NUFFIELD COUNCIL ON BIOETHICS

Response to National Data Guardian for Health and Care's Review of Data Security, Consent and Opt-Outs Consultation

September 2016

Introduction

This response draws on the conclusions of the Nuffield Council on Bioethics' report, *The collection, linking and use of data in biomedical research and health care: ethical issues* which was published in February 2015. The full report is available at http://nuffieldbioethics.org/project/biological-health-data/

General comments

We agree that there is a clear public interest in the responsible use of data to improve well-being through improved health advice, treatment and care, as well as through increasing economic prosperity more generally. It is clear that this must be accompanied by measures which manages threats to welfare and prevents possible harms to individuals, groups or the wider public (harm could potentially be caused by failure to use data appropriately in the public interest, as well as by misuse of data).

However, we would argue that the model put forward here is, in itself, insufficient and needs to be supplemented by further elements in order to prevent harms and secure public trust - an approach that focusses on data security and consent alone cannot guarantee that a use of data is morally desirable.

For example, while seeking consent respects rights that individuals may have to make decisions about matters that may affect their interests, it cannot protect them from potentially harmful consequences of data use. Merely acting in accordance with consent (or with the law) cannot excuse data users from their moral duties towards data subjects, indeed towards all those who have a morally relevant interest the data initiative, whether they are people from whom the data were initially collected or others who stand to be affected by their use.

In our report we identified a policy and governance vacuum between the overarching legal provisions, intended to safeguard the privacy of individuals, and the administration of data use aimed at securing public benefits. We argue that filling this vacuum requires a dynamic, reflective process that acknowledges the importance of general principles (like the right to consent) but gives effect to these against a background of norms that apply in concrete circumstances.

We suggest that three sorts of considerations are relevant to defining a set of morally reasonable expectations about how data should be used in any given initiative, giving proper attention to the morally relevant interests at stake:

- the norms of privacy and disclosure applicable among those who participate in a data initiative
- the ways in which individual freedoms are respected, for example, the freedom to modify these norms by consent
- the form of governance that will give acceptable assurance that people's reasonable expectations will be met

We recommend that the use of data in biomedical research and health care should be in accordance with a publicly statable (capable of being articulated in a way that is meaningful, and understandable to those with interests at stake) set of morally reasonable expectations and subject to appropriate governance.

- **The set of expectations about how data will be used in a data initiative should be grounded in the principle of respect for persons.** This includes recognition of a person's profound moral interest in controlling others' access to and disclosure of information relating to them held in circumstances they regard as confidential.
- **The set of expectations about how data will be used in a data initiative should be determined with regard to established human rights.** This will include limitations on the power of states and others to interfere with the privacy of individual citizens in the public interest (including to protect the interests of others).
- **The set of expectations about how data will be used (or re-used) in a data initiative, and the appropriate measures and procedures for ensuring that those expectations are met, should be determined with the participation of people with morally relevant interests.** This participation should involve giving and receiving public account of the reasons for establishing, conducting and participating in the initiative in a form that is accepted as reasonable by all. Where it is not feasible to engage all those with relevant interests – which will often be the case in practice – the full range of values and interests should be fairly represented.
- **A data initiative should be subject to effective systems of governance and accountability that are themselves morally justified.** This should include both structures of accountability that invoke legitimate judicial and political authority, and social accountability arising from engagement of people in a society. Maintaining effective accountability must include effective measures for communicating expectations and failures of governance, execution and control to people affected and to the society more widely.

The participation of people with morally relevant interests in the design and governance of data initiatives allows the identification of relevant privacy norms and the development of governance measures (such as design of consent and

authorisation procedures) in relation to these norms; it allows preferences and interests to be expressed and transformed through practical reasoning, and account to be given of how these interests are respected in decision making, helping to foster trust and cooperation. The principle of accounting for decisions ensures that expectations, as well as failures of governance and control, are communicated to people affected and to others more widely. It also ensures that data initiatives remain in touch with changing social norms.

Recommendations for this review:

In this model, we would like to see a clearer articulation of how the principles of participation and accountability will be put into practice in the governance of data. This goes beyond security measures and offering the opportunity to opt out of data sharing, and involves putting in place continued opportunities for those with relevant interests to *find out about, engage with and influence* how data are used.

For example, we have recommended that:

- An independent, broadly representative group of participants should be convened to develop a public statement about how data held by the HSCIC/NHS Digital should be used, to complement the Code of Practice on confidential information. This should clearly set out and justify what can reasonably be expected by those from whom data originate and be able to demonstrate that these expectations have been developed with the participation of people who have morally legitimate interests in the data held by the HSCIC, including data subjects, clinical professionals and public servants.
- In addition to implementing the recommendations of Sir Nick Partridge's review, all Data Sharing Agreements held by the HSCIC should be published, along with the findings of a periodic independent audit of compliance those agreements.
- HSCIC Data Sharing Agreements should include a requirement to maintain an auditable record of all individuals or other legal entities who have been given access to the data and of the purposes to which they are to be put; this should be made available to all data subjects or relevant authorities in a timely fashion on request

Comments on specific questions

Question 4: The review proposes ten data security standards relating to Leadership, People, Processes and Technology. Please provide your views about these standards.

Number 6 in this list reads *"Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately*

following a data breach or a near miss, with a report made to senior management within 12 hours of detection."

We would add to this that privacy breaches involving individual-level data that occur in health services and biomedical research projects should be reported in a timely and appropriate fashion to the individual or individuals affected, and that the Government should make enforceable provisions to ensure this happens.

Question 9: What support from the Department of Health, the Health & Social Care information Centre, or NHS England would you find helpful in implementing the ten standards?

We recommend that HSCIC / NHS Digital maintain prospective assessments to inform the most effective methods for preventing inadvertent or fraudulent accessing of personal health care data by unauthorised individuals.

Question 12: Do you support the recommendation that the Government should introduce stronger sanctions, including criminal penalties in the case of deliberate or negligent re-identification, to protect an individual's anonymised data?

We would support and welcome this recommendation, though we propose it should be broadened a little. In our report we recommended that the Government legislate to introduce criminal penalties, comparable to those applicable for offences under the Computer Misuse Act 1990, for *deliberate* misuse of data (not only anonymised data) *whether or not* it results in demonstrable harm to individuals, since it is possible that individuals may not be aware of the cause of disadvantages that they may experience as a result of data misuse, and our commissioned research showed that the legal test for harm is too difficult to meet in many cases of morally significant disadvantage. In response to the consultation on the role of the National Data Guardian (NDG) for Health and Care in December 2015, the Council recommended that the powers of the NDG should include the initiation of criminal proceedings for the deliberate misuse of data.