ICO consultation on the draft updated data sharing code of practice

Q1 Does the updated code adequately explain and advise on the new aspects of data protection legislation which are relevant to data sharing?

☒ Yes

☐ No

Q2 If not, please specify where improvements could be made.

Q3 Does the draft code cover the right issues about data sharing?

☒ Yes

☐ No

Q4 If no, what other issues would you like to be covered in it?

```



```

Q5   Does the draft code contain the right level of detail?

☒ Yes

☐ No

Q6   If no, in what areas should there be more detail within the draft code?

```



```

Q7   Has the draft code sufficiently addressed new areas or developments in data protection that are having an impact on your organisation's data sharing practices?

☐ Yes

☒ No

Q8   If no, please specify what areas are not being addressed, or not being addressed in enough detail

An emerging area is data sharing for purposes of analytics and insight across multiple organisations/data controllers and the associated data matching and meshing techniques which need to be developed. The balance has to be struck between identifying people (even if temporarily to do matching) in order to get meaningful results and the privacy of people. It is vital that this is all assessed (as part of DPIA work) prior to the processing. A lot of current guidance from ICO and NHS creates a stark distinction between 'de-identified' data and 'identifiable' personal data. The fact is there is a lot of grey in between with the increasing need to temporarily identify people to do data matching. SODA (Suffolk Office of Data & Analytics) has developed an Information Sharing Assurance Framework to do this

The Code could give more weight to one outcome of the DPIA being:

- Techniques for pseudonymisation, de-identification and data obfuscation prior to sharing or whether this is carried out shortly after sharing by one of the parties [cross reference ICO guidance on this].
- Agreement on whether special category data is strictly necessary (or could be stripped out) and how disclosive is the data when data-sets are meshed together from multiple organisations.
- Where a party is using a 'matching engine' using numbers and identifiers on data on subjects from multiple organisations. And how far such an 'engine' is used for one-off purposes or is added to over time which may increase privacy risks as you get a fuller picture of a person's interactions with multiple organisations.
- That once the agreed party has carried out the data matching (e.g. to be sure Mary Smith from council A is the same Mary Smith from health organisation B) then identifiers can be removed.
- The fact that all of the above is still personal data [but personal data with security controls which means there is a remote chance of re-identification by non-authorised person].
- That organisations could consider true anonymisation and dummy data for testing and some modelling purposes.
- For the data sharing partners to agree how far the outputs of the matching will be identifiable.

*much of this is in other ICO guidance, but it becomes especially important when there are multiple information sharing organisations so it could be alluded to in the code of practice.

Q9   Does the draft code provide enough clarity on good practice in data sharing?

☐ Yes

☒ No

Q10 If no, please indicate the section(s) of the draft code which could be improved, and what can be done to make the section(s) clearer.

Just a couple of points of detail:

Pg 27: Lawful basis: You could consider making reference to the fact that the lawful basis for one of the data controllers for the original purpose may not be the same for the purposes once it is shared with another party (e.g. original lawful basis for collection by Police may be law enforcement but once shared for a multi-organisational project it may be 'public task'). The DPIA has to look at whether the new lawful basis is compatible with the original one.

Pg 28: Perhaps something stronger on the parties when making an information sharing agreement to state the responsibilities as to information security reporting in a timely manner (when/how etc) in order to meet the 72 hours deadline if it should be reportable to the ICO. When there are multiple parties there can be confusion as to who you inform first (especially as data controllership may have changed).

Pg 32: Point out that the ISA should state who is data controller after the sharing (e.g. party A and B become joint data controllers after sharing etc.). This point is often misunderstood with a recipient of data believing they are merely a processor.

Q11 Does the draft code strike the right balance between recognising the benefits of sharing data and the need to protect it?

☒ Yes

☐ No

Q12 If no, in what way does the draft code fail to strike this balance?

Q13 Does the draft code cover case studies or data sharing scenarios relevant to your organisation?

☒ Yes

☐ No

Q14 Please provide any further comments or suggestions you may have about the draft code.

We welcome the new draft, particularly on the expanded section on law enforcement personal data sharing.
We also note there is a section on the emerging area of data ethics.
The NHS in England often cites 'common law' as a key consideration for sharing/not sharing patient data across organisations without consent in addition to GDPR/DPA. Is there scope for the Code to at least touch on this as there is often a lot of confusion?

Q15 To what extent do you agree that the draft code is clear and easy to understand?

☐ Strongly agree

☒ Agree

☐ Neither agree nor disagree

☐ Disagree

☐ Strongly disagree

Q16 Are you answering as:

☐ An individual acting in a private capacity (e.g. someone providing their views as a member of the public of the public)

☐ An individual acting in a professional capacity

☒ On behalf of an organisation

☐ Other

Please specify the name of your organisation:

Suffolk Office of Data & Analytics (SODA)

Thank you for taking the time to share your views and experience.