Important note: It is important to note that the principles in this guidance are relevant for requests from insurance companies only. The guidance does not extend to SARs from patients' solicitors. A patient can authorise a solicitor acting on their behalf to make a SAR (see p.3 of this guidance). Provided the solicitor has given the GP the patient's written consent for the disclosure of the full medical record, the SAR from the solicitor should be treated in the same way as if it was made directly by the patient.

Information Commissioner's view

The ICO has written to the ABI[1] to confirm that the right of subject access is not designed to underpin the commercial processes of the life insurance industry. The Commissioner takes the view that the use of subject access rights to access medical records in this way is an abuse of those rights and that the subsequent processing of full medical records by insurers is likely to fall foul of the UK GDPR in a number of ways.

One of the key points from the ICO's advice is that insurance companies which process full medical records are likely to breach the UK GDPR principle which states that information must be 'adequate, relevant' and limited to the purpose for it is processed.

The ICO's view, however, does not mean that GPs can refuse to respond to SARs for insurance purposes outright. The BMA has sought to clarify with the ICO how GPs can ensure they continue to meet their data controller obligations to process legitimate SARs and remain compliant with the other principles of the UK GDPR. Based on the ICO's view, we are providing the following advice to practices.

1 The ABI represents UK insurers and has over 250 member companies, accounting for over 90% of the UK insurance market. The ICO has also written to Legal & General, which is not currently a member of the ABI.

Advice for practices

The ICO has stated that when a SAR from an insurance company is received, GPs should contact the patient to explain the implications of such a request and the extent of the disclosure. The ICO is also clear that GPs should provide the SAR information to the patient themselves, rather than directly to the insurance company.

The ICO's Subject Access Code of Practice[2] states that *'If you think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, you may send the response directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.'*

The BMA has therefore produced a template letter for GPs to send to patients which is in-line with the advice from the ICO. The letter offers patients a choice between a SAR, whereby the medical record would be provided to them to share with the insurer as they wish or asking their insurance company to seek a GP report. The letter is attached at Appendix 1.

GP reports

It is our expectation that insurance companies will discontinue the use of SARs and will instead revert to requesting medical reports under the provisions of the Access to Medical Reports Act 1988 (AMRA). The BMA has separate guidance on this legislation.[3]

Practices are able to apply a fee for completion of these reports, in line with the work associated, and should seek to agree the fee with the requestor in advance of completion. Practices may also wish to seek advanced payment. Information on the BMA's recommended fee, plus guidance on completing insurance reports, is on the BMA website.[4]

SAR requests from third parties for non-insurance purposes

Following a number of queries received from practices, we would like to make it absolutely clear that this guidance relates to SARs for insurance purposes only. Under the UK GDPR, an individual is entitled to make a SAR via a third party, for example a solicitor acting on behalf of a client. The ICO's guidance is that such requests, where the third party is acting on behalf of the patient, are appropriate.

The ICO has drawn a clear distinction between this practice, where the third party can be seen as an agent of the patient, and insurance companies' use of SARs.

Where practices receive SARs from a third party (for non-insurance purposes), the ICO Code of Practice states '*In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney*'.

2 Right of access | ICO
3 Access to medical reports
4 BMA pay and contracts: Fees

Appendix 1

Template letter to a patient in response to a SAR

Dear [Patient]

I am writing to you as your insurance company has requested access to your full medical record. You will already be aware of this as you have agreed for the insurance company to make a Subject Access Request – as enclosed. I understand that you have signed a form of consent, however, we need to be satisfied that you have provided specific and informed consent for your full medical records to be shared with the insurance company. This is because your records may include extremely sensitive information which you may not expect to be shared or may not need to be shared as part of your application for insurance or the assessment of any claim.

I also want to let you know that our representative body (The British Medical Association) has questioned whether the law allows insurance companies to use Subject Access Requests to obtain confidential and sensitive personal data. The UK General Data Protection Regulation states that only data which is sufficient for the purpose for which it is required should be disclosed and sensitive personal data which is not relevant or excessive in relation to this purpose should not be disclosed.

The Information Commissioner's Office (ICO) has recently written to the insurance industry to confirm that they consider the use of subject access rights in this way is inappropriate and an abuse of that right.

As the guardian of your medical record, we are responsible for ensuring only necessary and relevant information held on your record is shared with an insurance company, however we also have a duty to comply with a subject access request made by you as a patient and do not want to cause any delays to your application.

We are therefore giving you a choice. We can provide you with a copy of your full medical records under a Subject Access Request. This would not be considered as excessive as we are providing the information to you, not the insurance company. It is then entirely your decision whether you give your medical records to the insurance company in full or not

Alternatively, you can ask your insurer to request a GP report from the practice which will only cover information in your record that is relevant to your application. Medical reports also exclude some information, in line with agreement reached with the insurance industry, such as genetic test results and certain information about sexually transmitted infections.

Please therefore let us know if you would like a copy of your full medical records under a subject access request or whether you plan to ask your insurer to seek a medical report.

The BMA has let the Association of British Insurers (ABI) and insurance companies know that we are offering patients this choice. If your insurance company expresses concern about this, please ask them to contact the ABI.

Yours faithfully

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

BMA 20240729