

Consultation by the Department for Digital, Culture, Media & Sport (DCMS):

“The UK Government’s intention to develop a National Data Strategy”

[Response from use MY data](#)

Closure date: 14 July 2019 to nationaldatastrategy@culture.gov.uk

National Data Strategy team,
Room 4.52,
100 Parliament Street,
Westminster,
London, SW1A 2BQ.

Introductory Note

We asked the members of the use MY data Advisory Group for views on the content of the consultation, which we have incorporated into a coordinated use MY data response.

As with all the responses we collate on behalf of use MY data, these may contain contrasting views from members. It is inevitable that we will receive a range of views from members, and all these will be included in our response. We have always seen our ability to represent contrasting views as a strength.

This is clearly a large consultation document, so members have made some brief comments which we are highlighting to you which you might want to consider.

We recognise that the consultation is about a data strategy which covers many different government datasets, and not just health. Whilst use MY data has focused largely on health data, our members have also been involved in conversations about the uses of wider data, and have previously responded to consultations on Artificial Intelligence, the Centre for Ethics and the National Data Guardian.

We note the positive commitment that a full consultation on the draft strategy will be run later in 2019 and look forward to more information on that.

Consultation questions

1.1. How can organisations (private, public or third sector) demonstrate trustworthiness in their use of data?

Our overall principles include: Transparency, inclusion, patient/citizen oversight.

Everything that happens should be clear and out in the open, so that there are no surprises. Public/patient oversight panels are useful. There should be clear accountability routes, and both discussions and decisions about how data are used should be published.

We would point out that the starting point here is not simply a case of DEMONSTRATING trust but BUILDING trust. Trust is a feeling of reassurance between two or more parties - it is not a case of one party 'demonstrating' it.

Organisations need to be as pro-active in this area as they are with what they consider to be 'good news'

1.2. How easy is it for the public to find about how information provided to or inferred about them by an organisation is being used?

Despite assurances related to the implementation of the GDPR in May 2018, we consider this remains very difficult.

We have heard from some that in health, finding this out from your GP and hospital is difficult and often unhelpful.

For example, of three recent healthcare Subject Access Requests submitted this year by one of our members as part of a test-project, none of the Data Controllers have responded with the information within the prescribed 30-day period (the average time taken was around 60 days).

We are aware that even when GP Practices use our data for reasonable purposes, outside of our direct care (national cancer diagnosis audit, CPRD), they do so on the basis that this fact will not be easy to find out.

Perversely, the GP is at the forefront of the conversation with their patients, not least about government uses of data which may cause harm or distress. We know that uses of data such as the Home Office link to Health data in 2018 caused significant concern to some members.

1.3. Are organisations (private, public or third sector) using personal data in ways that may damage trust?

We think that the levels of transparency overall are very poor, and that very few if any organisations meet our definition of transparency.

The buying of mail lists is still felt to be an ongoing problem (from members; personal experience).

In general, once you do know where data is being used, it is impossible to make a balanced, rational assessment unless you also know what the benefits are, where they may be consequences, who profits and who loses (in all meanings of the word).

1.4. In what ways are companies making money from personal data? How profitable are these activities?

Our members found this difficult to comment, but highlighted practices whereby they still receive phone calls about accidents they have not had, raising questions about where the companies are getting phone numbers from, particularly when ex-directory.

1.5. Do people know how information provided to, or inferred about them by, an organisation (private, public or third sector) is being used, stored and shared?

This is a very wide-ranging question, on which we do not have any specific evidence. However, but we could offer a view that as a general statement the bulk of the population do not know these matters.

As evidence for the lack of public knowledge we would flag up the lack of awareness of cancer registration that was flagged up in both the Cancer Research UK/Macmillan and Understanding Patient Data/Ipsos Mori work.

1.6. To what extent are people concerned about how data about them is used, stored and shared? Are some groups more concerned than others? Are there particular categories of data that raise more concerns than others?

This question sees a range of views from members, and again the question is very wide.

Whilst some members would not be concerned, we recognise that there may be certain groups (where perhaps their medical condition/lifestyle choices are still not socially acceptable to everyone) who would be concerned.

1.7. What commercial practices or behaviours have affected trust in the use of personal data? Have targeted advertising and 'recommending' affected trust?

We know that such things as the Deepmind/Royal Free deal was damaging to trust. The mechanism and accountability were unclear, as were the commercial benefits would be gained.

A slightly different concern was around the use of tracking cookies being an area where there is some concern. There are many internet business models

where services are provided for free only if you accept their terms and conditions re gathering, use and sharing of data.

1.8. Have the General Data Protection Regulation (GDPR) and Data Protection Act 2018 made people more concerned about how personal data is managed? How has it influenced their behaviour?

On the back of our recent use MY data workshops we could argue that it has raised peoples awareness, but that the concern (and nervousness) has been on the part of the large data controllers, as reflected by poorer and more confusion access routes for researchers to get access to the data.

We could express a view that GDPR seems to have made some of the public more aware but that it has not influenced their behaviour.

1.9. How far do existing protections, such as in the Data Protection Act, go in promoting transparency and trust? What, if anything, should the government do to further build trust?

The Act does not “promote”, but rather makes provision for this.

We have heard consistently from members that the government should have a concerted effort in the area of communications generally. We have also heard from workshops that there needs to be a rebalancing from “protection” to “usage and benefits”.

2.1. Are people aware of how to manage personal data about them? Do they know about tools to control access?

We would firstly ask how much of this question really is about the UK (as stated above), and how much is focused on England, because there are differences in what is available to people in different parts of the UK.

In general, we would consider that the vast majority of citizens do not about how to manage personal data about them, if you mean the rights to get personal data corrected or deleted.

In the case of the National Data Opt-out, we are aware that NHS Digital made a commitment¹ in May 2018 to monitor the implementation over a six-week period. We are not aware of the results of the monitoring being published.

In terms of tools to manage data (and in particular incorrect data), we would also like to reflect that we are not sure even the NHS knows how to get data properly corrected.

¹ <https://www.england.nhs.uk/2018/05/nhs-launches-public-campaign-to-highlight-new-stronger-protections-around-health-and-care-information/>

- 2.2. How does effective participation and data use differ by location and demographic group across the UK? What does this look like in urban areas, rural areas and more remote parts of the country?**

We would note that it might be useful to look at “disease” group too.

- 2.3. How does effective participation and data use differ by sector?**

Difficult to comment, as really not sure what is meant by participation in this context.

- 2.4. What barriers to participation do different groups face? How are marginalised and vulnerable groups affected?**

We would note that defensive attitudes by professionals - perceived probably as creating unnecessary additional work and suddenly being accountable for the cause of data errors.

- 2.7. In which professions are data skills most important?**

We would highlight that this is not a ‘professionals’ skill but is necessary for everyone - stop thinking in silos.

- 2.8. Are the relevant skills available and supported where they’re needed?**

No - outside of schools - it’s often necessary to have these skills to get most non-manual jobs (but we suspect there would be little appetite to train somebody in a job). There are computer skills classes available (at a charge) at local education establishments such as colleges and free one’s at libraries:

- 2.9. Is industry able to provide the relevant skills or is further skilling needed through the education system?**

We feel that this would not be a question of being able but of willingness. Clearly, the education system needs to respond to changes in skills needed for employment.

- 3.1. Are there specific challenges that small and medium businesses or non-profit organisations face? How do these vary among different types of organisations?**

There are specific challenges purely because of in small size businesses where the key skill may not be IT related but some other skill or knowledge that drives the business forward. Small businesses and non-profits are likely to have less financial knowledge and knowhow about how to implement IT within their business or how to keep IT and user knowledge up to date.

Generally, we see that access to (aggregated, non-disclosive) data remains difficult and fractured. There are no reasons why such data cannot be published and better managed, so that increasing stakeholders can utilise this asset. Where there are potential concerns about small-numbers (with the risk of potential reidentification), these concerns should be clearly expressed and public opinion sought as to the reality and impact of any perceived risk, balanced against the potential benefits.

4.7. What kinds of data should businesses and non-profit organisations make openly available? And why?

The default position should be data is open unless that can be shown to be harmful.

4.9. Where appropriate, how might government encourage businesses and non-profit organisations to share more data they hold, where it cannot be made open?

By taking a clear lead in these matters - don't just enact - act!

Exemplify opportunities to realise added value from third party exploitation of corporate information.

4.10. What is the best approach to valuing public sector data in order to reflect its potential to stimulate private sector growth and to offer wider public benefits (financial or non-financial)?

An option is to make it low fixed-cost and derive recompense from the added value generated by third parties. High fixed costs will make access to and exploitation of information the preserve of the FAANGs (Facebook, Apple, Amazon, Netflix and Google) and other large corporates. This will stifle innovation.

4.11. How can the public sector quantify, evaluate and weight these benefits in order to determine the terms on which the data could be made available?

Spend little time on attempting to forecast likely benefits but instead spend much more time on developing effective contracts for profit sharing.

5.1. How effectively are government and the wider public sector collecting, sharing, analysing and storing the data it holds? What does good practice look like? What does bad practice look like?

It is difficult to be specific, but in general it is felt that this is ineffective. We have silos of information in health which involves patients repeating information multiple times and health professionals not having all helpful information to hand to care for patients.

As an example of poor practice, we would highlight the lack of transparency over the sharing of health data between NHS Digital and the Home Office.

5.2. What are the main barriers to more effective data use within government? Are there barriers in cases where government works with the private sector?

Slow, inconsistent and possibly over-conservative decision making, including different rules for access to different health data.

Overarching thoughts

The development of Trust

We note that the aim of the National Data Strategy is to drive “*the collective vision*” that will support the UK to build a world-leading data economy. We would emphasise the term “collective” and would stress that patients and citizens are equal partners in the design, implementation and benefits.

“It will help ensure that all citizens and organisations trust the data ecosystem, are sufficiently skilled to operate effectively within it, and can get access to high-quality data when they need it.”

Intelligence, not just data

We would emphasise the difference between data and intelligence. We would expect any strategy with the aim of empowering citizens is focused on putting useful intelligence in their hands, from which they can make informed decisions. Our members have commented on many occasions that we are data-rich but intelligence-light. The strategy should reflect this.

Summary

We hope that the comments from use MY data are helpful.

We are happy to be contacted by the consultation team, and we are happy for our response to be shared as required by the consultation team. Our response, once submitted, will also be added to the use MY data website (www.useMYdata.org.uk)

Any contact should be made through Alison Stone, use MY data Coordinator, at alison@usemydata.org.uk

About use MY data

use MY data is a movement of patients, carers and relatives

use MY data supports and promotes the protection of individual choice, freedom and privacy in the sharing of healthcare data to improve patient treatments and outcomes.

use MY data endeavours to highlight the many benefits that appropriate usage of healthcare data can make, to save lives and improve care for all.

use MY data aims to educate and harness the patient voice to understand aspirations and concerns around the use of data in healthcare delivery, in service improvement and in research, aimed at improving patient decision making, treatment and experience.

Our vision

Our vision is of every patient willingly giving their data to help others, knowing that effective safeguards to maintain the confidentiality and anonymity of their data are applied consistently, transparently and rigorously.

What we do

- ❖ We promote the benefits of sharing and using data to improve patient outcomes with sensible safeguards against misuse.
- ❖ We act as a sounding board for patient concerns and aspirations over the sharing and using of data in healthcare and health research.
- ❖ We provide learning resources for patient advocates on patient data issues, including:
 - hosting workshops for patients and the public, focussing on topics related to patient data
 - a library of resources of data security, consent
 - narratives from individuals about how collecting, storing and using data can help patients.
- ❖ We advocate public policy that supports the effective use of patient data within appropriate frameworks of consent, security and privacy, and with the aim of providing benefit to patients and their health care services.

www.useMYdata.org.uk
getinvolved@useMYdata.org.uk
 **@useMYdata**