**Early draft - 6/10/2017: medConfidential response to the Cabinet Office Data Sharing Consultation**

1. medConfidential is grateful to the Cabinet Office for sharing a draft of the Codes with the Cabinet Office Privacy and Commercial Advisory Group of which we are a member. The Codes have clearly benefited from the listening and understanding that came from that process.
2. The culture that produced the policy behind these drafts contains a fatal flaw: an assumption that the system will always work, and that care.data could not happen “here”.
3. That is the same thinking that pervades the Home Office, and leads to them unapologetically threatening to deport mothers, and NHS hospitals demanding ID off an 8 day old baby - the examples are becoming endless, and will continue until the culture that creates them changes. This should be part of digital transformation.[[1]](#footnote-0)
4. For example, the Home Office[[2]](#footnote-1) believes its systems have sufficient integrity to deny an individual a bank account, and that theory is being tested in practice.[[3]](#footnote-2) Departments which are required to take actions in response to the Home Office statement should relay those statements to the citizen involved - and competency can be measured by the public, not other Departments. Do Departments wish to be the defender of Home Office mistakes, or the neutral messenger acting as a legitimate and responsible data controller to their data subjects?
5. GDPR requires transparency and accountability - it’s arguably the only new thing. How much are you going to require of Departments? There is no active support for digital transformation in the current proposals - it supports business as usual far more than supporting change.
6. One of the largest burdens on departments, and impediments to successful data matching and APIs, is error detection and correction.
7. Just because data sharing can be done, it does not necessarily mean it should be done. These principles and Code of Practice will be usable in future Governments, as well as the current administration.
8. In that light, we will comment on the Civil Registration Code of Practice in a separate submission.
9. Just as this Government is committed to telling taxpayers how their money was spent, it should tell citizens how *their* data was used. If the only narrative available to citizens is continual data loss, and if there is no way for citizens to see the benefits of data sharing in the public interest, then public support will continue to decline. On this issue, Cabinet Office and Government thinking is a very long way behind the considered position of the NHS.

**A new Data Protection Bill - with a coverup clause...**

1. The Digital Economy Act was passed with assurances and undertakings from the then-Minister Matthew Hancock MP that it did not amend the Data Protection Act, and the Data Protection Act was seen as a safeguard against some of the most invasive interpretations of the Digital Economy Act.
2. A year on, Matthew Hancock MP is now steering another Bill through Parliament - a new Data Protection Act.
3. As such, some of the “safeguards” that were in the original DEA should also be tested against the new Data Protection Bill. And they are found lacking, due to failures in Clause 15.
4. The goal of clause 15 seems to be to allow processing that was lawful under DPA to continue. However, that is not all clause 15 allows. Due to drafting failures, it allows any Department to exempt itself from the Data Protection Act if it claims the data will be used for a lawful purpose. This is overly broad, and has toxic implications for the Digital Economy Act Codes of Practice.
5. Our further briefings on the Data Protection Bill are available at <https://medconfidential.org/news> (published on or around the 6th October 2017)

##

##

## Comments across multiple codes

1. It is unclear why the Civil Registration code has a UK Statistics Authority imprinteur,[[4]](#footnote-3) and the PSD/fraud/debt has that of the Home Office.[[5]](#footnote-4) The Civil Registration code also seems.

**Resharing**

1. To determine eligibility for services, Departments may, and do, oblige a citizen to provide evidence of medical conditions and other highly sensitive personal data. The purpose of “ill health or mental ill-health” in these codes allows such data to be shared. Once shared, these codes contain no obligations on Departments not to reshare that data.
2. While in the interests of good governance, resharing should be expressly prohibited, since it is unlikely that will be the case until after a major scandal, it must be explicit in every data sharing agreement whether the recipient has the ability to reshare data or not. It is the Department that the citizen interacted with that will be held accountable by citizens through Parliament, the department to which it was (re)shared will receive less than its fair share of criticism.

**Review Boards**

1. The Review Boards that are proposed for Fraud and Debt should also exist for the wider “public service delivery” functions. That is does not is a symptom of wider “data science” governance failures that we address in more detail in other conversations with the Cabinet Office,[[6]](#footnote-5) but summarise the areas of interest to the Codes here.
2. During Bill passage, it was said by the Cabinet Office that the DEA would become the primary vehicle for data sharing in Government. Even if that is not the case, the Codes are likely to be the primary documented standard for data sharing processes.
3. From the perspective of the public, the gateway that Government uses should be irrelevant. The use of divergent standards will be confusing and lead to widespread public distrust - what do the lesser transparent projects have to hide?
4. Similarly, while there are a number of Registers of Data Sharing proposed, including for PSD, there will need to be a public front door to those mechanisms.[[7]](#footnote-6) That will almost certainly have to signpost the work being done by NHS Digital (for all NHS data sharing), and ONS/UKSA (for statistical and some research purposes), and beyond.[[8]](#footnote-7) This is akin to what GDS refer to as a “Register of Registers” - “you don’t have to know the answer, you just have to know where to find it”.[[9]](#footnote-8)
5. The Data Review Board for PSD should be sighted on every project that uses the (successor to) Cabinet Office Data Science Ethics Framework. While it may not cover everything, whatever the successor looks like should be a minimal standard for data sharing. That standard should be exceeded by the Registers, but also exceeded by the material published (the v1 framework assures readers that a PIA can be done in a single side of A4, which seems unwise).
6. The most senior data sharing body in HMG is likely to be the National Statistician’s Data Ethics Committee (NSDEC). It operates in a transparent fashion, to UKSA standards - we expect this to continue. While complex issues may need advice from NSDEC, it should not routinely review the minutiae of Government Departments operations, to deliver on its remit, there must be paperwork available to review.
7. In the case of future failures, which will happen, it will be necessary for there to be some assessment process. While whatever is put in place now will be shown to be insufficient by subsequent future events, a beginning will make that problem tractable. It would be unwise to repeat the chaos that followed the 2007 HMRC child benefit discs loss.
8. The Cabinet Office will be partially tasked with fixing the failures caused by flawed data sharing, and in the long, long, term, such failures will occur.[[10]](#footnote-9) Whether those failures are narrow or systematic depends only on quality and transparency of Governance that was put in place now. The examples of care.data, and Google DeepMind/Royal Free should be run through this model to test whatever is proposed.[[11]](#footnote-10)
9. It is becoming expected that public safeguards will be undermined in practice - the panoply of failures that led to Grenfell Tower will hopefully remain the largest monument to administrative failure for a long time.

## Detailed Comments

### Public Service Delivery (etc)

**Section 6 - transparency**

1. When documents are published, or be able to be read, it should be expected that they are published within the Cabinet Office Register.
2. Additionally, for agreements acquiring data which was supplied via a digital service, or where a digital service is used by some of those citizens via one of the involved department, then the data shared, reasons, and benefits *must* be visible via that digital service.
3. Just because data sharing can be done, it does not necessarily mean it should be done. These principles and Code of Practice will be usable in future Governments, as well as the current administration.
4. Just as this Government is committed to telling taxpayers how their money was spent, it should tell citizens how *their* data was used. If the only narrative available to citizens is continual data loss, and if there is no way for citizens to see the benefits of data sharing in the public interest, then public support will continue to decline. On this issue, Cabinet Office and Government thinking is a very long way behind the considered position of the NHS.

**Paragraphs**

1. **Paragraph 12 - Principle 1:** The Code of Practice proposes a higher standard for transparency than the minimum requirements of the ICO. Either the CO are committed to those standards or they are not. If they are committed to transparency, then Principle 1 should state what those standards are - it currently states the minimum anyone can get away with; not the standards the Code itself expects to be upheld (see Section 6).
2. There are other areas of guidance which cover data sharing, and the Principles should also cover those.
3. **Paragraph 12 - Principle 2:** The exceptions should not be named in the short version of the Principle. The Principle is transparency; the current wording suggests the Principle is primarily secrecy.
4. **Paragraph 12 - Principle 7:** Multiple processes are required, not just the DSEF, which is unfit for purpose, and unused by CO’s own admission.
5. **Paragraph 13** should become a new “Principle 0”: follow the law. While this should not need to be restated, given the tendency for data sharing projects to run into legal problems, it would be wise to make it entirely clear that following the Code of Practice is not the same thing as following the Law.
6. **Paragraph 14(2):** “use *or develop APIs to run binary checks”* - where an API is more appropriate (such as for the vast majority of transactional services), some APIs may need to be developed for the purpose - especially as the DEAct becomes established. As such, the Code should encourage the development of appropriate APIs, not just their use.
7. **Paragraph 25(8):** safeguarding and National Security issues are very different - those two should be separated into their own bullet points.
8. **Paragraph 91:** The categories of stakeholders mentioned should be “Government, ICO, *and the public***”.** Given the rhetoric of section 6 (transparency), it is surprising\* that it is missing in other places where that transparency should be effective.
9. **Paragraph 91:** whether should be “whether and how”. The details matter.

**Health data**

1. Paragraph 31: We note that the Secretary of State for Health remains outside of these powers, and the Cabinet Office has not consulted on modifying the Regulations to include them. It would require a public consultation on any change, and the Cabinet Office has chosen not to take this opportunity to do so. The current Codes make no special provision for health data, and would need to be rewritten to do so, which would also require a public consultation on what would be a substantial change.
2. It would be the height of absurdity for the medical records of the nation for it to be explicit policy for be treated with a level of disregard that GCHQ does not allow for their cafeteria menus.[[12]](#footnote-11)

## Research Code of Practice

1. **Paragraph 22:** Reword “Suffered a reported or suspected data breach”. While we agree with and understand the principle, it is the failings that caused a breach of the rules that should be rectified (/punished), not the reporting or the suspecting of a data breach. Doing the right thing should explicitly be rewarded, not penalised.
2. We raise several issues about how the Research Code is being applied in practice in our recent annual report (page 6).[[13]](#footnote-12)

## Statistics Code of Practice

1. **Paragraph 3.1:** “all that is necessary to minimize the risk” is not the standard that legislation requires. This is a clear example of the weakening of a statutory safeguard down to something meaningless and ineffective to satiate a bureaucrat whose demand for data is as great as their desire to avoid any accountability or responsibility for their actions[[14]](#footnote-13) - two desires that are impossible to entirely meet. This failing is one of the worst aspects of the civil service and should be removed from the Code, and replaced with the language that legislation, and public trust in statistics, requires - which is a higher standard than “minimize the risk”.
2. “Consent” here is that of the data controller/processor, and not the consent of the data subject. This paragraph ignores the data subject entirely, and does not require that dissent from processing be honoured - indeed, the Code as consulted doesn’t mention dissent at all. While this is primarily a GDPR issue, the scope of consent/dissent here must be considered given the effects of the Data Protection Bill. The Code must be as clear as the Law: **Where dissent is valid, it must be honoured.** While statistical purposes may override some dissents, it does not override them all. Given the pernicious effects of the Home Office[[15]](#footnote-14) desire to acquire any data acquired anywhere, such as the school census, if the Statistics Code is not explicit on the punitive reuse of data, then many of the claims of statistical impartiality are ineffective.
3. Information should be on a central ONS/UKSA site showing the overall benefit of research/statistical data use, and not separated across data silos. The register of data uses within this code, should, in practice, be part of a larger mechanism to inform citizens who wish to look (because, for example, they have just responded to a survey/census) about how the UKSA/ONS uses data, and the benefits of the information that is provided. The census has long assumed public trust. While it has done so correctly, since 2011, the longer term effect of the Home Office use of the school census to deport children’s classmates means that the next census will not, entirely, take place in a culture of unwavering acceptance. It would be unwise of UKSA to ignore that issue until the problem has had statistically measurable effects.

medConfidential

1. See paragraphs 1 and 2 of our the recent supplement to our annual report: <http://medconfidential.org/wp-content/uploads/2017/09/government-supplement.pdf> [↑](#footnote-ref-0)
2. While the culture is pervasive across Whitehall, the examples of mistakes are most clearly recognisable in the Home Office. Which, while it may consider citizens the same way DEFRA considers animals, DEFRA has the advantage that the cages it regulates don’t contain data subjects with human rights. [↑](#footnote-ref-1)
3. [https://www.theguardian.com/uk-news/2017/sep/22/home-office-errors-already-leading-to-people- being-denied-bank-accounts](https://www.theguardian.com/uk-news/2017/sep/22/home-office-errors-already-leading-to-people-being-denied-bank-accounts) [↑](#footnote-ref-2)
4. [https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and- regulations/data-sharing-code-of-practice](https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and-regulations/data-sharing-code-of-practice) [↑](#footnote-ref-3)
5. [https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and- regulations/information-sharing-code-of-practice-public-service-delivery-debt-and-fraud](https://www.gov.uk/government/consultations/digital-economy-act-part-5-data-sharing-codes-and-regulations/information-sharing-code-of-practice-public-service-delivery-debt-and-fraud) [↑](#footnote-ref-4)
6. At the time of writing, it is our intent to publish a detailed piece on that alongside our publication of this response. Both will be found at <https://medconfidential.org/news> if we forget to update this footnote. [↑](#footnote-ref-5)
7. This will not be part of the DEA Codes itself, but where it interfaces with the rest of GDS. There should be a single URL, likely owned by the National Statistician, which serves as a single start point. It is “extremely likely” that there will be a single URL, owned by a civil society organisation, doing similar, although it will likely have a different focus... [↑](#footnote-ref-6)
8. GDPR will require additional publications of which the ICO may require some form of index. [↑](#footnote-ref-7)
9. <https://quoteinvestigator.com/2012/04/02/know-where-to-find/> [↑](#footnote-ref-8)
10. It could be argued that issues in the CO Data Science Ethics Framework v1 were designed to last only as long as it would take for them to be someone else’s problem. PS: Good luck in your next role [↑](#footnote-ref-9)
11. We are happy to assist in this work. [↑](#footnote-ref-10)
12. It may already be true, but it would be unfortunate to deliberately make it worse. [↑](#footnote-ref-11)
13. <http://medconfidential.org/wp-content/uploads/2017/09/annual-report.pdf> [↑](#footnote-ref-12)
14. There is currently a monument to such bureaucratic indifference in West London. [↑](#footnote-ref-13)
15. Seebriefings for second reading of the Data Protection Bill at <https://medconfidential.org/news> [↑](#footnote-ref-14)