ICO consultation on the draft right of access guidance

The right of access (known as subject access) is a fundamental right of the General Data Protection Regulation (GDPR). It allows individuals to find out what personal data is held about them and to obtain a copy of that data. Following on from our initial GDPR guidance on this right (published in April 2018), the ICO has now drafted more detailed guidance which explains in greater detail the rights that individuals have to access their personal data and the obligations on controllers. The draft guidance also explores the special rules involving certain categories of personal data, how to deal with requests involving the personal data of others, and the exemptions that are most likely to apply in practice when handling a request.

We are running a consultation on the draft guidance to gather the views of stakeholders and the public. These views will inform the published version of the guidance by helping us to understand the areas where organisations are seeking further clarity, in particular taking into account their experiences in dealing with subject access requests since May 2018.

If you would like further information about the consultation, please email SARguidance@ico.org.uk.

Please send us your response by 17:00 on **Wednesday 12 February 2020**.

Privacy statement

For this consultation, we will publish all responses received from organisations but we will remove any personal data before publication. We will not publish responses received from respondents who have indicated that they are an individual acting in a private capacity (e.g. a member of the public). For more information about what we do with personal data see our privacy notice.

Please note, your responses to this survey will be used to help us with our work on the right of access only. The information will not be used to

consider any regulatory action, and you may respond anonymously should you wish.

Please note that we are using the platform Snap Surveys to gather this information. Any data collected by Snap Surveys for ICO is stored on UK servers. You can read their Privacy Policy.

Q1 Does the draft guidance cover the relevant issues about the right of access?

Yes

No

Unsure / don't know

If no or unsure/don't know, what other issues would you like to be covered in it?

We have answered yes to the question but would request that the ICO consider the issue below.

Adults lacking capacity

The guidance on pages 11 – 12 states that: 'However, it is reasonable to assume that an attorney with authority to manage the property and affairs of an individual has the appropriate authority to make a SAR on their behalf'.

We disagree that reliance on a property and affairs LPA would render access to medical information lawful. The one possible exception might be where access to the individual's medical information was necessary to fulfil an obligation under a property and affairs LPA – in which case it would seem reasonable to permit access to information relevant to fulfilling the obligation.

We are not aware of any case law in this area, however, in our view there is a clear distinction between a property and affairs LPA and a health and welfare LPA. It is entirely plausible that an individual might wish to grant an LPA to a person to manage their financial affairs (eg manage the sale of their house) but would not wish the same person to access their medical record (unless the exception above applies).

Q2 Does the draft guidance contain the right level of detail?

Yes

No

Unsure / don't know

If no or unsure/don't know, in what areas should there be more detail within the draft guidance?

Dealing with third party information

Pages 41 – 44 provide advice about taking into account any duty of confidentiality when deciding whether to disclose information about a third party without their consent. Further guidance on this complex issue in the context of medical records would be helpful. An area of enquiry to the BMA from GP practices is the question of whether to disclose information shared by a third party who requested confidentiality. If the third party is not a patient of the practice then it is unclear whether a duty of confidence exists in this context.

We note the sentence on p.44 which states that: '…depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent'.

We would welcome guidance on the question of whether the ICO would expect disclosure of information provided by a third party who requested confidentiality if:

- the information provided relates to the data subject; and
- the name of the third party is withheld (bearing in mind the data subject might still be likely to be able to identify the third party without a name).

For example, the daughter of a patient at a practice tells the GP that her father is 'getting very confused' - but asks the GP not to tell her father that she has shared this information. The daughter is not a patient of this practice. The father puts in a SAR. Should the information provided by the daughter - but not the identity of the daughter - be disclosed?

This issue is also important in relation to prevention of risk of harm to third parties. Our members report instances where information about patients has been provided to doctors by third parties who might be at risk if the information they provided is not appropriately redacted, or withheld, when complying with a SAR. This is particularly important in relation to domestic violence and child abuse cases where the victim of violence (or a child) is at risk if the violent partner discovers they have shared details of the abuse. Sometimes the redaction itself indicates the presence of information from which the source can be easily identified.

Section titled 'What about requests for health data from a third party?' (p. 66)

As the ICO is aware the question of SARs from solicitors acting on behalf of patients has caused a great deal of confusion for GP practices perpetuated by the recent case of *Major v Jackson & Others* concerning disclosures under civil procedure rules.

Our objective is to ensure that GPs have clear advice so that they can comply with the law and ICO advice. This must be done in a way which places the minimum burden on busy practices which are dealing with increased volumes of solicitor requests since GDPR came into effect.

The advice on page 66 (and on p. 11) is clear that solicitors (or other authorised third parties) can make SARs on behalf of their clients and that data controllers must respond directly to the third party unless there is a genuine cause for doubt. Where GPs have a genuine concern that the request is excessive they should contact the patient to make them aware of the concerns.

Would it be possible to reference the joint BMA and Law Society template consent form here? The aim of the form is to reduce the burden on GPs by providing assurance that patients:

- have given consent to the disclosure to their solicitor; and
- are informed about the scope of the disclosure.

It would be helpful if the ICO guidance provided more details on the options which are available to practices when they are complying with SARs and, importantly, the limitations to the various options. Specifically, we understand that practices can:

- offer or invite online access to records to patients – provided it is made clear that other paper-based options are also available;
- offer to provide electronic copies of the record;
- ask patients (or solicitors when they are acting for patients) to clarify the extent of the information being sought.

We understand, however, that practices cannot insist on the method of access where this is contrary to the expressed wishes of the patient or the patient's authorised solicitor. If, for example, a patient's solicitor requests a paper copy of the record be posted to them we understand that practices can offer an electronic version but cannot insist upon this method of providing access. It would be helpful to make this clear for practices so they can avoid unknowingly breaching GDPR.

Q3 Does the draft guidance contain enough examples?

Yes

No

Unsure / don't know

If no or unsure/don't know, please provide any examples that think should be included in the draft guidance.

We suggest inclusion of an example of a SAR from a solicitor to a GP practice to illustrate some of the points discussed above.

Page 4 states that individuals are not entitled to data relating to others unless their data also relates to other individuals. It would be helpful to include an example of how one data subject's data can make another data subject's data disclosable in the

context of medical records which can often contain information about family members.

Page 31 – Do we need to provide remote access?
We suggest inclusion of an example of NHS records and the use of Patient Online.

Page 63 – Is health data exempt if disclosure goes against an individual's expectations and wishes?
Some of our members found this section difficult to interpret. It would help to include an example. We suggest an example which explains how the following scenario should be handled. The parents of a competent 15 year-old ask for data on their daughter. The daughter provided the GP with information relating to the contraceptive pill on the basis this information would not be shared with her parents.

Q4 We have found that data protection professionals often struggle with applying and defining 'manifestly unfounded or excessive' subject access requests. We would like to include a wide range of examples from a variety of sectors to help you. Please provide some examples of manifestly unfounded and excessive requests below (if applicable).

We have no comments on this question.

Q5 On a scale of 1-5 how useful is the draft guidance?

1 - Not at all useful | 2 – Slightly useful | 3 – Moderately useful | 4 – Very useful | 5 – Extremely useful

Q6 Why have you given this score?

The guidance makes clear what the ICO expects of data controllers based on the wording within the GDPR / DPA 18.

Q7 To what extent do you agree that the draft guidance is clear and easy to understand?

Strongly disagree | Disagree | Neither agree nor disagree | Agree | Strongly

Q8 Please provide any further comments or suggestions you may have about the draft guidance.

Page 10
We are aware that individuals do not have to tell data controllers their reason for making a SAR. As currently worded, this could be interpreted as meaning that data controllers cannot ask requesters if only certain elements of the record would satisfy the request, rather than the entire record.

We would welcome clarity in the ICO guidance to ensure that GP data controllers are not led to believe they cannot enquire if less than the full medical record would satisfy the SAR. For information, the BMA's guidance states that:

'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.'

Page 11
There is reference to a third party's provision of written authority to make a request. It would be helpful to include more detail on what form this written authority should take – as mentioned in our response to Q2 the BMA and Law Society have a joint template consent form to provide solicitors with authorisation to access the medical records of their clients.

Page 12 - Section on responding to requests made via a third party online portal.
The guidance states that data controllers 'need to consider' certain factors to determine if they should comply with an online request. The guidance also states that data controllers 'are not obliged to take proactive steps' to discover that a SAR has been made. It would be helpful to more clearly distinguish the difference between the responsibility to consider a SAR which has been made (and which the data controller knows has been made) and having to search for evidence that a SAR has (or has not) been made.

Page 15 - Can we deal with a request in our normal course of business?
The guidance states: 'For example, if an individual requests copies of letters which you have sent to them previously, it is unlikely that you need to deal with this as a formal SAR'.
It is unclear how this might relate to hospital letters which a GP knows have been copied to a patient – does the GP need to provide these letters in response to a SAR?

Page 16
It would be helpful to mention here that data controllers do not need to comply with a SAR if one of the exemptions applies – and refer to the section on exemptions.

Page 21
The example box suggests provision of evidence of date of birth as a means of verifying a request. Given the sensitivity of information in medical records we would suggest a stronger identification check where doubt about identity exists.

Where further steps are taken to verify identification, we suggest that data controllers are advised to document action taken so that is clear when the clock

starts ticking on the time period for compliance.

Page 25
The statement that information cannot be retained indefinitely is not correct in the context of medical records. Most medical records must be retained indefinitely while the patient is alive. Following the death of a patient, NHS national retention periods must be followed - the standard retention period being 10 years after the death of the patient.

Page 35
'You can refuse to comply with a SAR if it is….'
We suggest inclusion of the words '*if you believe* it is...'
This nuanced change to the wording is based on our understanding that there is no definition of 'unfounded' or 'excessive' requests therefore it is ultimately the decision of the data controller as to whether these exemptions apply. Data controllers must, of course, be able to justify their decision.

Page 66
'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'.
It might be helpful if the guidance also included an additional example of a request which falls outside of a SAR ie where a solicitor acting for someone else wishes to access information about a data subject and applies for a court order.

Q9 Are you answering as:

An individual acting in a private capacity (eg someone providing their views as a member of the public)

An individual acting in a professional capacity

On behalf of an organisation

Other

Please specify the name of your organisation:

British Medical Association

What sector are you from:

Trade Union and Professional Association

Q10 How did you find out about this survey?

- ICO Twitter account
- ICO Facebook account
- ICO LinkedIn account
- ICO website
- ICO newsletter
- ICO staff member
- Colleague
- Personal/work Twitter account
- Personal/work Facebook account
- Personal/work LinkedIn account
- Other

If other please specify:

Thank you for taking the time to complete the survey.