Upholding information rights

Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

By email only:

26 August 2021

Dear

The Information Commissioner's response to the consultation on Adult Support and Protection Guidance for General Practitioners and Primary Care Teams

The Information Commissioner's Office (ICO) is pleased to respond to the Scottish Government's consultation on the Guidance for General Practitioners and Primary Care Teams which consists of two online documents – a guidance booklet and a supporting one-page Quick Guide.

The Commissioner is independent of government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

We welcome the inclusion of references to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) within the guidance reflecting changes in data protection legislation since the original was published in 2013. However, we wish to highlight that, at the end of the UK's transition period when exiting the EU, the GDPR was incorporated into UK data protection law as the 'UK GDPR' and this sits alongside the DPA 2018. This should be updated within the text of the guidance throughout.

We have reviewed the consultation document and have provided some comments that focus in particular on; lawful basis for sharing data, the right to object, data minimisation, and data sharing. As many of the consultation questions fall outside of the scope of the Information Commissioner's regulatory role we have elected to respond outside of the survey.

It is worth noting at the outset of this response that data protection law enables organisations and businesses to share personal data securely, fairly and proportionately. The ICO's Data Sharing Code of Practice and the resources available at our Data Sharing Information Hub provide detailed guidance, tools and other resources to aid data sharing in compliance with data protection law and you may wish to provide links to these resources in the guidance.

Data sharing between data controllers

On page 6 of the guidance it states the following:

> *Under those sections, the data controller is the local authority/the Council Officer making the request; and the GP or Primary Care Team (in receipt of this request) is the subject.*

We assume that this is a reference to the respective status of the Council and the Primary Care Team under data protection law. If that is the case, from a data protection perspective this statement is incorrect. A data subject is someone who can be identified from personal data, ie they are the 'subject' of the data. A data controller has the responsibility of deciding how personal data is processed - they are the main decision-makers and exercise overall control over the purposes and means of the processing of personal data. Both the Council and the GP/Primary Care Teams are likely to be controllers. The data subjects will be the adults under their care and about whom the enquiry is being made/whose records are being examined. The Council Officer will not be a controller in their own right but will instead be acting for the Council.

Primary Care providers including GPs should be clear about whether they are a controller, joint controller or processor for the personal data that they intend to share.

Planning for Data Sharing

We would strongly recommend that GPs and Primary Care Teams take the time to consider all of the scenarios in which they may share data about vulnerable adults in their care and associated third parties. Some of this sharing may take place under the 2007 Act but other sharing may take place outwith the Act.

Where data sharing is a regular occurrence there should be Data Sharing Agreements (DSAs), informed by Data Protection Impact Assessments (DPIAs), which will help to ensure that data sharing is carried out in compliance with the law. For instance on page 8 it states:

> *"When sharing information to the appropriate authorities seeks to address a **perceived risk of harm** to that individual, **practitioners should consider whether the sharing is necessary for the exercise of their statutory function under the 2007 Act** …is vital that GPs are aware of their **local contact and protocol** for making such a referral and should familiarise themselves with the details."*

We welcome the inclusion of the above paragraph and we would recommend including data sharing agreements, alongside the local contacts and protocols, as something that GPs should be aware of.

Data sharing in an emergency

GPs and Primary Care Providers can also carry out forward planning for emergency situations.

In particular organisations and practitioners should be confident that relevant personal information can be shared lawfully if it is to protect someone from serious physical, emotional or mental harm, including safeguarding within a medical context. GPs and Primary Care Teams can be made aware that in an emergency they should go ahead and share data as is necessary and proportionate. The ICO has a section on data sharing in an urgent situation or in an emergency in the Data Sharing Code of Practice. The Code sets out that an emergency includes:

- preventing serious physical harm to a person;
- preventing loss of human life;
- protection of public health;
- safeguarding vulnerable adults or children;

In these situations, it might be more harmful not to share data than to share it.

We would strongly recommend that controllers plan ahead for urgent or emergency situations as far as possible. Controllers should consider what data sharing might need to take place, what data should be shared and how this can be done in compliance with the law. This may involve preparing DPIAs and implementing DSAs to cover emergency situations which can include the relevant lawful bases and any conditions for processing as well what is likely to be

necessary and proportionate in the context of the sharing. In an urgent or emergency situation, decisions have to be made rapidly and it can be difficult to make sound judgements about whether to share information. Spending time forward planning is key.

To Share or Not to Share Checklist

We welcome the inclusion of the bulleted list on public task and the "to share or not to share" checklist on pages 12 and 13 however we would recommend the following amendments:

- "*Are there any exemptions in the Data Protection Act 2018 to sharing? (e.g. special category data exemptions)*". Conditions for processing special category data and exemptions from particular UK GDPR provisions are different and should not be conflated. You may wish to rephrase along the lines of "are you sharing special category data? Are you able to identify a condition for processing from Article 9 UK GDPR that you can you rely on? Do you need to identify an additional condition from the DPA 2018? See the section on special category data for more details". It may also be worth providing a link to the ICOs guidance page on special category data.

- "*This lawful basis may be relied upon if processing personal data*" is amended to "this is a possible lawful basis" You can rely on this lawful basis if you need to process personal data: 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law.

- "*Has consent been obtained e.g. of the person, an attorney or guardian, or another third party?"* is made clearer to distinguish between medical consent and consent under data protection law.

- "*Is there an organisational / in house protocol to be respected*?" includes reference to a Data Sharing Agreement.

- "*Has the individual been consulted with openness and transparency? If not, reasons should be documented*." We recommend that this also include reference to a controllers transparency obligations under data protection law, the transparency obligations apply unless a valid exemption in the DPA 2018 can be identified.

- "*Whether the information was shared with or without consent*" should be clarified or re-worded for clarity.

4. Does the guidance effectively address the question of sharing information with and without patient consent?

We think the section in the guidance on 'Consent' could be clearer.

For processing to be lawful under the UK GDPR, controllers must identify (and document) a lawful basis for the processing. Consent is only one of six lawful bases and the UK GDPR sets a high standard for controllers to demonstrate that the conditions required for consent have been met.

Under data protection law it is unlikely that consent can be relied upon as a lawful basis for processing in this scenario as it requires that individuals have a real choice and control about the processing of their personal data. If GPs/ Primary Care Teams cannot offer patients a genuine choice – such as when there is a legal duty to process the data or if they intend to make the referral regardless - consent will not be appropriate. Furthermore, due to the power imbalance between adults and GPs / Primary Care Teams, it will be difficult to demonstrate that consent was freely given. As the guidance notes there are other lawful bases that controllers can look to, in this particular context legal obligation and public task are the most relevant.

In the section Information Requests and Responses – Sections 4, 5 and 10 on page 6 it says "*For the avoidance of doubt, data processing, in relation to this request, is necessary for compliance with legal obligations under sections 4, 10 and 49(2) of the 2007 Act*" later it goes on to say "*practitioners should consider whether the sharing is necessary for the exercise of their statutory function under the 2007 Act . This would constitute the legal basis of public task"*. To avoid confusion we would suggest that the guidance provides links to the ICO's guidance on public task and legal obligation as well as directing GPs and Primary Care Teams to work with their Data Protection Officer (DPO) to determine which basis is most appropriate in different circumstances and to document that.

Relying on a lawful basis other than consent does not prevent GPs or other practitioners seeking the adult's input or views and being transparent about the sharing, indeed it is an important component of a controllers transparency and fairness obligations under data protection law.

We would also suggest that the section in the guidance on consent:

- Makes a clear distinction between medical consent and consent under data protection law.

- Sets out clearly why consent is unlikely to be an appropriate lawful basis for processing patient data for adult protection purposes but directs GPs and Primary Care Teams to 'Public Task' and 'Legal Obligation', and encourages these bodies to determine and document which lawful basis they can rely on in different scenarios. This should be done in consultation with their DPO.

- Emphasises the importance of transparency with the patient, controllers transparency obligations under data protection law and that relying on public task or legal obligation does not prevent patient views being sought.

Special category data and criminal offence data

As the guidance notes on page 9, where special category data is being processed an additional condition under Article 9 of the UK GDPR is required. The guidance should also set out that where criminal offence data, including data relating to alleged offences and to victims, is being processed an additional condition under Article 10 of the UK GDPR is required.

It may be useful to note in the guidance that the DPA 2018 contains specific legal gateways for processing special category and criminal offence data for safeguarding purposes namely those at Schedule 1, Part 2, Paragraphs 18 (Safeguarding of children and of individuals at risk) and Paragraph 19 (Safeguarding of economic well-being of certain individuals).

Individuals' Information Rights

The Data protection legislation provides individuals with a number of qualified rights in relation to the processing of their personal data including the right to be informed, the right of access, the right to rectification and the right to object. GPs and Primary Care Teams should be aware of these and have clear processes in place to allow individuals to access their rights, they should make individuals aware of how they can access their rights in privacy information.

The UK GDPR and the DPA 2018 does set out exemptions from some of the rights and obligations in some circumstances. If an exemption applies, you may not have to comply with all the usual rights and obligations. Exemptions should only

be applied on a case by case basis and, where they are being relied upon, the reasoning for doing so should be documented.

It may be that, the requirement to comply with, for instance, the right to be informed, could, in certain circumstances, prejudice the referral process. There are exemptions available that may be relied on in these cases. Article 14 (5)(b) for example, sets out that the requirements do not apply when the provision of this information to the individual is likely to 'render impossible or seriously impair the achievement of the objectives of that processing'. Furthermore there is a specific exemption from Article 15 requirements (confirmation of processing and the right of access) when a serious harm test is met. It exempts you from the UK GDPR's provisions on the right of access regarding your processing of health data. The exemption only applies to the extent that compliance with the right of access would be likely to cause *serious harm* to the *physical* or *mental health* of any individual. This is known as the 'serious harm test' for health data. You may wish to reference this within the text of the guidance.

Schedules 2, 3 and 4 of the DPA 2018 contain further exemptions which can be considered on a case-by-case basis. We also have more detail in our guidance page on exemptions.

Right to Object

In particular it may be useful for the guidance to reference an individual's Right to Object which only applies in certain circumstances and can be exercised either verbally or in writing. Individuals can object where the processing is on the basis of 'public task'. However it is important to note that the right is not absolute. An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.

Article 5(1)(c) UK GDPR - Data Minimisation

The data minimisation principle requires that personal data being processed is adequate, relevant and limited to what is necessary in order to fulfil the purpose for which it is being processed. At various points in the document it advises practitioners that information sharing should be "relevant and proportionate", for instance at page 4 it states that "*When deciding to make a referral and what information to share, consider what you believe is relevant and proportionate to the specific concerns you have*" and on page 10 it states "*Please ensure that you provide relevant and proportionate information to assist risk assessment and appropriate decision making*." In our experience controllers often overlook the

‘adequate’ aspect of the data minimisation principle, adequacy means that enough information is shared in order to fulfil the purpose for which it is being shared, you may wish to amend the text to include this detail for practitioners.

Further details on the data minimisation principle can be found on our website.

Please note that we have not reviewed the draft guidance line by line for accuracy however we trust this response is a helpful steer. We recommend that the final draft of the guidance is shared with the Scottish Government Data Protection team who will be able to advise further. If there is anything that you would like clarification on please do not hesitate to get in touch either with myself or my colleague

We have copied in the Data Protection team to this response for information.

Yours sincerely

Senior Policy Officer
0330 313 1715