medConfidential response to the ICO data sharing code consultation

The rights of data subjects are forgotten

Throughout this Code, the rights, needs, and interests of data subjects seem to be as forgotten as they are in the most narrow-minded of data-driven techno-utopianism. The Code provides nothing that ensures data subjects will be able to meaningfully and straightforwardly understand how their data is shared and used under the principles of the Data Protection Act.

If the ICO's own Code of Practice on Data Sharing does not make it crystal clear what organisations can and should do, why would any organisation bother following such guidance?

We are aware that some organisations would like to cower in dark corners and share data without scrutiny; it is such intent that has undermined public confidence in both data use and data sharing, and this is something the Code should address. In its current form, that it does not do so, is a significant missed opportunity.

Indeed, the Government's own Code of Practice under the Digital Economy Act has higher standards than the ICO appears (in this Code) to believe Government should have – in particular with regard to the register of projects, and the presumption of publication of paperwork.

Shortly after this consultation closes, a publication to which medConfidential has contributed will likely illustrate the folly of this approach.

Overall, the Code has metastasised, from 59 pages in 2011 to over 100 in the current version - and that is without counting the numerous off-Code references, none of which carry any legal force according to statements made on page 9.

If the new Code cannot say what needs to be said in what is almost double the space of the previous Code, then it should be edited with a much stronger focus on the necessary - by which we mean addressing long-standing, well-known issues - tackling head-on those excuses we already know people give for ignoring best practice and the letter and spirit of the law.

Particular points

'Summary'

- The 2011 Code states, *"This code explains how the Data Protection Act 1998 (DPA) **applies to the sharing of personal data**. It also provides good practice advice that will be relevant to **all organisations that share personal data**."* The 2019 Code however (p4, bullet point 2) states, *"This code covers the sharing of personal data **between organisations which are controllers**."*
    - Why has the scope and application of the Code been so radically narrowed? What about data sharing between controllers and processors, or data subjects and either controllers or processors? If indeed the Code covers only the sharing of data between controllers, then it is difficult to see how it even meets the full statutory requirements of Section 121(1)(a) of DPA 2018.

- Mandatory DPIA (p5, final bullet point): while people should indeed think carefully about sharing children's data, this is far from the only situation in which a DPIA is compulsory. The summary is dangerously misleading in this regard; Article 35(1) & (3) are very clear that this is about high risks to the rights and freedoms of <u>all</u> natural persons, as well as specific types of processing.
    - The Code must make this absolutely clear, even in summary - REDRAFT!

- DEA framework (p6, bullet point 2): it is notable that while <u>all</u> data sharing under DEA 2017 must be recorded in a register, the ICO has much lower standards within this Code.
    - Why has the ICO not replicated in its Code the standard for the public sector that Government has imposed on itself in the DEA Code?

- Data trusts (p6, bullet point 3): while it may be desirable to have a section somewhere in the Code on novel, largely untested concepts that - while theoretically possible in commercial and contract law - still present significant challenges[1] with regard to personal data (especially special category data like health data), it seems extremely unbalanced to include such a thing in the Code summary when far more fundamental issues - such as anonymisation, which receives just one entirely ambiguous mention in the entire document! - have not been properly covered.
    - Add something on anonymisation in the summary, and remove the reference to data trusts. And add a clear and credible summary explanation of anonymisation, pseudonymisation and de-identification (vs. anonymous data) elsewhere in the Code *before* linking off to more detailed information on the ICO website. It was failure to handle this properly in past Codes that led to enormous trouble, and loss of public trust.

[1] https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf

- Failure to do this clearly, and in the body of the Code - for, as it says on p9, *"the code **stands alone** as your guide to data sharing"* - will simply replicate (or exacerbate) past failures. This is especially true given the statement at the top of p9: *"Any further reading or other resources which are mentioned in or linked from this code **do not form part of the code**"* - in other words, all the advice on the ICO website can (and will) be ignored with impunity by those who choose to use the most literal interpretation of what the Code itself says.

Examples on pages 14 & 15

- Given previous comments, it seems unwise and again unbalanced to include three narrow examples all focused within healthcare. Could the ICO not find examples of the benefits of data sharing from three different areas? Also, there is no indication in the examples of the data subjects having any indication of how data about them is being shared and used. Are evidence of fairness and transparency not benefits too? And where DPA (or other arrangements) offers data subjects the right to dissent or object, should that not also be clearly signposted? To have three examples from health that make no mention whatsoever of, e.g. the National Data Opt-out, seems rather remiss...

Pages 16 & 17

- As noted in comments on the summary, *"For the purposes of this code, **it does not include sharing data with employees, or with processors**"* is a radical narrowing in scope from the previous Code, which explicitly <u>does</u> cover such forms of sharing, as in, e.g. *"a retailer providing customer details to a payment processing company"* (p6, 'About the Code').

    - If the entire premise of the Code is based on controller-to-controller sharing *only*, then it is utterly unfit for purpose. A huge number of controllers need to share data with processors, and a huge number of processors need to know what applies when data is shared with them. Were this Code to be published in its current form, it would simply be inviting Judicial Review.

    - We note that you use the very same example, i.e. *"a retailer provided customer details to a payment processing company"* on p17, having stated just a few lines above that the Code does not cover such activities! Which is it to be? Logical inconsistencies such as this are clearly unacceptable in a statutory Code, and would not be addressed by the mere removal of the contradictory example. That a draft has been published containing such a glaring contradiction is not just a matter of 'proof reading'; it raises the question of whether the Code *in its entirety* has been properly thought through.

- Given the significant issues generated by interpretations of similar statements in the previous Code (and related ones), *"Neither the GDPR, the DPA, nor this code of*

practice, applies to the sharing of information that does not constitute personal data" is utterly inadequate. And, as pointed out in previous comments, trying to address this matter on the ICO website rather than in the body of the Code makes all such advice or guidance eminently ignorable.

    - Rewrite this section, providing clarity on the difference between **anonymised**, **pseudonymised** and **de-identified** data (i.e. data to which various methods of removing or obscuring *some* obvious identifiers) and actually **anonymous** data (i.e. aggregated statistics to which rigorous statistical disclosure controls have been applied, or data that does not pertain to a natural person at all).

Page 18

- This should be 3 scenarios, not 2, for public bodies.
    - Bulk data sharing
    - Individual data sharing
    - exceptional/emergencies (ie vital interest)

- The current structure encourages public bodies to treat routine behaviour as an emergency, and conflate actions for individuals with actions against groups.

'Deciding to share data'

- What about the right of individuals to be informed about the collection and use of their personal data? What about the Fairness and Transparency requirements of Principle (a)? This section talks about sharing and DPIAs and Data Sharing Agreements but makes no mention *at all* of the provision of information to data subjects!
    - When deciding to share data, one of the things that should be in the forefront of people's minds is the information that they must share with data subjects. If it is, they may think differently about the data they decide to share and process than if they were not thinking about this at all. For this practical reason alone - not to mention the legal requirements, subject rights and underlying principles - this section should be REDRAFTED. (It's almost as if someone wrote this as a tick-box theoretical process, with no sense of how things operate in the real world...)

- Sufficient information must be published such that a data subject, without needing to ask permission of the (public) body - such as by FOI - **should be able to understand how their data is used and why**.

- For larger organisations, the use of a Data Sharing Register - with all relevant documents *proactively* published (otherwise someone will just FOI them...) - would be both good practice and easier for all, especially the data subjects whose rights GDPR and DPA 2018 are supposed to strengthen...

Page 26

- While not explicitly mentioned, the last 2 questions on p26 once again raise the question of data processors: not *"all the organisations that will be involved in the data sharing"* will be controllers in all instances. To have a Code of Practice on data sharing that does not cover situations that will arise naturally as an everyday occurrence would be a complete nonsense.

    - Rethink the decision to make the Code 'controller-to-controller' only, and do the work to make things clear for data subjects and data processors!

Page 27

- The final bullet point contains the single appearance of the word "anonymised" in the entire Code. And it is wrong. The implication in this context is that "anonymised" data is not personal data "at all" - but anonymised data is not necessarily anonymous data, as is well understood.

    - Either explain this properly (as suggested in previous comments) every time the concept appears, or replace the word "anonymised" with the word "anonymous" here so that it is at least legally correct and not misleading.
    - We note you appear to have used the word "anonymous" correctly in three places in the Code - though this is slightly undermined on p22 by the possible inference that "anonymising" will necessarily result in anonymous data.

Page 29

- Bullet point 2: It would only be helpful for a Data Sharing Agreement to have *"a model form for seeking individuals' consent for data sharing"* if consent is the legal basis for sharing. Given consent is not a proper legal basis in many instances, blanket advice like this is unhelpful - tending to reinforce some of the very misconceptions about GDPR and DPA 2018 that the ICO purports to be challenging. (You really do begin to wonder by this stage whether all examples were necessarily chosen for clarity of readers and in law...)

'Fairness and transparency'

- Having taken until 40 pages into the Code to mention these "central" principles, which (as pointed out in other comments) are vital for people to keep in mind from the very outset of thinking about sharing data, this section is disappointingly sparse (just 3 and a bit pages, compared with 6 in the previous Code - which was itself half the length of this one) and poorly illustrated, as well as being weak and lower than other norms for data sharing, notably section 5 of the Code of Practice for data sharing under the Digital Economy Act.

- How does/should the information to existing data subjects change as new data sharing is begun? Especially where, for example, HM Government redefines a public task without legislation?
    - New shares are picked up on p73 in the 'At a glance' box, in the context of data brokers, marketing and credit reference agencies - but not more widely. This should be remedied.

- For public bodies, outside of national security and law enforcement, can any public tasks be justifiably hidden from the public?

'Security'

- While data security is vital, if all data subjects know about data use is that people keep losing it, data sharing is untenable in the long term. We note elsewhere that there should be additional information in the Code about communications with data subjects. While this is often looked at as solely fair processing, given the increased GDPR obligations to report data breaches, organisations with partners who are unusually prone to having accidents,[2] larger entities who do reputationally-significant volumes of data sharing (principally NHSD, DWP, and HMRC) should give serious consideration to the opportunities that come data subjects having a broader range of information on data sharing to give a more informed base when security breaches do happen.

- This section talks about performing "an information risk analysis", and mentions you should "regularly review your security measures" - but it doesn't mention ongoing audit. If you need to know which of your staff have handled what data, that needs to be recorded. Systematically. If data subjects are to be able to know how their data has been used, and by who, then the controllers must continuously record such (meta)data. A Code of Practice on Data Sharing in 2019 that doesn't mention end-to-end audit as good practice will not age well!

- Just noting that the heading, *"Are we still responsible after we've shared the data?"*, on p48 raises once again entirely reasonable questions about 'controller-to-processor' sharing that the Code states it does not cover. Will the version laid before Parliament remain mute on these considerations as well?

'Rights of individuals'

- Given that this section is about *"policies and procedures that allow data subjects to exercise their individual rights with ease"*, it would help if the example of a Data Release Register were provided as good practice - especially for large organisations and public bodies. (If not in this section, then elsewhere in the Code.) As well as demonstrating transparency, such registers provide a central point from which - if

[2] https://www.TheySoldItAnyway.com

done correctly - individuals are more readily able to determine the information they want, while reducing the burden on the organisation of having to manage multiple similar requests.

    - (In general, this and the next section on 'Other legal requirements' are far more clearly understandable and more substantive than vital sections like 'Fairness and transparency'. Maybe exercise a bit more content and quality control from the perspective of novice readers in the next draft?)

'Other legal requirements'

- While Article 8 is clearly one of the most important rights with regard to data sharing, it is not the only one - nor is HRA the only legislation to which (public) bodies must have a regard. It would be helpful to mention HRA Article 14, and the Equality Act 2010, in this section as discrimination arises in data sharing as well as data processing.

- p61: given you mention the duty of confidence here, it would be worthwhile explaining more clearly what that is, how it arises in (common) law, and who - e.g. the National Data Guardian for Health and Social Care - is most competent to determine what this means. A link to the NDG site would be helpful too.

Page 76

- *"If you use a third party organisation to send out campaign materials on your behalf using your database,* ***you are sharing data*** *with that external organisation. You should apply diligence in checking and monitoring what the third party is doing.* ***You are responsible as controller for that data*** *and for compliance with the legislation."*

    - So in this section, again, you are talking about something that the Code has explicitly stated it does not cover (i.e. the controller-processor relationship). Given the long and sordid history of data sharing in political campaigning, and the calibre of lawyer retained by some of the entities involved, one would hope the final Code does not retain such rudimentary loopholes through which any competent lawyer would no doubt drive an entire court case...

'Urgent / emergency data sharing'

- p80: This section should state clearly up front that such data sharing must be *in the* ***vital interests*** *of an* ***identifiable*** *data subject* ***only***.

    - The section should also define "emergency" - in a way that is not something that, say, direct marketers could evade...

DEA Codes

- This section should point out the requirement that documents be published alongside register entries (see the various parts of section 5.1 of the DEA Code) under other Data Protection principles.
    - DEA specifically designed its documents to be routinely publishable. If this Code is not to be (seen to be) weaker than DEA, then his model should be replicated in other parts of this Code, e.g. around templates.

- The Code should be clearer on restrictions that are placed on data as shared. Once a recipient has it, are they permitted to reuse it for any purposes? How is that communicated by the original data controller to the data subject? How is that reflected in the data release register and in whose fair processing?

Data trusts and ethics

- As mentioned in comments above, and given there is no legal form for these as yet - and that any legal form will likely require primary legislation - and because this section is extremely 'forward-looking', rather than reflecting any legal norms, the ICO should simply note that all Data Trusts must follow Data Protection law and this Code, and leave it at that.
    - You might perhaps reference a future code that might exist, should Data Trusts become anything other than a political and legal fiction. But, as written, this section will age very badly.

- For a Code that will likely be published sometime in 2020, intended to last for a decade(?) a 'newsy' update on *"What has been happening in the area of data ethics?"* referencing things done 5 years ago - and just one of a plethora of new bodies that have popped up laying claim to "ethics" in some context or other - will likely also not age well. CUT.

Checklist for Annex A + Annex B templates

- The Code should align with the Digital Economy Act templates, for what should be proactively published in a register of data sharing.

‘Case studies’

- At least the following are necessary, but currently missing:
    - There should be an example of direct care-only data sharing, where someone then wishes to reuse the data for secondary uses. This case study should include the NHS-only opt-out processes such as the National Data Opt-out.
    - Another example should make reference to the treatment of personal data that is required in order for data to be considered anonymous for the purposes of sharing. For example, is merely having a contract or agreement in place sufficient to lawfully share what would ‘otherwise’ be sensitive personal data?
    - No example currently illustrates data subjects dissenting from data sharing for purposes beyond the original purpose for which personal data was provided. This is a serious omission, and should be rectified in the final Code.

‘Things to avoid’

- While it was only a single page (p35 in the 2011 Code), clearly stating what people should avoid when data sharing was very helpful. Firstly, because it cleared up some potential ambiguities, and secondly because stating things succinctly and ‘as a negative’ has a stronger impact - especially in a document of the length of the new Code. The current draft of the Code would benefit from cutting/editing some of the less well-written sections, removing some of the less relevant parts altogether, and adding a short section like this instead.

medConfidential